ID	Space / Document	Type	Title
SYT-4909	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	Säteilyturvakeskuksen määräys ydinlaitosten ja niiden toimintaan liittyvien ydinaineiden ja ydinjätteen kuljetusten turvajärjestelyistä
SYT-4910	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	Luku 1 Yleiset säännökset

SYT-4908	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**1 § Soveltamisala**
SYT-5227	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Tätä määräystä sovelletaan ydinvoimalaitoksiin, käytetyn ydinpolttoaineen ja muu...

SYT-6089	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Tätä määräystä sellaisenaan sovelletaan myös sellaisiin ydinlaitoksiin, jotka si...
SYT-6090	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Muihin kuin 1 ja 2 momentissa tarkoitettuihin ydinlaitoksiin ei sovelleta, mitä...
SYT-6088	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyihin kuuluvat fyysiset turvajärjestelyt ja tietoturvallisuus.

SYT-4906	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**2 § Määritelmät**
SYT-5228	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Definition	1) uhkatilanteella tilannetta, jossa havaitaan tai on syytä epäillä turvallisuut...
SYT-5225	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Definition	2) poikkeamalla normaalitilasta poikkeavaa tilannetta, jossa tapahtuu onnettomuu...

SYT-5226	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Definition	3) vaarallisella esineellä esinettä, esineen jäljitelmää ja ainetta, jolla voida...
SYT-5223	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Definition	4) yhteisvialla ydinlaitoksen kahden tai useamman järjestelmän, rakenteen tai la...
SYT-5224	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Definition	5) turvallisuuslohkolla sellaisia fyysisesti toisistaan eroteltuja tiloja ja nii...

SYT-5221	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Definition	6) turvallisuuden kannalta keskeisellä järjestelmällä, rakenteella tai laitteell...
SYT-5222	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Definition	7) vasteella turvallisuutta vaarantavan toiminnan pysäyttämistä, tilanteen halli...
SYT-5219	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Definition	8) hälytyskeskuksella toimintoa ja tilaa, jossa seurataan turvavalvontajärjestel...

SYT-5220	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Definition	9) valvomolla tai ohjauspaikalla toimintoa ja tilaa, jossa seurataan ja ohjataan...
SYT-4907	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**Luku 2 Turvajärjestelyjen periaatteet ja suunnitteluperusteet**

SYT-5231	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**3 § Turvajärjestelyjen yleiset periaatteet**
SYT-5232	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyjen perusperiaatteista ja vaatimuksista määrätään ydinaineita ja...
SYT-5229	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyt on suunniteltava ja toteutettava syvyyssuuntaisen puolustuksen...

SYT-5230	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyihin liittyvät järjestelmät, rakenteet, laitteet ja ohjelmistot s...
SYT-5246	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Ydinlaitos ja kuljetukset, sekä niiden toiminnot, järjestelmät, rakenteet, laitt...

SYT-5235	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**4 § Riskienhallinta**
SYT-5237	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyt on suunniteltava ja toteutettava riskitietoisesti. Luvanhaltija...
SYT-5233	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Sen lisäksi, mitä kyberturvallisuuslain (124/2025) 7 §:ssä säädetään kyberturval...

SYT-5234	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Ydinlaitoksen riskienhallinnassa on otettava huomioon kansainväliseen ydinmateri...
SYT-5247	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**5 § Suunnitteluperusteuhkan mukaiset suojaustarpeet**
SYT-5243	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyt on suunniteltava ja toteutettava suunnitteluperusteuhkan mukais...

SYT-5241	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Toteutuksessa on otettava huomioon erilaiset tavat 1 momentissa tarkoitetun toim...
SYT-5242	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Tilaturvallisuudessa on suojauduttava fyysisiä uhkia, vakoilua ja vaikuttamista...
SYT-5239	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**6 § Syvyyssuuntaisen puolustuksen periaatteen toteuttaminen**

SYT-5240	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on suunniteltava ja toteutettava turvajärjestelyt siten, että turv...
SYT-5236	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyjen ennaltaehkäisevät toimet, havaitseminen, viivytys ja vaste se...
SYT-5238	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyihin liittyvät järjestelmät on pääsääntöisesti suunniteltava ja t...

SYT-5250	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvallisuuden kannalta keskeisten tietojärjestelmien tietoliikenne on puhelinjä...
SYT-5248	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**7 § Turvallisuusmerkityksen arviointi ja konfiguraationhallinta**

SYT-5249	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on arvioitava järjestelmien, rakenteiden, laitteiden, ohjelmistoje...
SYT-5244	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on ylläpidettävä ajantasaista tietoa turvajärjestelyihin liittyvis...

SYT-5245	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on varmistettava, että ydinlaitoksen toiminnassa ja kuljetuksissa...
SYT-5261	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**Luku 3 Johtaminen ja toimintakulttuuri**

SYT-5262	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**8 § Turvajärjestelyjen johtaminen**
SYT-5259	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyjen hallintajärjestelmän on sisällyttävä luvanhaltijan johtamisjä...

SYT-5260	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Tietoturvallisuuden hallintajärjestelmän on toteutettava standardia ISO/IEC 2700...
SYT-5257	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**9 § Turvajärjestelyt organisaation toimintakulttuurissa**

SYT-5258	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelynäkökohdat on otettava huomioon luvanhaltijan toimintakulttuuriss...
SYT-5255	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelynäkökohdat on otettava huomioon turvallisuuteen liittyvien inhimi...
SYT-5256	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**10 § Insider-uhkien torjunta**

SYT-5252	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijalla on oltava järjestelmälliset ja monialaiset menettelyt, joilla ha...
SYT-5253	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on tunnistettava tehtävät, joissa yhdelle henkilölle voi syntyä ma...

SYT-5254	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**11 § Turvajärjestelyjen ja turvallisuuden muiden osa-alueiden rajapintojen hallinta**
SYT-5251	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Ydinlaitosta ja sen kuljetuksia sekä muuta toimintaa koskevassa päätöksenteossa...

SYT-5271	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	Luku 4 Henkilöstö ja osaaminen
SYT-5272	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	12 § Henkilöstö

SYT-5269	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on määriteltävä turvajärjestelyihin liittyvät tehtävät sekä tehtäv...
SYT-5270	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyjen henkilöstömitoituksen on perustuttava suunnitteluperusteuhkaa...
SYT-5267	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Keskeisten turvajärjestelyihin liittyvien henkilöiden ja muiden resurssien on ol...

SYT-5268	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**13 § Osaaminen**
SYT-5265	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvaorganisaation osaamisen kehittämiseen ja koulutukseen on oltava käytettävis...
SYT-5266	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on huolehdittava siitä, että koko ydinlaitoksessa ja kuljetuksissa...

SYT-5263	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**14 § Turvahenkilön asu**
SYT-5264	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Sen lisäksi, mitä ydinenergialain 156 §:ssä säädetään turvahenkilön asusta, on t...

SYT-5282	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	Luku 5 Ydinlaitoksen alue ja vyöhykkeet
SYT-5284	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	15 § Turvajärjestelyvyöhykkeet ja tietoverkkojen vyöhykkeet

SYT-5280	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Ydinlaitokselle on määriteltävä sisäkkäiset turvajärjestelyvyöhykkeet. Vyöhykkei...
SYT-5281	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Ydinlaitoksen turvajärjestelyvyöhykkeitä ovat

SYT-5278	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on suojattava tietoverkot jakamalla ne tietoturvavyöhykkeisiin nii...
SYT-5279	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Tietojärjestelmien riskimerkityksen perusteella on toteutettava tietoliikenteen...

SYT-5276	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**16 § Liikkumis- ja oleskelurajoitusalueen merkitseminen**
SYT-5277	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Sen lisäksi, mitä liikkumis- ja oleskelurajoituksista annetun sisäministeriön as...

SYT-5292	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**17 § Laitosalueen rajaaminen ja kulku**
SYT-5293	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Laitosalue on rajattava kaksoisesteellä ja sen väliin jäävällä eristysvyöhykkeel...
SYT-5295	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Laitosalueelle johtavien kulkuaukkojen lukumäärä on pidettävä niin pienenä kuin...

SYT-5290	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**18 § Suojattu ja vitaalinen alue**
SYT-5291	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Suojatut ja vitaaliset alueet on määriteltävä riskitietoisesti laitoksen ominais...
SYT-5288	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Liikkuminen ja oleskelu vitaalisella alueella on rajoitettava turvallisuuden kan...

SYT-5289	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**19 § Turvajärjestelyvyöhykkeiden valvonta**
SYT-5286	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyvyöhykkeillä on tehtävä valvontaa teknisin menetelmin ja partioim...

SYT-5287	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyvyöhykkeillä on oltava jatkuvatoimisia turvavalvontajärjestelmiä,...
SYT-5283	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Laitosalueella turvavalvontajärjestelmien on oltava mahdollisimman katveettomia.

SYT-5285	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**20 § Tietoverkkojen ja -järjestelmien valvonta**
SYT-5296	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Tietoverkkojen ja -järjestelmien normaalitila on määritettävä ja niitä on valvot...
SYT-5294	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijalla on oltava menettelyt tietojen eheyden ja saatavuuden varmistamis...

SYT-5304	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	Luku 6 Rakenteelliset, tekniset ja toiminnalliset turvajärjestelyt
SYT-5306	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	21 § Rakenteelliset ja tekniset turvajärjestelyt

SYT-5302	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on varmistettava rakenteellisin ja teknisin järjestelyin riittävä...
SYT-5303	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyjen kannalta merkitykselliset järjestelmät on erotettava ja suoja...
SYT-5300	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**22 § Liikenteen valvonta**

SYT-5301	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Henkilöitä, ajoneuvoja ja tavaraliikennettä on valvottava ydinlaitokselle sisään...
SYT-5298	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Vaarallisten esineiden ja haitallisten laitteiden pääsy ydinlaitokseen ja kuljet...
SYT-5299	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Ajoneuvojen turvallisuustarkastus on suoritettava sitä varten erikseen rajatulla...

SYT-5332	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**23 § Henkilöiden kulun järjestäminen**
SYT-5333	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Pääsyoikeudettomien henkilöiden pääsy ydinlaitokseen ja kuljetukseen on estettäv...
SYT-5335	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on järjestettävä henkilöiden kulku laitosalueelle ja sieltä pois s...

SYT-5328	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Liikkuminen ydinlaitoksessa ja sen alueella, sekä ydinaineen tai ydinjätteen kul...
SYT-5330	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Henkilöiden liikkumista ja tavaroiden säilytystä ja niiden siirtoa on valvottava...
SYT-5324	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Ydinlaitoksen hätäpoistumisreitit on toteutettava siten, että henkilöt voivat tu...

SYT-5326	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**24 § Pääsynhallinta**
SYT-5320	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on hallittava, todennettava ja valvottava pääsyä turvallisuuden ka...
SYT-5322	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvattoman tai haitallisen järjestelmän, rakenteen, laitteen tai ohjelmiston käy...

SYT-5305	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on hallittava ja rajattava pääsy- ja käyttöoikeudet pienimpien oik...
SYT-5307	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Henkilöiden tunnistukseen on käytettävä tarkoitukseen soveltuvia pääsynhallintaj...

SYT-5317	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**25 § Avainten ja tunnisteiden hallinta**
SYT-5314	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Avaimia, salausavaimia, tunnisteita ja tunnistetietoja on hallinnoitava turvalli...
SYT-5315	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Avainten, salausavainten ja tunnisteiden hallinnassa on käytettävä ajantasaiseen...

SYT-5312	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**26 § Turvallinen viestintä**
SYT-5313	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on huolehdittava tietoturvallisen viestintäverkon käytettävyydestä...

SYT-5310	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyihin liittyvä viestintä on toteutettava siten, että turvaorganisa...
SYT-5311	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Kuljetuksessa on käytettävä tietoturvallista viestiyhteyttä, joka mahdollistaa n...
SYT-5308	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**27 § Turvajärjestelyjen operatiivisen johtamisen järjestäminen**

SYT-5309	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyjen operatiivista johtamista varten on oltava asianmukaiset tilat...
SYT-5319	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyjen operatiiviseen johtamiseen varatut tilat on suojattava onnett...
SYT-5337	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Ydinlaitoksella on oltava poliisin käyttöön osoitettu ja varustettu tila, josta...

SYT-5338	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Sama henkilö ei saa toimia ydinlaitoksella samanaikaisesti sekä turvajärjestelyj...
SYT-5334	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**28 § Hälytysten käsittely ja hälytyskeskus**
SYT-5336	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvavalvontajärjestelmistä saatavat hälytykset ja turvaorganisaatiolle tulevat...

SYT-5329	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Ydinlaitoksen hälytyskeskuksessa ja varahälytyskeskuksessa on oltava järjestelmä...
SYT-5331	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Hälytyskeskukset on suojattava onnettomuuksien, muiden poikkeamien ja uhkatilant...
SYT-5325	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Hälytyskeskusten sähkönsyöttö on varmennettava. Hälytyskeskusten olosuhteet on t...

SYT-5327	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Hälytyskeskuksessa on oltava vähintään kaksi turvahenkilöä.
SYT-5321	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Varahälytyskeskuksen on oltava eroteltu hälytyskeskuksesta siten, että niitä ei...

SYT-5323	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**29 § Valvomot ja ohjauspaikat**
SYT-5318	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Päävalvomon ja varavalvomon on sijaittava vitaalisella alueella. Päävalvomosta o...
SYT-5316	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Laitosalueen ulkopuolella sijaitsevat ydinlaitoksen ohjaamiseen tai valvontaan k...

SYT-5346	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	Luku 7 Turvajärjestelyjen elinkaaren hallinta
SYT-5348	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	30 § Turvajärjestelyjen ylläpitäminen

SYT-5344	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyistä on huolehdittava ydinlaitoksen ja sen järjestelmien, rakente...
SYT-5345	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvavalvontajärjestelmiä ja rakenteellisia turvajärjestelyjä on koestettava mää...
SYT-5342	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvajärjestelyjen tehokkuus ei saa merkittävästi laskea yksittäisen järjestelmä...

SYT-5343	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on toteutettava korvaavat ja samantasoiset turvajärjestelyt tilant...
SYT-5340	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Kokemuksista oppimista on hyödynnettävä turvajärjestelyjen toteuttamisessa ja ke...
SYT-5341	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on hankittava tietoa käytössä olevien tietojärjestelmien teknisist...

SYT-5356	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**31 § Suunnittelun ja muutosten hallinta**
SYT-5357	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Turvallisuuden kannalta keskeisten järjestelmien, rakenteiden, laitteiden ja ohj...
SYT-5358	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on noudatettava järjestelmällisiä ja jäljitettäviä muutostenhallin...

SYT-5354	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**32 § Tietoturvallisuustestaus**
SYT-5355	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on huolehdittava järjestelmien, laitteiden ja palveluiden tietotur...
SYT-5352	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Tietoturvatestauksen aikana on varmistettava turvajärjestelyjä koskevien vaatimu...

SYT-5353	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**33 § Turvajärjestelyihin liittyvien järjestelmien turvallinen elinkaari**
SYT-5350	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Ydinlaitoksen toimintaan liittyvissä järjestelmissä on noudatettava turvallisen...
SYT-5351	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on laadittava ja otettava käyttöön palveluiden hallintamenettelyt,...

SYT-5347	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**34 § Viranomaisten osallistuminen turvajärjestelyjen suunnitteluun**
SYT-5349	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on varattava poliisille mahdollisuus osallistua uhkatilanteita kos...
SYT-5359	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on määritettävä, luotava ja ylläpidettävä riittävät yhteistyömenet...

SYT-5366	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	Luku 8 Poikkeamat ja uhkatilanteet
SYT-5367	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	35 § Varautuminen poikkeamiin ja uhkatilanteisiin

SYT-5364	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijalla on oltava menettelyt poikkeamien ennalta ehkäisemiseksi ja havai...
SYT-5365	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijalla on oltava menettelyt turvajärjestelyjä koskeviin poikkeamiin ja...
SYT-5362	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**36 § Toiminta poikkeamissa ja uhkatilanteissa**

SYT-5363	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Poikkeamissa ja uhkatilanteissa on viipymättä ryhdyttävä tilanteen vaatimiin toi...
SYT-5360	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on huolehdittava oikea-aikaisesta viranomaisten hälyttämisestä ja...
SYT-5361	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on tuettava poliisia yhteisen tilannekuvan ylläpidossa ja tilantee...

SYT-5372	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**37 § Poikkeamista ja uhkatilanteista ilmoittaminen ja raportointi**
SYT-5373	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Ydinenergialain 374 §:ssä tarkoitettu ydinlaitoksen tapahtumista ilmoittaminen k...
SYT-5374	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on raportoitava turvajärjestelyihin liittyvästä poikkeamasta ja uh...

SYT-5370	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Kyberturvallisuutta koskevien poikkeamien ilmoittamisesta säädetään kyberturvall...
SYT-5371	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**38 § Jatkuvuuden hallinta**
SYT-5368	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijalla on oltava testatut jatkuvuuden hallinnan menettelyt turvajärjest...

SYT-5369	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Järjestelmiä ja varmuuskopioita on hallittava riskiarvion ja jatkuvuusvaatimuste...
SYT-5381	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**Luku 9 Tiedonhallintaa koskevat vaatimukset**

SYT-5383	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**39 § Dokumentointi ja tiedonhallinta**
SYT-5379	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on dokumentoitava turvajärjestelyt, mukaan lukien analyysit, poikk...
SYT-5380	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on suojattava turvajärjestelyjen kannalta keskeiset tiedot ja tall...

SYT-5377	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on määritettävä tiedon luokittelun ja merkitsemisen periaatteet ja...
SYT-5378	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on laadittava henkilöstölle ohjeet, joita henkilöstön tulee noudat...
SYT-5375	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**40 § Viranomaisen turvallisuusluokitellun ja salassa pidettävän tiedon käsittely**

SYT-5376	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Viranomaisen turvallisuusluokitteleman ja muun salassa pidettävän tiedon tietotu...
SYT-5391	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Ennen viranomaisen turvallisuusluokittelemaa tai muuta salassa pidettävää tai nä...
SYT-5392	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**Luku 10 Toiminnan arviointi ja kehittäminen**

SYT-5394	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**41 § Turvajärjestelyjen arviointi**
SYT-5388	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on määritettävä, toteutettava ja valvottava turvajärjestelyjensä p...
SYT-5390	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on arvioitava säännöllisesti turvajärjestelyjen vaatimustenmukaisu...

SYT-5386	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on tehtävä turvajärjestelyiden itsearviointeja. Turvajärjestelyide...
SYT-5387	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**42 § Turvajärjestelyharjoitukset**
SYT-5384	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on toteutettava turvajärjestelyjä koskeva harjoitustoiminta säännö...

SYT-5385	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Harjoitustoiminnan on sisällettävä yhtäaikaisia onnettomuus- ja uhkatilanteita,...
SYT-5382	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Onnettomuus- ja uhkatilanteiden toimivaltaisille viranomaisille on varattava mah...
SYT-5396	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**43 § Turvajärjestelyjen vaikuttavuuden osoittaminen ja kehittäminen**

SYT-5393	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on varmistettava turvajärjestelyjen vaikuttavuus poikkeamia ja uhk...
SYT-5395	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijan on järjestettävä ydinlaitoksessa turvajärjestelyjen koekäyttöjakso...
SYT-5389	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijalla on oltava järjestelmälliset menettelyt rakenteellisten, tekniste...

SYT-5403	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	Luku 11 Turvajärjestelyt kuljetuksissa
SYT-5404	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	44 § Vaatimusten soveltaminen kuljetuksiin

SYT-5401	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Sen lisäksi, mitä tässä 1–10 luvussa määrätään kuljetuksista, sovelletaan kuljet...
SYT-5402	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**45 § Kuljetuksen seuranta ja tarkastus**
SYT-5399	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Vastaanottajan valmiudesta vastaanottaa kuljetus on varmistuttava ennen kuljetuk...

SYT-5400	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Luvanhaltijalla on oltava tieto sen lukuun tehtävän kuljetuksen lähdöstä ja saap...
SYT-5397	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Kuljetusta varten on oltava yhteyskeskus kuljetuksen seuraamista, yhteydenpitoa,...
SYT-5398	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Kuljetusvälineiden turvallisuustarkastus sekä ydinaineen tai ydinjätteen lastaus...

SYT-5412	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**46 § Kuljetukseen liittyvät poikkeamat ja uhkatilanteet**
SYT-5413	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Hyväksytyistä suunnitelmista saa kuljetuksen aikana poiketa vain odottamattomist...
SYT-5414	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Mikäli olosuhteet edellyttävät, on arvioitava tarve kuljetuksen ajankohdan siirt...

SYT-5410	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**47 § Suojaluokan II ja I ydinaineita koskevat lisävaatimukset**
SYT-5411	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Kuljetusvälineen luvaton käyttö kuljetuksen aikana on estettävä teknisesti ajone...
SYT-5408	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Käytetyn ydinpolttoaineen ja muun suojaluokan II ydinaineen maantie-, rautatie- ...

SYT-5409	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Requirement	Ydinenergialain 184 §:n 2 momentissa tarkoitettujen ydinaseiden leviämisen estäm...
SYT-5406	**Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt**	**Heading**	**Luku 12 Voimaantulo- ja siirtymäsäännökset**

SYT-5407	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	48 § Voimaantulo
SYT-5405	Määräysluonnokset / Ydinlaitoksen ja kuljetusten turvajärjestelyt	Heading	49 § Siirtymäsäännökset

Description

Tätä määräystä sovelletaan ydinvoimalaitoksiin, käytetyn ydinpolttoaineen ja muun korkea-aktiivisen ydinjätteen käsittelyyn, varastointiin ja loppusijoittamiseen tarkoitettuihin laitoksiin.

Tätä määräystä sellaisenaan sovelletaan myös sellaisiin ydinlaitoksiin, jotka sijaitsevat 1 momentissa tarkoitettujen ydinlaitosten kanssa samalla liikkumis- ja oleskelurajoitusalueella.

Muihin kuin 1 ja 2 momentissa tarkoitettuihin ydinlaitoksiin ei sovelleta, mitä tämän määräyksen 14 §:ssä, 18 §:ssä, 22 §:n 3 momentissa, 23 §:n 2 momentissa ja 28 §:n 5 momentissa määrätään.

Turvajärjestelyihin kuuluvat fyysiset turvajärjestelyt ja tietoturvallisuus.

1) *uhkatilanteella* tilannetta, jossa havaitaan tai on syytä epäillä turvallisuutta vaarantavaa toimintaa;

2) *poikkeamalla* normaalitilasta poikkeavaa tilannetta, jossa tapahtuu onnettomuus, turvajärjestelyjen heikentyminen, häiriötilanne tai läheltä piti -tilanne;

3) *vaarallisella esineellä* esinettä, esineen jäljitelmää ja ainetta, jolla voidaan vaarantaa ydinlaitoksen, kuljetuksen tai henkilöiden turvallisuutta;
4) *yhteisvialla* ydinlaitoksen kahden tai useamman järjestelmän, rakenteen tai laitteen yhtäaikaisesti tai lyhyessä ajassa tapahtuvaa vikaantumista yksittäisen tapahtuman tai syyn seurauksena;
5) *turvallisuuslohkolla* sellaisia fyysisesti toisistaan eroteltuja tiloja ja niiden sisältämiä rakenteita ja laitteita, joihin sijoitetaan kunkin turvallisuusjärjestelmän yksi moninkertaisuusperiaatetta toteuttava osa;

6) *turvallisuuden kannalta keskeisellä järjestelmällä, rakenteella tai laitteella* sellaista järjestelmää, rakennetta tai laitetta, joka turvallisuuden näkökulmasta riskitietoisesti arvioituna on merkittävä ko. järjestelmää, rakennetta tai laitetta koskevasta turvallisuusluokasta riippumatta;
7) *vasteella* turvallisuutta vaarantavan toiminnan pysäyttämistä, tilanteen hallintaan saattamista, seurausten estämistä ja rajoittamista;
8) *hälytyskeskuksella* toimintoa ja tilaa, jossa seurataan turvavalvontajärjestelmiä ja arvioidaan tarvittava vaste. Se toimii myös ensimmäisenä yhteyspisteenä, kun onnettomuuksia, väärinkäytöksiä, lainvastaista toimintaa tai muita uhkia ilmenee;

9) *valvomolla tai ohjauspaikalla* toimintoa ja tilaa, jossa seurataan ja ohjataan ydinlaitoksen käyttöön ja turvallisuuteen liittyviä prosesseja ja järjestelmiä.

Turvajärjestelyjen perusperiaatteista ja vaatimuksista määrätään ydinaineita ja ydinlaitoksia koskevista turvajärjestelyistä tehdyssä yleissopimuksessa (SopS 72/1989) ja sen muutoksessa (SopS 19-20/2016).

Turvajärjestelyt on suunniteltava ja toteutettava syvyyssuuntaisen puolustuksen periaatteen mukaisesti.

Turvajärjestelyihin liittyvät järjestelmät, rakenteet, laitteet ja ohjelmistot sekä tekniset ratkaisut on suunniteltava ja toteutettava siten, että ne ohjaavat toimimaan turvallisesti sekä ehkäisevät turvallisuutta heikentävää toimintaa.
Ydinlaitos ja kuljetukset, sekä niiden toiminnot, järjestelmät, rakenteet, laitteet ja ohjelmistot on suunniteltava ja toteutettava siten, että turvajärjestelyt voidaan toimeenpanna tarkoituksenmukaisesti.

Turvajärjestelyt on suunniteltava ja toteutettava riskitietoisesti. Luvanhaltijan turvajärjestelyjen riskienhallintaprosessin on katettava lainvastaiseen ja muuhun laitoksen turvallisuutta vaarantavaan toimintaan liittyvät riskit, mukaan lukien kuljetuksiin liittyvät riskit.

Sen lisäksi, mitä kyberturvallisuuslain (124/2025) 7 §:ssä säädetään kyberturvallisuuden riskienhallinnasta, ydinlaitoksen kyberturvallisuutta koskevalla riskienhallinnalla on pyrittävä estämään tai minimoimaan poikkeamien vaikutus ydinlaitoksen ja kuljetusten turvallisuuteen.

Ydinlaitoksen riskienhallinnassa on otettava huomioon kansainväliseen ydinmateriaalivalvontaan kuuluvan laitteiston ja tiedonsiirron osalta laitokseen kohdistuva riski.

Turvajärjestelyt on suunniteltava ja toteutettava suunnitteluperusteuhkan mukaisesti. Sen perusteella on varauduttava lainvastaista tai muuta turvallisuutta vaarantavaa toimintaa vastaan. Varautumisessa on otettava huomioon:

1) vakoilu;

2) ampuma-aseiden, räjähteiden, kemiallisten ja biologisten aineiden ja muiden vaarallisten esineiden käyttö;

3) sähkömagneettinen häirintä;

4) kulkuneuvon törmäys;

5) tietoturvallisuusuhat;

6) muut suunnitteluperusteuhan sisältämät uhat.

Toteutuksessa on otettava huomioon erilaiset tavat 1 momentissa tarkoitetun toiminnan toteuttamiseksi, välineiden käyttämiseksi tai toimittamiseksi kohteeseen, fyysinen tai tietoturvahyökkäys, ulkopuolinen ja insider -uhka sekä näiden yhdistelmät.
Tilaturvallisuudessa on suojauduttava fyysisiä uhkia, vakoilua ja vaikuttamista vastaan suunnitteluperusteuhan mukaisesti.

Luvanhaltijan on suunniteltava ja toteutettava turvajärjestelyt siten, että turvallisuutta vaarantavan toiminnan torjuntaa varten on olemassa toisistaan riippumattomia turvallisuuden hallintakeinoja.
Turvajärjestelyjen ennaltaehkäisevät toimet, havaitseminen, viivytys ja vaste sekä palautuminen on toteutettava kokonaisuutena, jossa otetaan huomioon näiden osa-alueiden väliset riippuvuudet.
Turvajärjestelyihin liittyvät järjestelmät on pääsääntöisesti suunniteltava ja toteutettava siten, että turvallisuuden ja uhkien hallinta ei ole yksinomaan ohjelmistopohjaisten järjestelmien varassa.

Turvallisuuden kannalta keskeisten tietojärjestelmien tietoliikenne on puhelinjärjestelmiä lukuun ottamatta suunniteltava ja toteutettava siten, ettei se ole yksinomaan langattomien yhteyksien varassa.

Luvanhaltijan on arvioitava järjestelmien, rakenteiden, laitteiden, ohjelmistojen, ydinaineiden, ydinjätteiden sekä luvanhaltijan toimintaan liittyvien tietojen turvallisuusmerkitys ja niiden riskit turvajärjestelyjen kannalta. Arvioinnissa on otettava huomioon lainvastaisen tai muun turvallisuutta vaarantavan toiminnan mahdollisuus. Turvajärjestelyt ja muut järjestelyt on toteutettava arviointia vastaavasti.
Luvanhaltijan on ylläpidettävä ajantasaista tietoa turvajärjestelyihin liittyvistä järjestelmistä, rakenteista, laitteista, ohjelmistoista ja tiedoista sekä niiden versioista, asetuksista, rajapinnoista ja sijaintipaikoista turvajärjestelyjen toteuttamiseksi ja niiden turvallisen elinkaaren varmistamiseksi. Muutokset on tehtävä hallitusti ja ne on oltava jäljitettävissä.

Luvanhaltijan on varmistettava, että ydinlaitoksen toiminnassa ja kuljetuksissa käytetään turvajärjestelyihin vain järjestelmiä, rakenteita, laitteita ja ohjelmistoja, jotka luvanhaltija on hyväksynyt käyttöön.

Turvajärjestelyjen hallintajärjestelmän on sisällyttävä luvanhaltijan johtamisjärjestelmään.

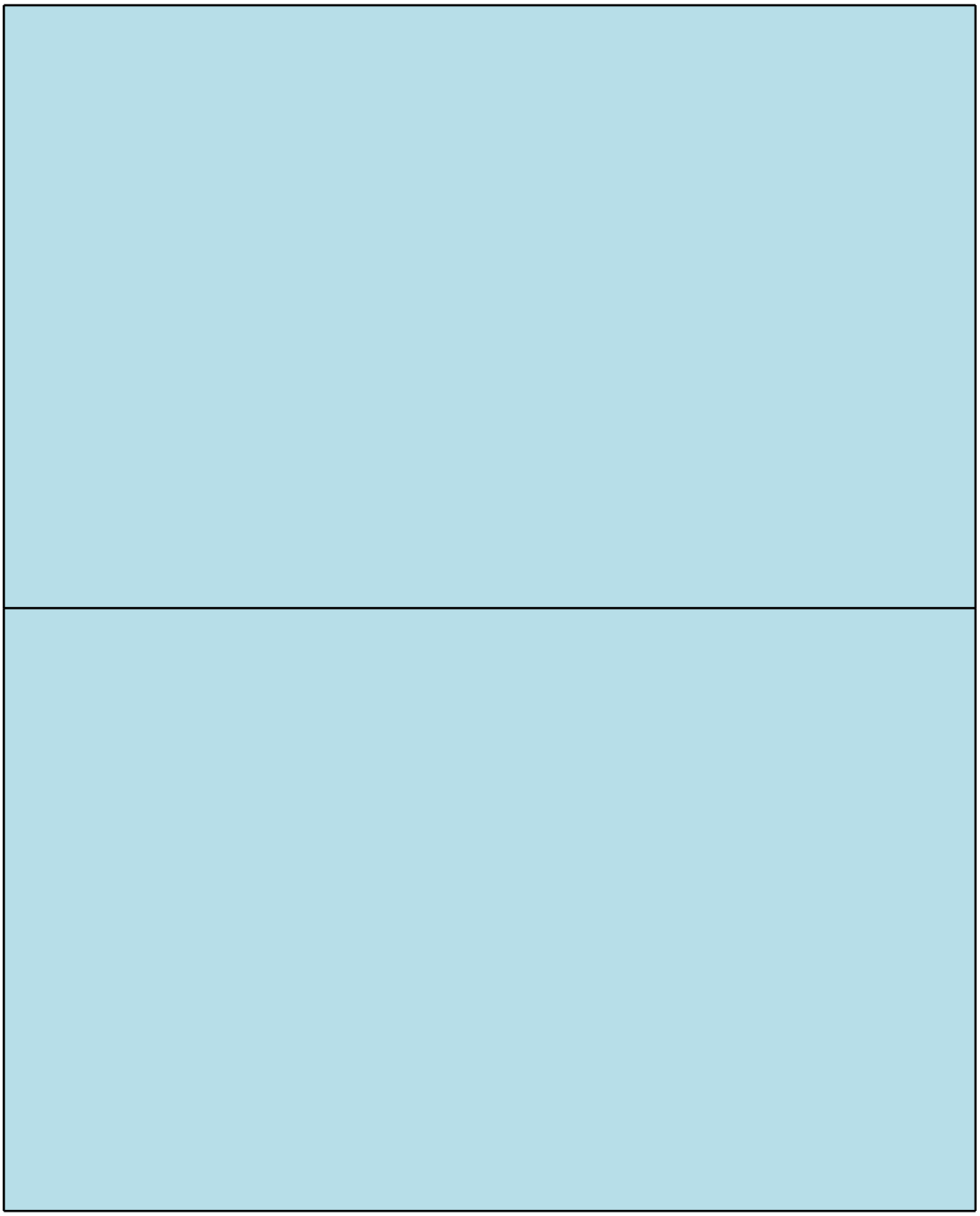
Tietoturvallisuuden hallintajärjestelmän on toteutettava standardia ISO/IEC 27001 vastaava turvallisuustaso ydinlaitoksen turvallisuuden kannalta asianmukaisella tavalla.

Turvajärjestelynäkökohdat on otettava huomioon luvanhaltijan toimintakulttuurissa ja sen arvioinnissa.

Turvajärjestelynäkökohdat on otettava huomioon turvallisuuteen liittyvien inhimillisten tekijöiden hallinnassa.

Luvanhaltijalla on oltava järjestelmälliset ja monialaiset menettelyt, joilla hallitaan uhkaa, joka liittyy henkilöihin, joilla on luvallinen pääsy ydinlaitokseen tai kuljetukseen taikka niiden järjestelmiin, rakenteisiin, laitteisiin tai niitä koskeviin tietoihin (insider-uhka). Menettelyjen on katettava myös toimitusketjut riskitietoisesti.
Luvanhaltijan on tunnistettava tehtävät, joissa yhdelle henkilölle voi syntyä mahdollisuus tehdä vahinkoa tai mahdollisuus turvallisuutta vaarantaviin väärinkäytöksiin. Tällaiset tehtävät on erotettava toisistaan tai ehkäistävä väärinkäyttöä muilla keinoin.

Ydinlaitosta ja sen kuljetuksia sekä muuta toimintaa koskevassa päätöksenteossa on varmistettava fyysisten turvajärjestelyjen ja tietoturvallisuuden huomioiminen.

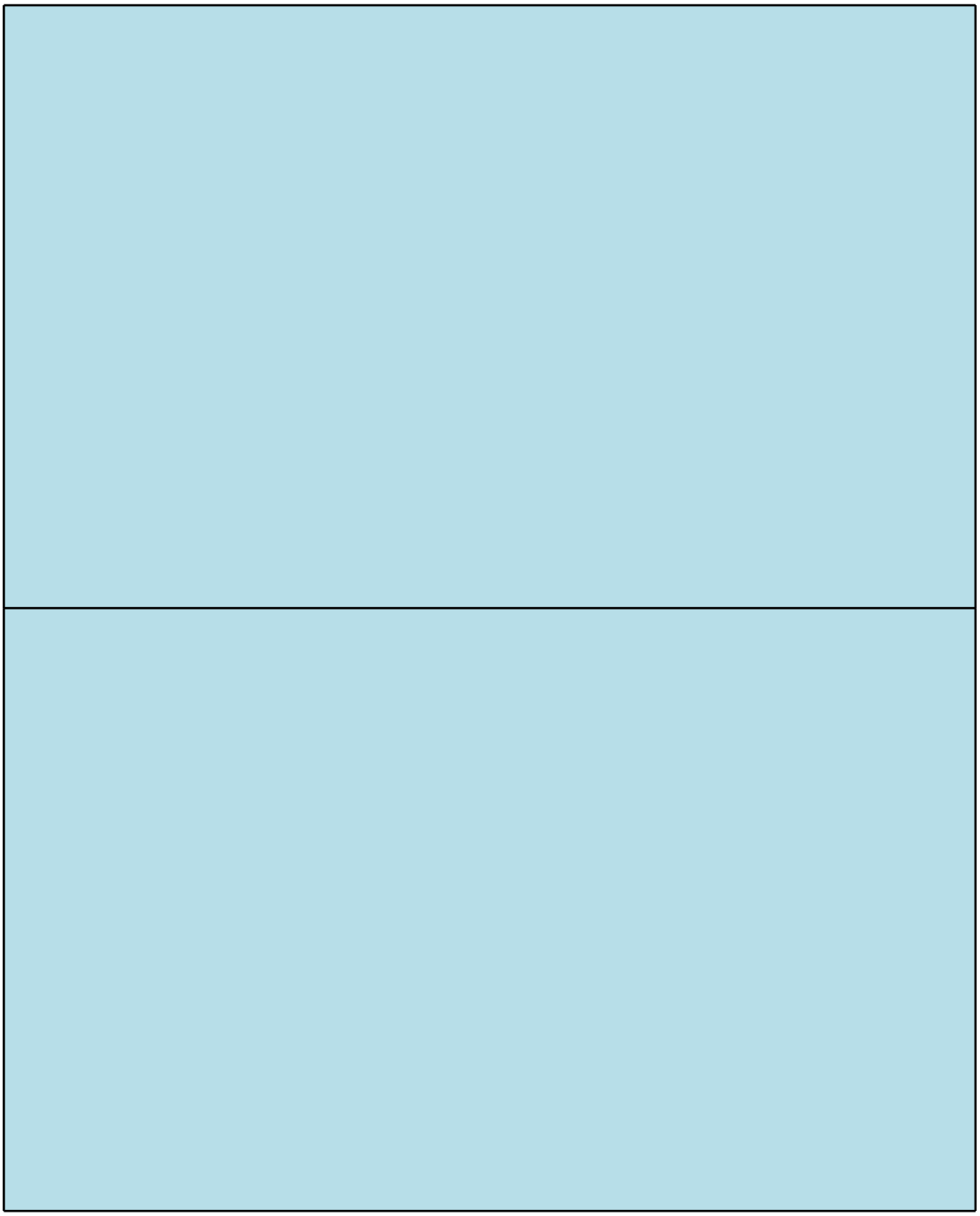


Luvanhaltijan on määriteltävä turvajärjestelyihin liittyvät tehtävät sekä tehtäviin liittyvät vastuut ja valtuudet. Tehtävät on kuvattava ja tehtävänkuvaukset on saatettava tietoon tehtävissä toimiville henkilöille.
Turvajärjestelyjen henkilöstömitoituksen on perustuttava suunnitteluperusteuhkaan ja ajantasaisen tilannekuvan perusteella arvioituihin suojaustarpeisiin.
Keskeisten turvajärjestelyihin liittyvien henkilöiden ja muiden resurssien on oltava luvanhaltijan palveluksessa tai operatiivisessa hallinnassa.

Turvaorganisaation osaamisen kehittämiseen ja koulutukseen on oltava käytettävissä turvajärjestelyjen tarkoituksenmukaisen toteuttamisen kannalta asianmukaiset resurssit ja harjoitteluolosuhteet, mukaan lukien voimankäytön koulutukseen ja harjoitteluun tarvittavat tilat, alueet ja välineet.

Luvanhaltijan on huolehdittava siitä, että koko ydinlaitoksessa ja kuljetuksissa työskentelevälle henkilöstölle järjestetään turvajärjestelyjä koskevaa koulutusta ja henkilöstön osaamista ylläpidetään. Turvajärjestelyihin liittyvien koulutuksien sisältö on oltava ajan tasalla ja niiden suorittamista ja koulutuksen vaikuttavuutta on seurattava ja tulokset dokumentoitava.

Sen lisäksi, mitä ydinenergialain 156 §:ssä säädetään turvahenkilön asusta, on turvahenkilön asussa olevien merkkien ja tekstien oltava tämän määräyksen liitteen 1 mukaisia.



Ydinlaitokselle on määriteltävä sisäkkäiset turvajärjestelyvyöhykkeet. Vyöhykkeiden määrittämisen perusteena on niiden merkitys turvajärjestelyjen syvyyssuuntaisen puolustuksen tarkoituksenmukaiselle toteuttamiselle. Toteuttamisessa on huomioitava uhkan ennalta ehkäisy, havaitseminen, viivytys ja vaste. Vyöhykkeiden ja niiden rajapintojen on muodostettava turvajärjestelyjen toteuttamisen kannalta tarkoituksenmukainen kokonaisuus, jossa huomioidaan niiden rakenteellinen kestävyys, viivytyskapasiteetti ja havaitsemisen toteuttaminen.

Ydinlaitoksen turvajärjestelyvyöhykkeitä ovat

1) liikkumis- ja oleskelurajoituksista annetun sisäministeriön asetuksen (1104/2013) liitteessä 4 määritelty liikkumis- ja oleskelurajoitusalue;

2) ydinenergialain 5 §:ssä tarkoitettu laitosalue;

3) suojattu alue, jolla tarkoitetaan laitosrakennusten ulkoseinällä rajattua aluetta tai muuta turvallisuusmerkitykseltään vastaavaa aluetta; ja

4) vitaalinen alue, jolla tarkoitetaan turvallisuuden kannalta erityisen merkittävää aluetta.

Luvanhaltijan on suojattava tietoverkot jakamalla ne tietoturvavyöhykkeisiin niihin liittyvän riskiarvion perusteella, joko eriyttämällä loogisesti tai eristämällä fyysisesti. Järjestelmä-, laite- ja ohjelmistokohtaiset turvallisuuden hallintakeinot on toteutettava turvallisuusmerkityksen mukaisesti tietoturvavyöhykkeistä riippumatta.

Tietojärjestelmien riskimerkityksen perusteella on toteutettava tietoliikenteen ulkopuolisten yhteyksien rajoittaminen tai fyysinen yksisuuntaistaminen tai molempia rajoitustapoja.

Sen lisäksi, mitä liikkumis- ja oleskelurajoituksista annetun sisäministeriön asetuksen 4 ja 5 §:ssä säädetään, ydinlaitoksen alue on merkittävä tämän määräyksen liitteen 2 mukaisesti.

Laitosalue on rajattava kaksoisesteellä ja sen väliin jäävällä eristysvyöhykkeellä. Kaksoiseste ja eristysvyöhyke sekä välittömästi niiden molemmin puolin oleva alue on varustettava valaistuksella ja toisistaan riippumattomilla valvontajärjestelmillä siten, että tunkeutuminen voidaan havaita ja valvontajärjestelmien tuottamat hälytykset arvioida. Kaksoiseste on lisäksi varustettava ajoneuvoesteellä.

Laitosalueelle johtavien kulkuaukkojen lukumäärä on pidettävä niin pienenä kuin käytännössä on mahdollista. Laitosalueelle ja sieltä pois tapahtuva liikenne on keskitettävä ensisijaisesti yhteen kohtaan. Sisään ja ulos menevän liikenteen kulku on toteutettava yksitellen.

Suojatut ja vitaaliset alueet on määriteltävä riskitietoisesti laitoksen ominaisuuksien ja toiminnan perusteella. Luvanhaltijan on toimitettava vitaalisen alueen määrittelyn menettely Säteilyturvakeskukselle osana turvasuunnitelmaa.

Liikkuminen ja oleskelu vitaalisella alueella on rajoitettava turvallisuuden kannalta tarpeellisiin tehtäviin. Tämä on otettava huomioon järjestelmien ja laitteiden suunnittelussa ja sijoittelussa.

Turvajärjestelyvyöhykkeillä on tehtävä valvontaa teknisin menetelmin ja partioimalla.

Turvajärjestelyvyöhykkeillä on oltava jatkuvatoimisia turvavalvontajärjestelmiä, joiden on kokonaisuutena:

1) mahdollistettava turvajärjestelyjen valvonta ja väärinkäytön havaitseminen;

2) mahdollistettava luvattoman tunkeutumisen luotettava ja oikea-aikainen havaitseminen ja paikantaminen;

3) mahdollistettava hälytysten oikea-aikainen arviointi ja tarvittaessa hälytysten priorisointi;

4) ilmoitettava häiriöstä tai yrityksestä vahingoittaa järjestelmän laitetta tai sen toimintaa;

5) ilmoitettava selkeästi hälytyskeskukseen ääni- ja optisin signaalein yrityksestä läpäistä esteet;

6) mahdollistettava tallentavilla valvontajärjestelmillä laitosalueen tarkkailu siten, että turvajärjestelyvyöhykkeillä olevia henkilöitä ja muita kohteita voidaan valvoa oikea-aikaisesti ja luotettavasti;

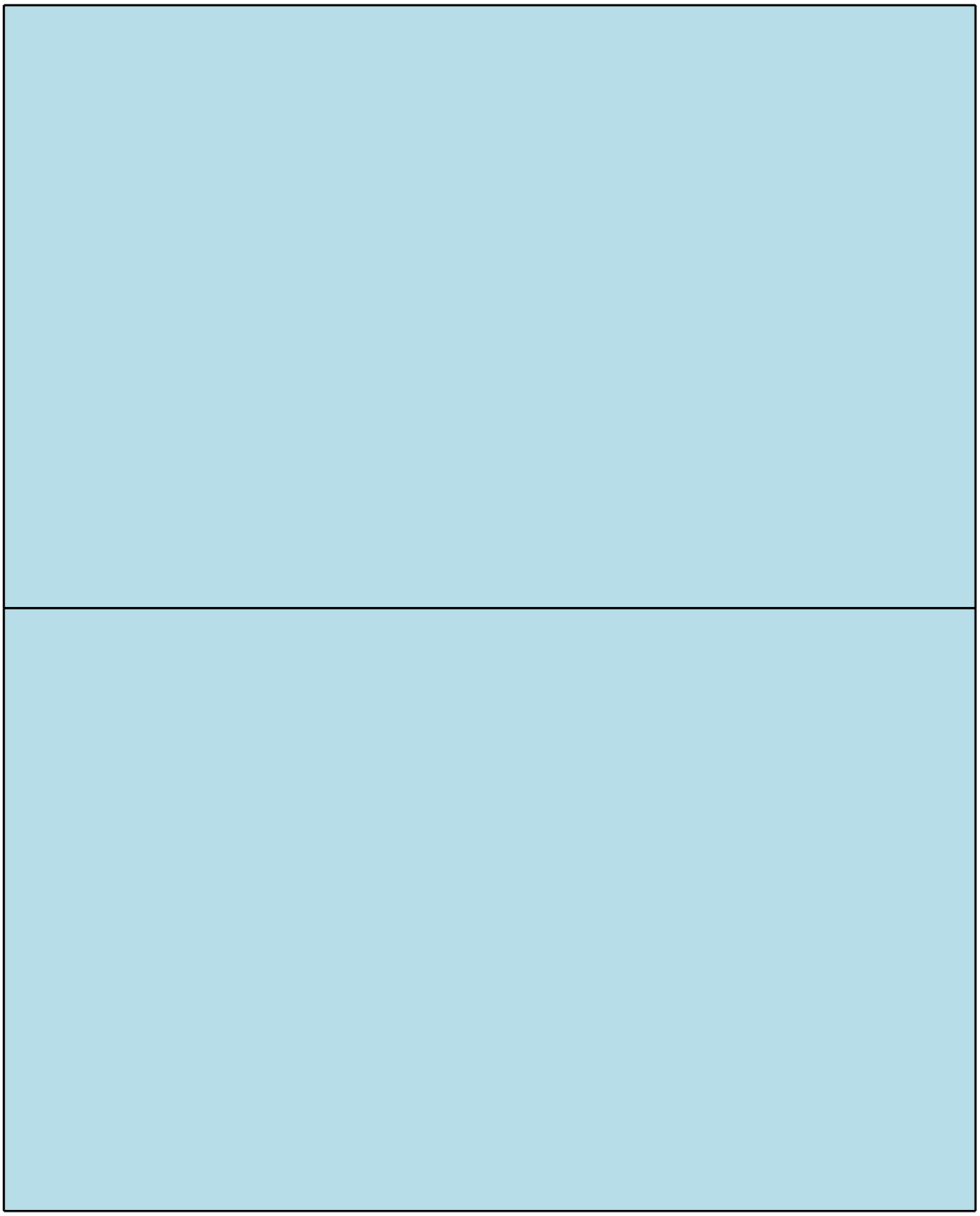
7) rekisteröitävä kulkutapahtumat;

8) tallennettava tapahtumat niiden selvittämisen ja tutkinnan edellytysten turvaamiseksi.

Laitosalueella turvavalvontajärjestelmien on oltava mahdollisimman katveettomia.

Tietoverkkojen ja -järjestelmien normaalitila on määritettävä ja niitä on valvottava poikkeamien havaitsemiseksi. Niistä on kerättävä tietoa kattavasti siten, että poikkeamat voidaan havaita sekä tutkia mahdollisimman kiistattomasti.

Luvanhaltijalla on oltava menettelyt tietojen eheyden ja saatavuuden varmistamiseksi sekä tietojen luvattoman käsittelyn ehkäisemiseksi.



Luvanhaltijan on varmistettava rakenteellisin ja teknisin järjestelyin riittävä viivytys ydinlaitoksen turvallisuutta vaarantavaa toimintaa vastaan, jotta vaste voidaan tehokkaasti toteuttaa.

Turvajärjestelyjen kannalta merkitykselliset järjestelmät on erotettava ja suojattava rakenteellisesti ja teknisesti.

Henkilöitä, ajoneuvoja ja tavaraliikennettä on valvottava ydinlaitokselle sisään ja sieltä ulos mentäessä.
Vaarallisten esineiden ja haitallisten laitteiden pääsy ydinlaitokseen ja kuljetukseen on estettävä. Ydinaineiden, ydinjätteiden ja muiden radioaktiivisten aineiden luvaton vieminen ydinlaitokselle tai ydinlaitokselta on estettävä.
Ajoneuvojen turvallisuustarkastus on suoritettava sitä varten erikseen rajatulla alueella siten, että tarkastamattomia ajoneuvoja tai henkilöitä ei pääse laitosalueelle.

Pääsyoikeudettomien henkilöiden pääsy ydinlaitokseen ja kuljetukseen on estettävä. Ydinlaitoksessa ja sen alueella asioivien sekä ydinaineen tai ydinjätteen kuljetukseen osallistuvien henkilöllisyydestä on varmistuttava.

Luvanhaltijan on järjestettävä henkilöiden kulku laitosalueelle ja sieltä pois siten, että

1) laitosalueelle ja laitosalueelta kuljetaan yksitellen;

2) henkilöt ja henkilöiden mukana olevat tavarat turvallisuustarkastetaan sisään päin mentäessä;

3) turvallisuustarkastus tehdään ennen laitosalueelle pääsyä;

4) turvallisuustarkastetut henkilöt eivät laitokselle mentäessä kohtaa sellaisia henkilöitä, joille ei ole tehty turvallisuustarkastusta;

5) ulos mentäessä henkilöt ja tavarat tarkastetaan radioaktiivisen aineen poisviennin varalta. Muita turvallisuustarkastuksia voidaan tehdä myös satunnaisotannalla;6) turvallisuustarkastusta ei edellytetä uhka- ja hätätilanteissa turvahenkilöiltä tai poliisilta tai pelastusviranomaisilta.

Liikkuminen ydinlaitoksessa ja sen alueella, sekä ydinaineen tai ydinjätteen kuljetuksen välittömässä läheisyydessä on oltava asioinnin tarkoituksen mukaan rajoitettua ja valvottua.

Henkilöiden liikkumista ja tavaroiden säilytystä ja niiden siirtoa on valvottava laitosalueella. Muiden kuin itsenäiseen liikkumiseen hyväksyttyjen henkilöiden on liikuttava laitosalueella saatettuina.

Ydinlaitoksen hätäpoistumisreitit on toteutettava siten, että henkilöt voivat turvallisesti poistua vaara-alueelta, mutta kuitenkin siten, että niitä ei voida käyttää tunkeutumisreitteinä. Hätäpoistumisreittien suunnittelussa on otettava huomioon uhka- ja onnettomuustilanteet, eivätkä reitit saa johtaa turvallisuuslohkosta toiseen.

Luvanhaltijan on hallittava, todennettava ja valvottava pääsyä turvallisuuden kannalta keskeisiin pääsynhallintaa edellyttäviin kohteisiin ja tietoihin. Pääsynhallinta on suunniteltava ja toteutettava kohteen turvallisuusmerkityksen perusteella. Pääsynhallinnan vaatimus koskee henkilöitä ja ohjelmistoja.

Luvattoman tai haitallisen järjestelmän, rakenteen, laitteen tai ohjelmiston käyttö ydinlaitoksen toiminnassa tai kuljetuksessa on estettävä.

Luvanhaltijan on hallittava ja rajattava pääsy- ja käyttöoikeudet pienimpien oikeuksien periaatteiden mukaisesti työtehtävien perusteella. Henkilökohtaisilla käyttäjätunnuksilla ja mahdollisilla yhteiskäyttötunnuksilla ja niihin liittyvillä salasanoilla on oltava omistaja ja hallintamenettelyt. Pääsy- ja käyttöoikeuksien hallintamenettelyiden toteutumista on valvottava ja ne on pidettävä ajantasaisina. Käyttöoikeudet on katselmoitava säännöllisesti ja työtehtävien muutosten yhteydessä.
Henkilöiden tunnistukseen on käytettävä tarkoitukseen soveltuvia pääsynhallintajärjestelmiä yhdessä luotettavan tunnistusteknologian kanssa. Järjestelmän ja teknologian on varmistettava, ettei turvajärjestelyvyöhykkeiden rajapintojen kulkuaukoista voi kulkea samalla kulkutunnisteella peräkkäin useampi kuin yksi henkilö.

Avaimia, salausavaimia, tunnisteita ja tunnistetietoja on hallinnoitava turvallisesti ja riittävän reaaliaikaisesti.

Avainten, salausavainten ja tunnisteiden hallinnassa on käytettävä ajantasaiseen teknologiaan perustuvia menettelyjä, joilla minimoidaan tunnisteiden ja avainten väärinkäytön mahdollisuus.

Luvanhaltijan on huolehdittava tietoturvallisen viestintäverkon käytettävyydestä ydinlaitoksessa.

Turvajärjestelyihin liittyvä viestintä on toteutettava siten, että turvaorganisaatio voi kommunikoida sisäisesti ja viranomaisen kanssa tietoturvallisesti. Viestintäjärjestelyille on oltava varajärjestelmä.

Kuljetuksessa on käytettävä tietoturvallista viestiyhteyttä, joka mahdollistaa nopean ja tehokkaan viestinnän ja kuljetuksen seurannan. Viestijärjestelmälle on oltava varajärjestelmä.

Turvajärjestelyjen operatiivista johtamista varten on oltava asianmukaiset tilat, välineet, viestintäyhteydet ja henkilöt. Näille on lisäksi oltava varajärjestelyt. Varajärjestelyt on oltava eroteltu varsinaisista järjestelyistä siten, että niitä ei menetetä samasta ulkoisesta tai sisäisestä syystä samanaikaisesti.
Turvajärjestelyjen operatiiviseen johtamiseen varatut tilat on suojattava onnettomuuksien, muiden poikkeamien ja uhkatilanteiden varalta. Tiloissa työskentelyn on oltava mahdollista ilman suojavarusteita erilaisten tilanteiden aikana. Tilojen sähkönsyöttö on varmennettava.
Ydinlaitoksella on oltava poliisin käyttöön osoitettu ja varustettu tila, josta poliisi voi johtaa toimintaa ydinlaitokseen kohdistuvan uhkatilanteen torjumiseksi.

Sama henkilö ei saa toimia ydinlaitoksella samanaikaisesti sekä turvajärjestelyjen operatiivisesta johtamisesta että hälytysten käsittelystä ja arvioinnista vastaavana henkilönä.

Turvavalvontajärjestelmistä saatavat hälytykset ja turvaorganisaatiolle tulevat ilmoitukset on käsiteltävä ja arvioitava oikea-aikaisesti ja luotettavasti tilannekuvan muodostamiseksi ja ylläpitämiseksi.

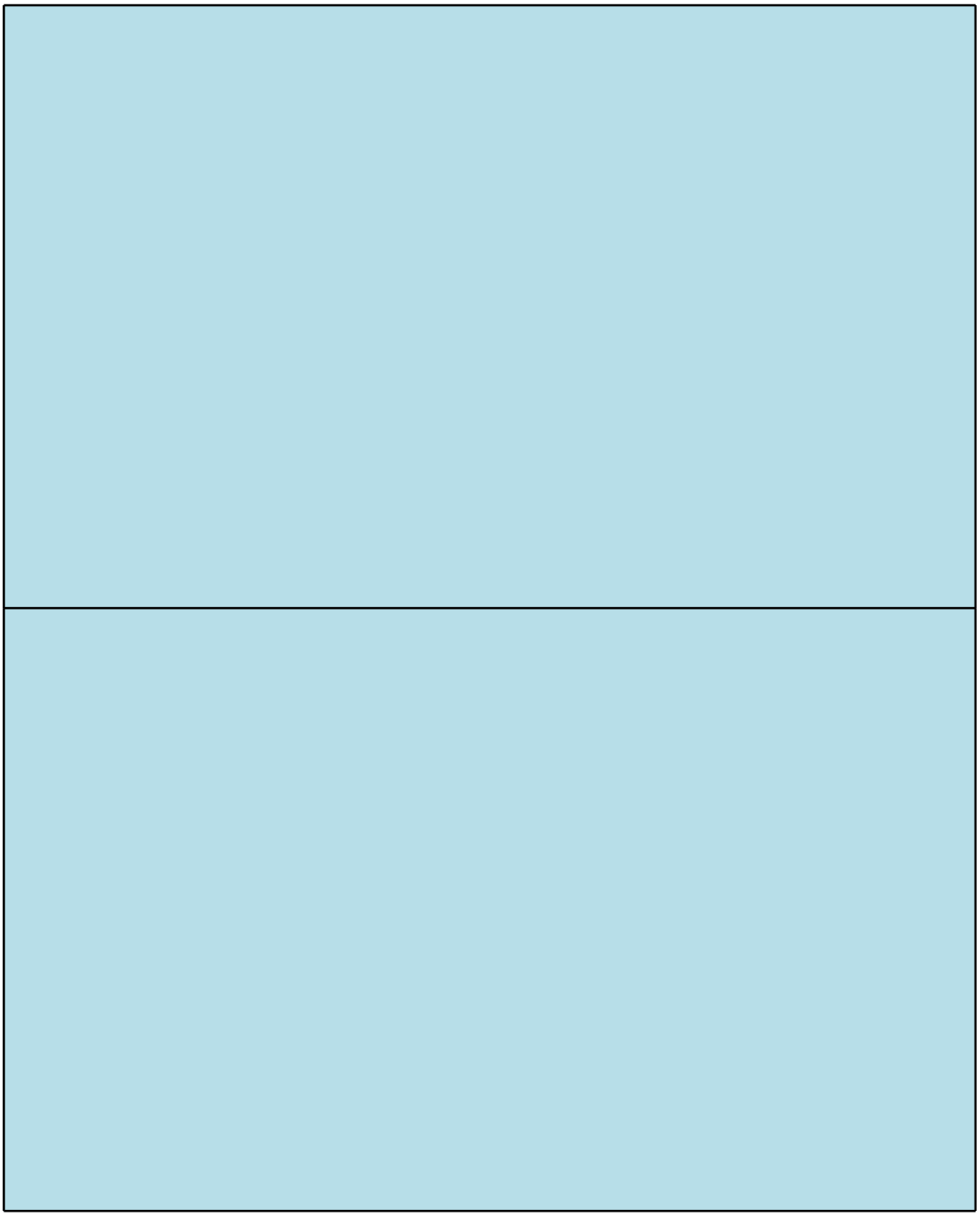
Ydinlaitoksen hälytyskeskuksessa ja varahälytyskeskuksessa on oltava järjestelmät hälytysten käsittelyä ja arviointia varten sekä varmennetut, tietoturvalliset yhteydet poliisiin, ydinlaitoksen turvajärjestelyjen operatiiviseen johtamiseen tarkoitettuihin tiloihin ja ydinlaitoksen valvomoon.
Hälytyskeskukset on suojattava onnettomuuksien, muiden poikkeamien ja uhkatilanteiden varalta. Tiloissa työskentelyn on oltava mahdollista ilman suojavarusteita erilaisten tilanteiden aikana. Hälytyskeskuksen on sijaittava suojatulla alueella tai muussa vastaavalla tavalla suojatussa paikassa laitosalueella. Varahälytyskeskus voi sijaita muualla, jos sen osoitetaan olevan turvallista.
Hälytyskeskusten sähkönsyöttö on varmennettava. Hälytyskeskusten olosuhteet on toteutettava siten, että se mahdollistaa turvajärjestelyiden tehokkaan toteutumisen.

Hälytyskeskuksessa on oltava vähintään kaksi turvahenkilöä.

Varahälytyskeskuksen on oltava eroteltu hälytyskeskuksesta siten, että niitä ei menetetä samasta ulkoisesta tai sisäisestä syystä samanaikaisesti. Hälytyskeskuksesta on tarvittaessa voitava siirtyä varahälytyskeskukseen turvallisesti.

Päävalvomon ja varavalvomon on sijaittava vitaalisella alueella. Päävalvomosta on voitava siirtyä varavalvomoon turvallisesti.

Laitosalueen ulkopuolella sijaitsevat ydinlaitoksen ohjaamiseen tai valvontaan käytettävät tilat on suojattava rakenteellisesti ja teknisesti. Näiden tilojen tietoliikenneyhteydet on suojattava ja kahdennettava. (Lisätään myöhemmin viittaus toiseen määräykseen).



Turvajärjestelyistä on huolehdittava ydinlaitoksen ja sen järjestelmien, rakenteiden, laitteiden ja ohjelmistojen sekä niitä koskevan tiedon koko elinkaaren ajan esisuunnitteluvaiheesta käytöstä poistoon ja tiedon tuhoamiseen.

Turvavalvontajärjestelmiä ja rakenteellisia turvajärjestelyjä on koestettava määräajoin niiden käyttökuntoisuuden ja toiminnan varmistamiseksi. Turvavalvontajärjestelmien ja rakenteellisten turvajärjestelyiden huoltaminen on toteutettava suunnitelmallisesti toimintakuntoisuuden varmistamiseksi (ennakkohuolto-ohjelma) ja tarvittavien varaosien saatavuus on varmistettava.

Turvajärjestelyjen tehokkuus ei saa merkittävästi laskea yksittäisen järjestelmän, rakenteen, laitteen tai ohjelmiston vikaantumisen tai häiriön takia. Turvajärjestelyistä on kyettävä huolehtimaan ydinlaitoksen mahdollisten yhteisvikojen, sähkön menetyksen ja muiden laajuudeltaan vastaavien tapahtumien sattuessa.

Luvanhaltijan on toteutettava korvaavat ja samantasoiset turvajärjestelyt tilanteissa, joissa turvajärjestelyjä koskevista ensisijaisista menettelyistä joudutaan poikkeamaan.
Kokemuksista oppimista on hyödynnettävä turvajärjestelyjen toteuttamisessa ja kehittämisessä.
Luvanhaltijan on hankittava tietoa käytössä olevien tietojärjestelmien teknisistä haavoittuvuuksista ja hallittava niihin liittyviä riskejä ajantasaisesti.

Turvallisuuden kannalta keskeisten järjestelmien, rakenteiden, laitteiden ja ohjelmistojen päivitettävyys on otettava huomioon niiden suunnittelussa.

Luvanhaltijan on noudatettava järjestelmällisiä ja jäljitettäviä muutostenhallinnan menettelyjä turvajärjestelyjen kannalta merkittävien järjestelmien, rakenteiden, laitteiden ja ohjelmistojen muutoksissa. Ydinlaitosten suunnittelu- ja muutostöissä on kiinnitettävä huomiota turvallisuuden osa-alueiden rajapintojen hallintaan.

Luvanhaltijan on huolehdittava järjestelmien, laitteiden ja palveluiden tietoturvallisuuden testauksesta riskitietoisesti suunnittelun, käyttöönoton ja muutosten yhteydessä.

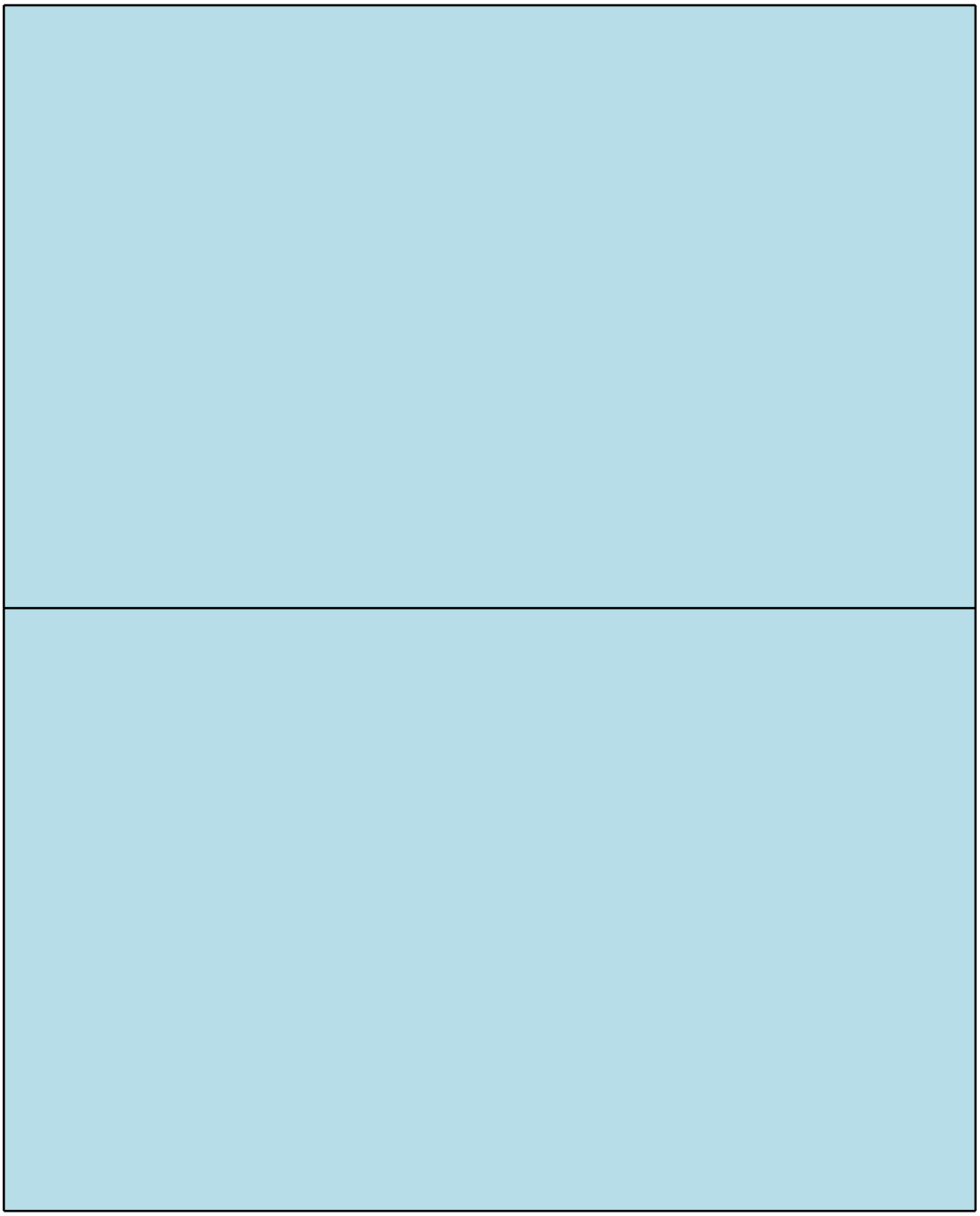
Tietoturvatestauksen aikana on varmistettava turvajärjestelyjä koskevien vaatimusten toteutuminen, mukaan lukien tiedon saatavuus, eheys ja luottamuksellisuus.

Ydinlaitoksen toimintaan liittyvissä järjestelmissä on noudatettava turvallisen elinkaaren hallinnan menettelyjä, jotka sisältävät asianmukaiset suunnittelun, toteutuksen, ylläpidon ja käytöstä poiston vaiheet.

Luvanhaltijan on laadittava ja otettava käyttöön palveluiden hallintamenettelyt, jotka kattavat riskitietoisesti palveluiden hankinnan ja käytön sekä palveluista poistumisen.

Luvanhaltijan on varattava poliisille mahdollisuus osallistua uhkatilanteita koskevien turvajärjestelysuunnitelmien ja -toimenpiteiden valmisteluun.

Luvanhaltijan on määritettävä, luotava ja ylläpidettävä riittävät yhteistyömenettelyt tarvittaviin toimivaltaisiin viranomaisiin sekä toimialan kannalta olennaisiin sidosryhmiin.



Luvanhaltijalla on oltava menettelyt poikkeamien ennalta ehkäisemiseksi ja havaitsemiseksi. Turvajärjestelyjä koskevat poikkeamat ja uhkatilanteet on tunnistettava, arvioitava, vahingot on rajattava ja asianmukainen vaste on toteutettava oikea-aikaisesti.

Luvanhaltijalla on oltava menettelyt turvajärjestelyjä koskeviin poikkeamiin ja uhkatilanteisiin liittyvien tietojen keräämiseksi, suojaamiseksi, säilyttämiseksi ja hallitsemiseksi siten, että tutkinnan edellytykset varmistetaan.

Poikkeamissa ja uhkatilanteissa on viipymättä ryhdyttävä tilanteen vaatimiin toimiin tilanteen hallintaan saattamiseksi, seurausten estämiseksi ja rajoittamiseksi.
Luvanhaltijan on huolehdittava oikea-aikaisesta viranomaisten hälyttämisestä ja tilannekuvan välittämisestä.
Luvanhaltijan on tuettava poliisia yhteisen tilannekuvan ylläpidossa ja tilanteen turvallisuusperusteisessa johtamisessa uhkatilanteen ajan. Luvanhaltijan on järjestettävä poliisin avuksi riittävästi asiantuntemusta ydinlaitoksesta, ydinaineesta, laitosturvallisuudesta sekä turvajärjestelyistä.

Ydinenergialain 374 §:ssä tarkoitettu ydinlaitoksen tapahtumista ilmoittaminen kattaa ydinlaitoksen tai kuljetuksen turvajärjestelyjen osalta tiedot poikkeamasta tai uhkatilanteesta sekä vasteesta.

Luvanhaltijan on raportoitava turvajärjestelyihin liittyvästä poikkeamasta ja uhkatilanteesta kirjallisesti Säteilyturvakeskukselle kuukauden kuluessa tapahtumasta. Raportissa on esitettävä tapahtuman kuvaus, seuraukset sekä tarvittavat korjaavat toimenpiteet, joihin luvanhaltija on ryhtynyt tai ryhtyy vastaavan tapahtuman estämiseksi tulevaisuudessa.

Kyberturvallisuutta koskevien poikkeamien ilmoittamisesta säädetään kyberturvallisuuslain (124/2025) 11–13 §:ssä.

Luvanhaltijalla on oltava testatut jatkuvuuden hallinnan menettelyt turvajärjestelyjen ylläpitämiseksi.

Järjestelmiä ja varmuuskopioita on hallittava riskiarvion ja jatkuvuusvaatimusten mukaisesti. Varmuuskopiot on säilytettävä turvallisuusmerkityksen edellyttämällä tavalla. Tietojen palautusta on testattava säännöllisesti.

Luvanhaltijan on dokumentoitava turvajärjestelyt, mukaan lukien analyysit, poikkeamat, uhkatilanteet, harjoitukset ja arvioinnit siten, että sen perusteella järjestelmien, rakenteiden, laitteiden ja organisaation toiminnan vaatimustenmukaisuus voidaan osoittaa ja todentaa. Turvajärjestelyjä koskevat asiakirjat on pidettävä ajan tasalla.

Luvanhaltijan on suojattava turvajärjestelyjen kannalta keskeiset tiedot ja tallenteet katoamiselta, tuhoutumiselta, väärentämiseltä, luvattomalta käytöltä sekä luvattomalta luovuttamiselta ja varmistettava tietojen eheys ja saatavuus.

Luvanhaltijan on määritettävä tiedon luokittelun ja merkitsemisen periaatteet ja toteutettava niitä koskevat menettelyt turvallisuusmerkityksen perusteella.

Luvanhaltijan on laadittava henkilöstölle ohjeet, joita henkilöstön tulee noudattaa tietojen käsittelyssä sekä tietojärjestelmien käytössä.

Viranomaisen turvallisuusluokitteleman ja muun salassa pidettävän tiedon tietoturvallisuudesta on huolehdittava saman tasoisesti kuin asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetussa valtioneuvoston asetuksessa (1101/2019) säädetään.

Ennen viranomaisen turvallisuusluokittelemaa tai muuta salassa pidettävää tai näistä johdettua tietoa sisältävän aineiston luovuttamista kolmannelle osapuolelle luvanhaltijan on otettava yhteys Säteilyturvakeskukseen tai kyseisen tiedon laatineeseen muuhun viranomaiseen.

Luvanhaltijan on määritettävä, toteutettava ja valvottava turvajärjestelyjensä palvelutasot ja -vaatimukset.

Luvanhaltijan on arvioitava säännöllisesti turvajärjestelyjen vaatimustenmukaisuus ydinlaitoksen ja kuljetustoiminnan osalta. Arvioinnissa havaitut puutteet on korjattava asianmukaisesti.

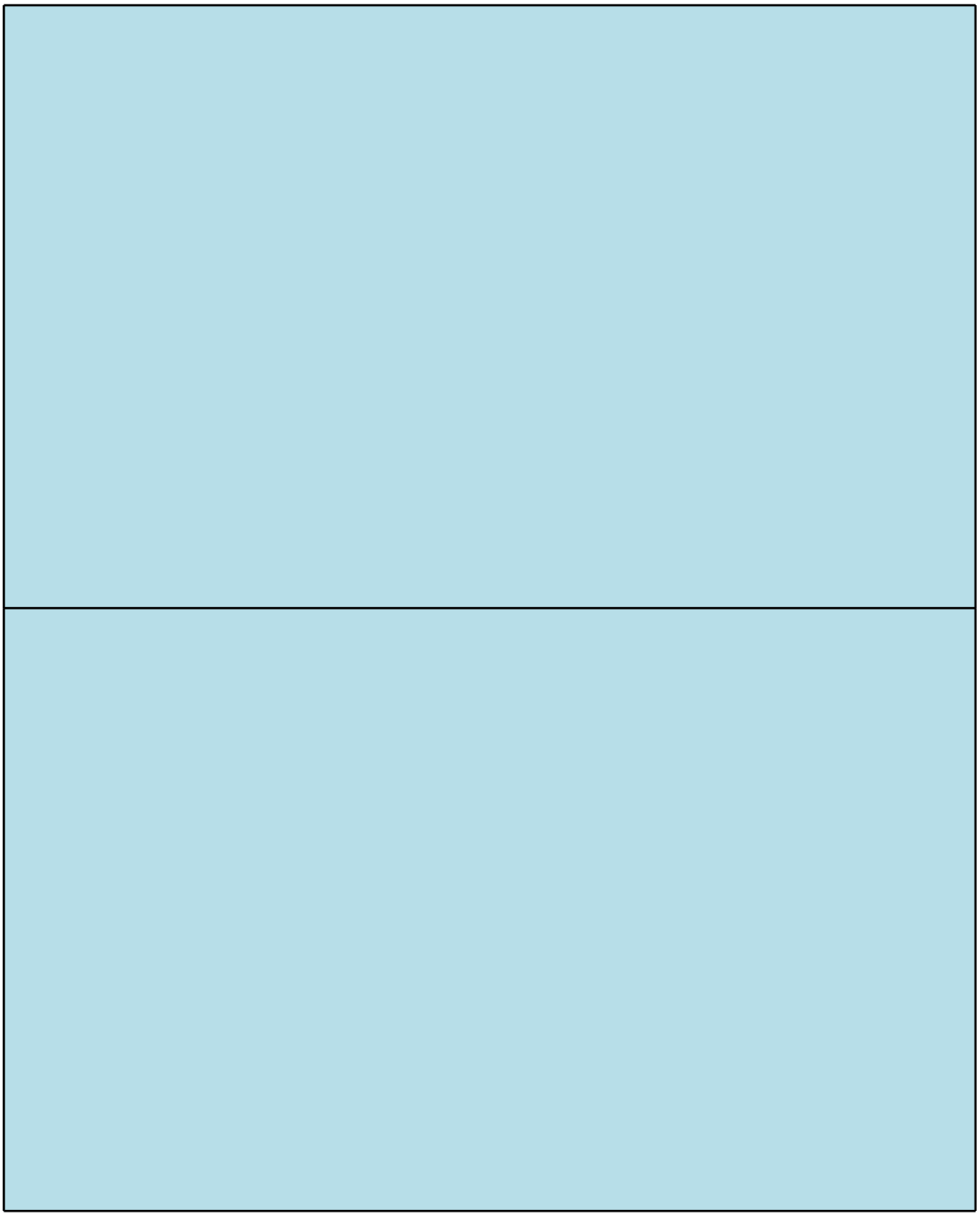
Luvanhaltijan on tehtävä turvajärjestelyiden itsearviointeja. Turvajärjestelyiden toimivuuden ja riittävyyden arvioinnissa on huomioitava myös riskien arviointiin ja uhkakuvaan tulleet muutokset ja ajanjaksolla ilmenneet turvallisuustapahtumat.

Luvanhaltijan on toteutettava turvajärjestelyjä koskeva harjoitustoiminta säännöllisesti, suunnitelmallisesti ja dokumentoidusti.

Harjoitustoiminnan on sisällettävä yhtäaikaisia onnettomuus- ja uhkatilanteita, fyysisiä ja tietoturvallisuusuhkia ja poikkeamia sekä suunnitteluperusteuhkan mukaisia tapahtumankulkuja, joiden avulla voidaan arvioida ja osoittaa suojaustavoitteiden täyttymistä. Harjoittelun on sisällettävä turvajärjestelyjen havainnointi- ja vastekyvykkyyden testausta.

Onnettomuus- ja uhkatilanteiden toimivaltaisille viranomaisille on varattava mahdollisuus osallistua harjoituksiin ja niiden suunnitteluun.

Luvanhaltijan on varmistettava turvajärjestelyjen vaikuttavuus poikkeamia ja uhkatilanteita vastaan. Vaikuttavuuden osoittamiseksi on käytettävä analyyseja, arviointeja ja harjoituksia, joiden perusteella turvajärjestelyjä on kehitettävä jatkuvan parantamisen periaatteella.
Luvanhaltijan on järjestettävä ydinlaitoksessa turvajärjestelyjen koekäyttöjakso ennen laitoksen käyttöönottoa. Koekäyttöä varten on oltava suunnitelma. Koekäytössä on osoitettava turvajärjestelyjen toteuttamisesta vastaavan organisaation osaaminen ja turvavalvontajärjestelmien ja -prosessien toimivuus. Koekäyttöjaksoon on sisällytettävä poikkeama- ja uhkatilanneharjoituksia. Koekäytön tulokset on arvioitava ja dokumentoitava.
Luvanhaltijalla on oltava järjestelmälliset menettelyt rakenteellisten, teknisten ja toiminnallisten turvajärjestelyjen ja tietojärjestelmien testaamiseen ja vaatimusten mukaisuuden osoittamiseen ennen käyttöönottoa sekä niiden toimivuuden ja turvallisuuden varmistamiseen käytön aikana.



Sen lisäksi, mitä tässä 1–10 luvussa määrätään kuljetuksista, sovelletaan kuljetusten turvajärjestelyihin tämän luvun vaatimuksia. Vaatimuksia sovelletaan myös kuljetukseen liittyvään tilapäiseen säilytykseen.

Vastaanottajan valmiudesta vastaanottaa kuljetus on varmistuttava ennen kuljetuksen aloittamista.

Luvanhaltijalla on oltava tieto sen lukuun tehtävän kuljetuksen lähdöstä ja saapumisesta Suomessa sekä kuljetuksen ajantasaisesta sijainnista Suomen alueella, kuten myös kuljetuksen maahan saapumisesta ja maasta poistumisesta.
Kuljetusta varten on oltava yhteyskeskus kuljetuksen seuraamista, yhteydenpitoa, ilmoituksia ja hälytyksiä varten. Yhteyskeskuksen on oltava siten suojattu, että sen toimintakyky säilyy myös uhkatilanteissa.
Kuljetusvälineiden turvallisuustarkastus sekä ydinaineen tai ydinjätteen lastaus, purku ja tilapäinen säilytys on tehtävä ympäristöstä rajatulla alueella, jolla liikkumista valvotaan.

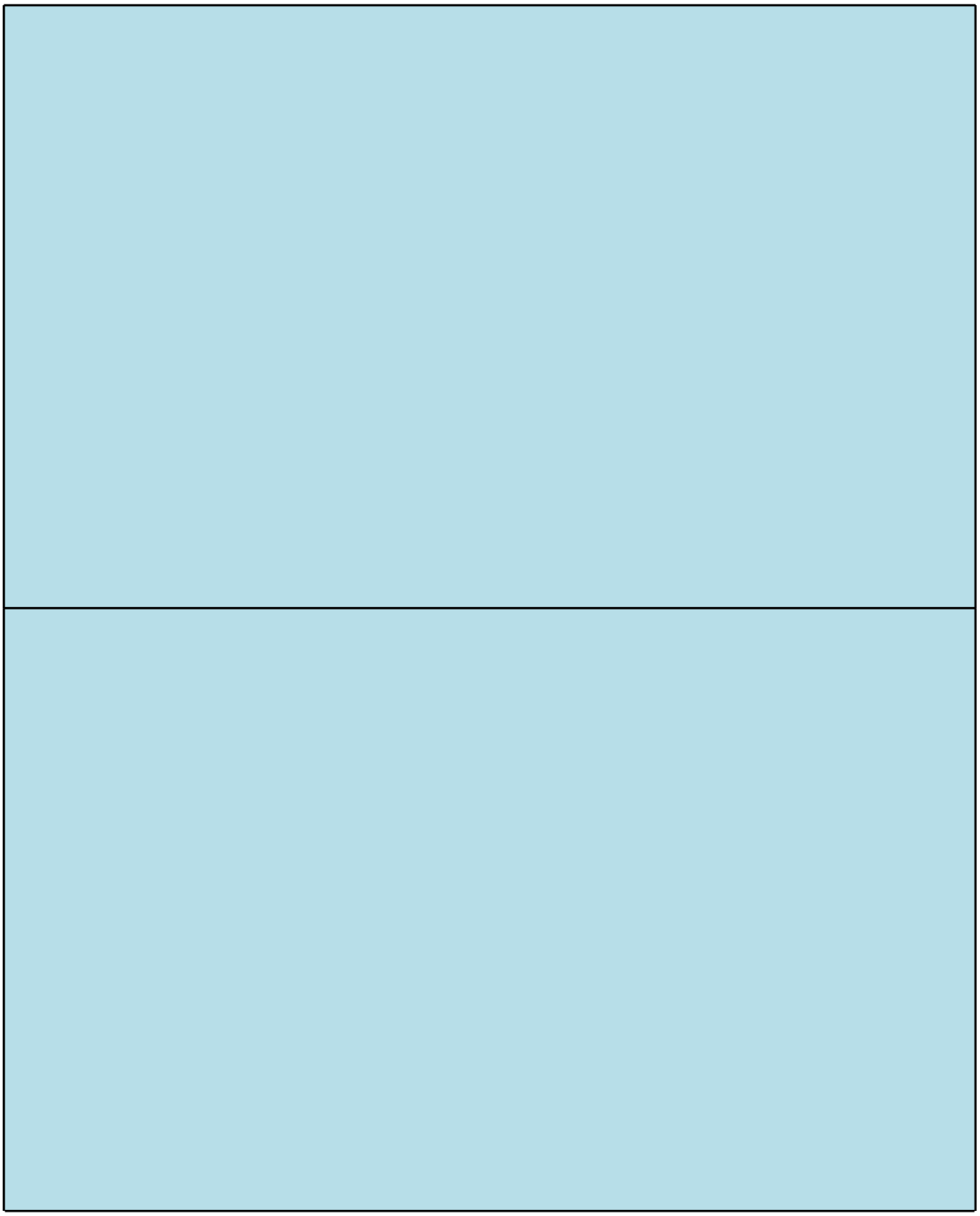
Hyväksytyistä suunnitelmista saa kuljetuksen aikana poiketa vain odottamattomista, pakottavista syistä. Suunnitelmista poikkeamisesta on ilmoitettava viipymättä Säteilyturvakeskukselle ja muille viranomaisille, joita poikkeaminen koskee.

Mikäli olosuhteet edellyttävät, on arvioitava tarve kuljetuksen ajankohdan siirtämiselle, suunnitellun kuljetusreitin vaihtamiselle tai kuljetuksen turvajärjestelyjen tehostamiselle. Kuljetukselle on suunniteltava varareittejä.

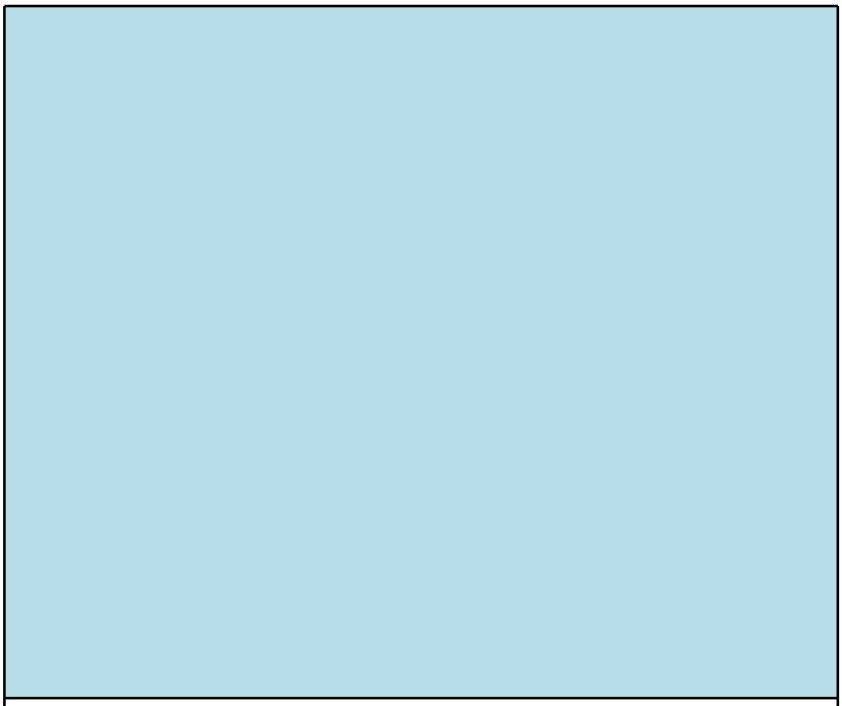
Kuljetusvälineen luvaton käyttö kuljetuksen aikana on estettävä teknisesti ajonestojärjestelmällä liitteessä 3 tarkoitettujen suojaluokan II ja I ydinaineiden kuljetuksessa.

Käytetyn ydinpolttoaineen ja muun suojaluokan II ydinaineen maantie-, rautatie- ja merikuljetus on suoritettava yksinkäytössä. Suojaluokkien II ja I ilmakuljetus on tehtävä rahtikoneella. Suojaluokan I ydinaine on kuljetettava siten, että se on kuljetusvälineen ainoa lasti.

Ydinenergialain 184 §:n 2 momentissa tarkoitettujen ydinaseiden leviämisen estämisen kannalta erityisen merkittävien ydinaineiden kuljetuksesta on tehtävä Säteilyturvakeskukselle kirjallinen ilmoitus 72 tuntia ennen kuljetuksen suunniteltua aloitusta. Ydinaseiden leviämisen estämisen kannalta erityisen merkittävien ydinaineiden kuljetuksella tarkoitetaan suojaluokan I kuljetusta.



Perustelut

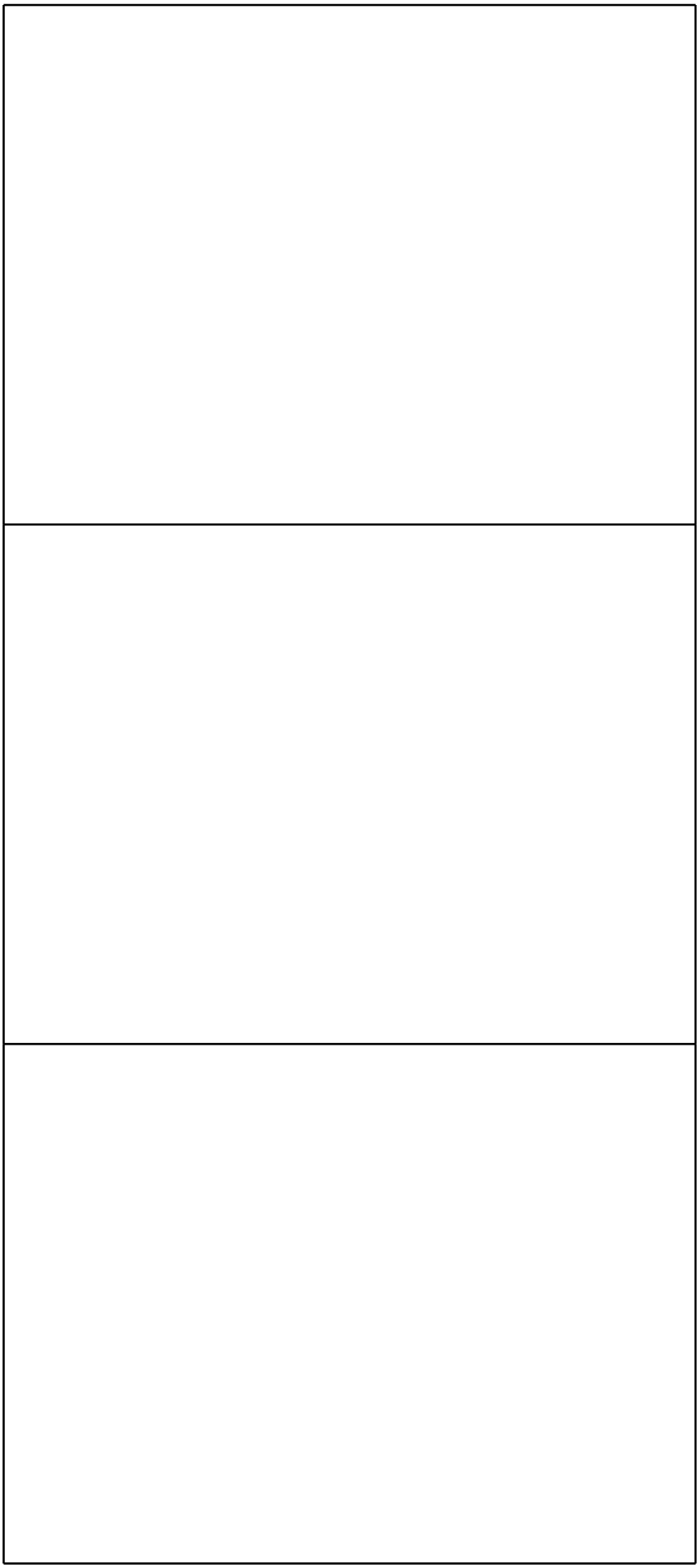


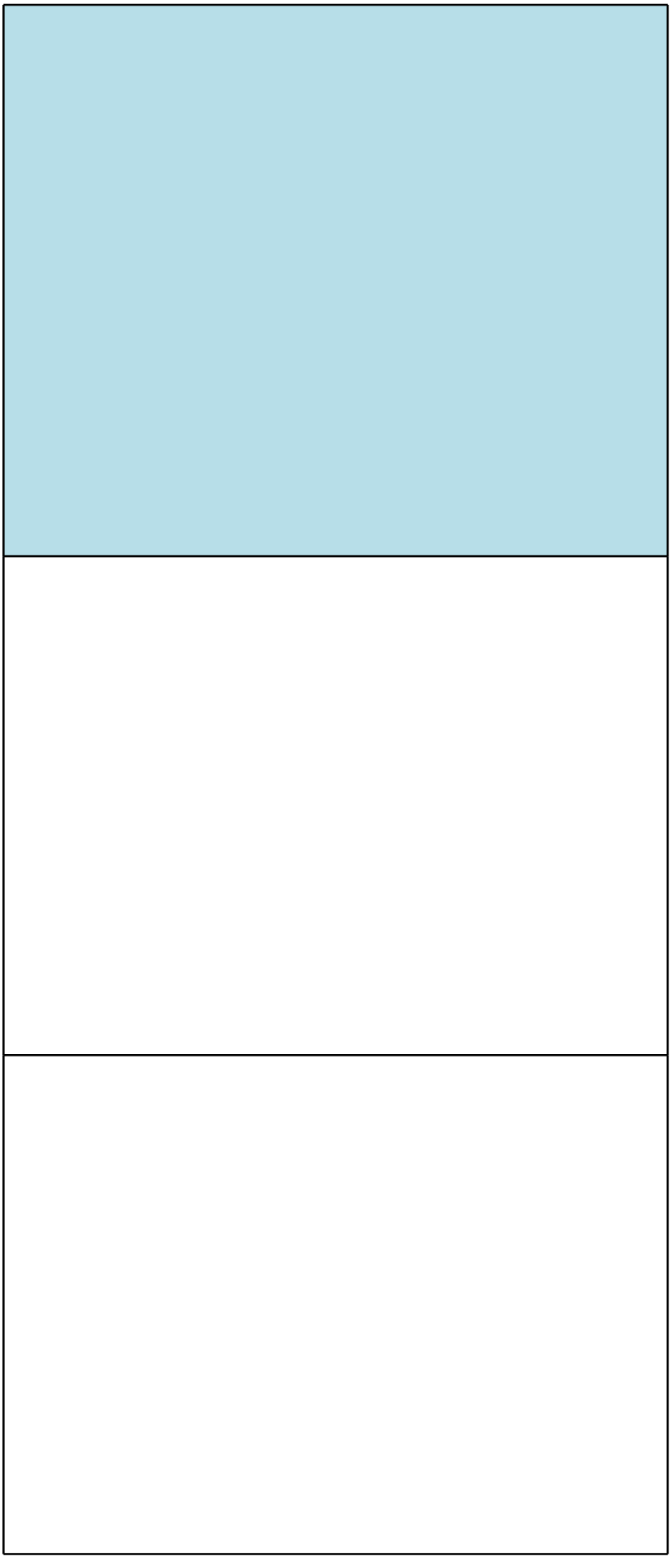
Pykälässä määrättäisiin määräyksen soveltamisalasta. Määräys koskee ydinlaitosten sekä ydinlaitosten toimintaan liittyvien ydinaineen ja ydinjätteen kuljetusten turvajärjestelyjä. *Ydinlaitoksella* tarkoitetaan ydinenergialain mukaista ydinvoimalaitosta, ydinteknistä laitosta, ydinpolttoaineen tuotantolaitosta ja loppusijoituslaitosta; ei kuitenkaan ydinaineen talteenottolaitosta. *Ydinteknisellä laitoksella* puolestaan tarkoitetaan ydinenergialain mukaan itsenäistä ydinlaitosta, jota käytetään:

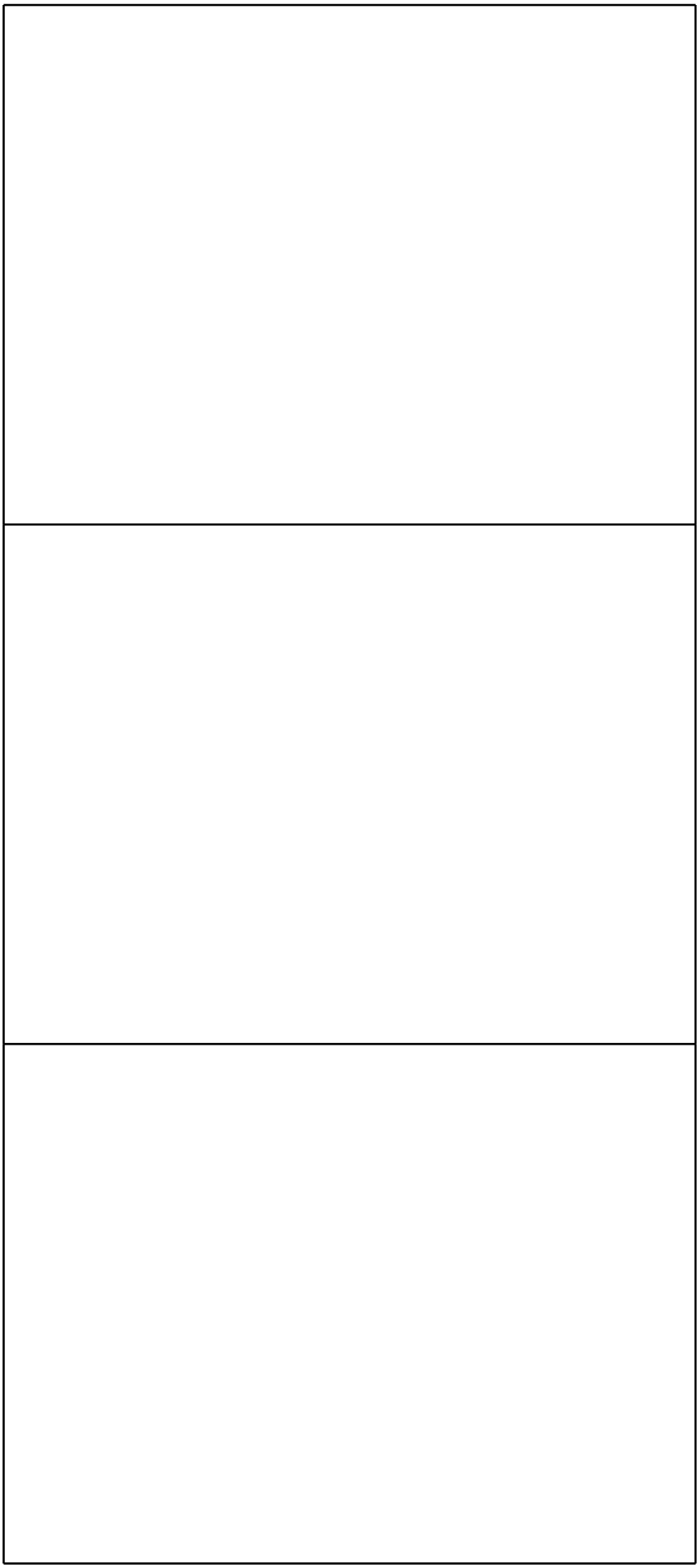
a) erityisen halkeamiskelpoisen aineen tai lähtöaineen käsittelyyn, pakkaamiseen, varastointiin tai muuhun huoltoon, kun kerralla säilytetään mainittuja ydinaineita yhteensä enemmän kuin 1 efektiivinen kilogramma sellaisena kuin se on määritelty komission asetuksen 2 artiklan 16 kohdassa (Euratom 2025/974);

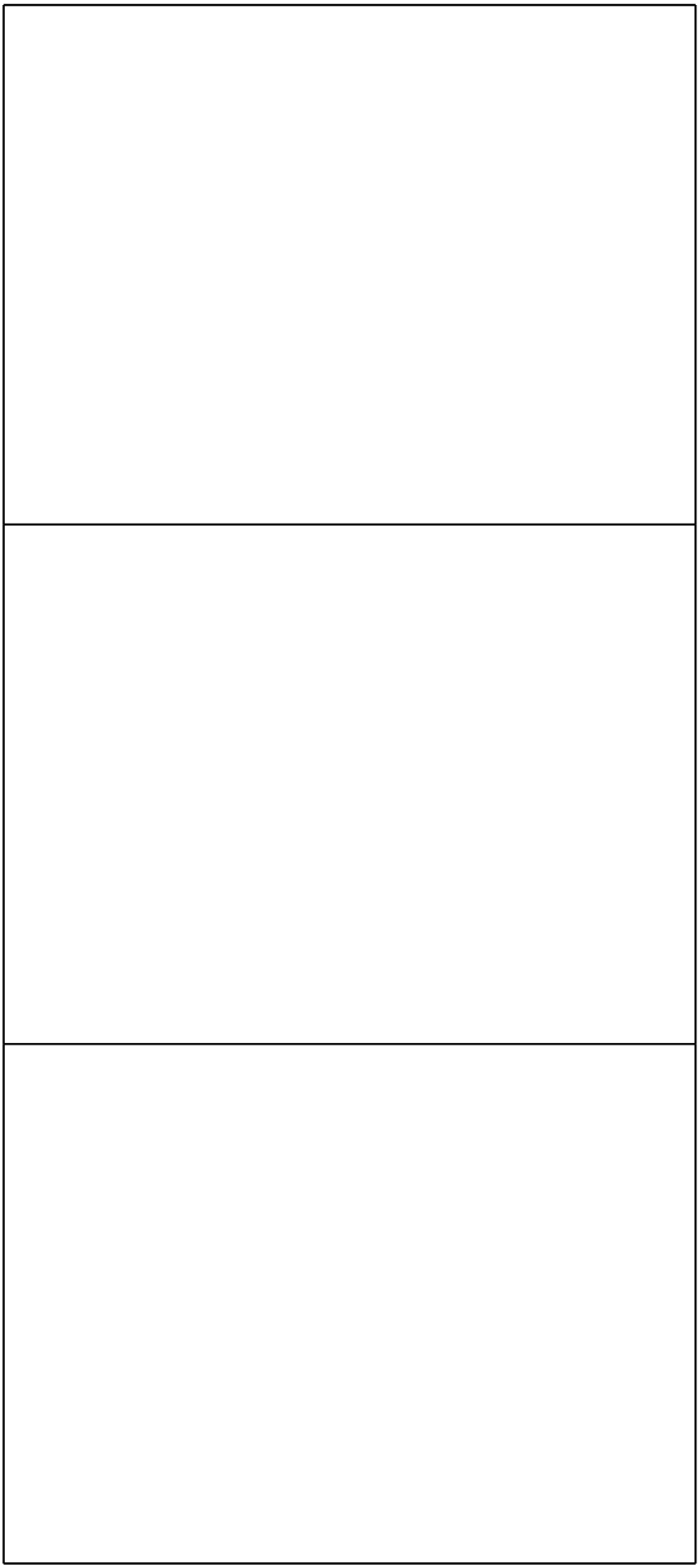
b) ydinjätteen käsittelyyn, pakkaamiseen, varastointiin tai muuhun huoltoon, ei kuitenkaan loppusijoitukseen;

Turvajärjestelyjen sisältö koostuu fyysisistä turvajärjestelyistä ja tietoturvallisuudesta, joista jälkimmäinen sisältää myös kyberturvallisuuden. Osa-alueet tukevat toisiaan eikä niitä voida tai pidä käsitellä toisistaan riippumattomasti. Tietoturvallisuuden merkitystä digitalisoidussa, ohjelmoitavassa laitosympäristössä on korostettu määräyksessä.

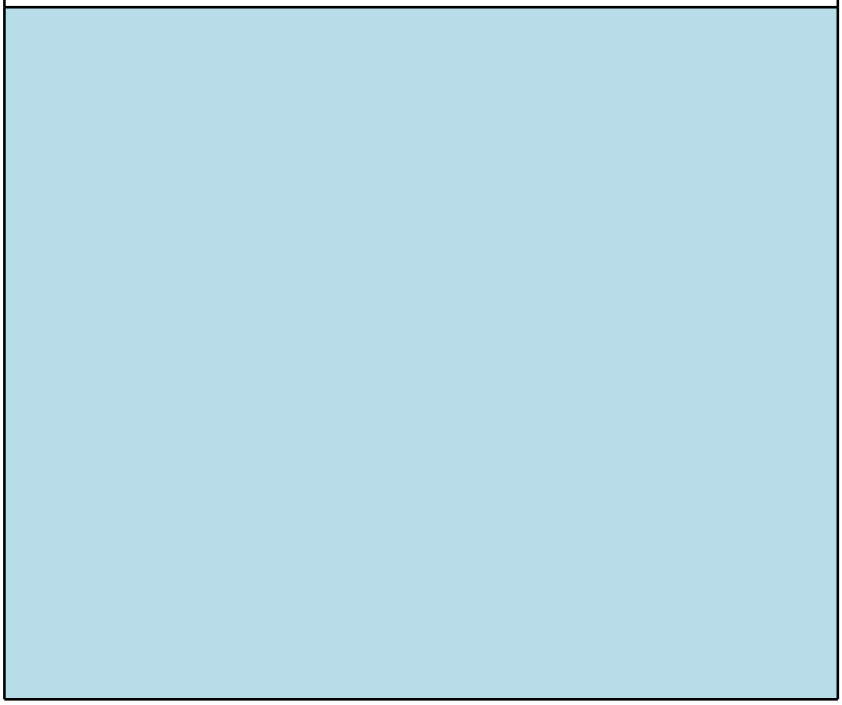


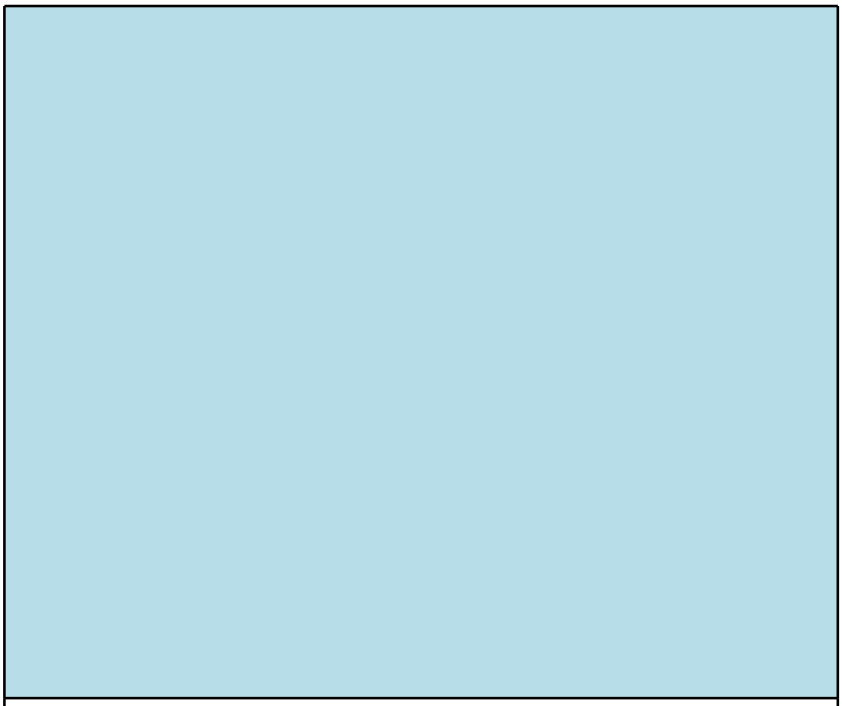






Pykälässä esitettäisiin määräyksessä käytettyjen keskeisten käsitteiden määritelmiä. Määritelmät ovat sinänsä ydinalalla vakiintuneita, mutta ne ovat hyödyllisiä esimerkiksi mahdollisille uusille toimijoille ydinalalla, esimerkkinä ovat vaikkapa erot hälytyskeskus vs. valvomo ja käsite turvallisuuslohko. Poikkeaman määritelmässä mainitut läheltä piti -tilanteet ovat tietoturvallisuuden osalta erityisen merkittäviä, sillä läheltä piti -tilanteen ja laajemman häiriön välinen raja voi olla hyvin hienojakoinen.

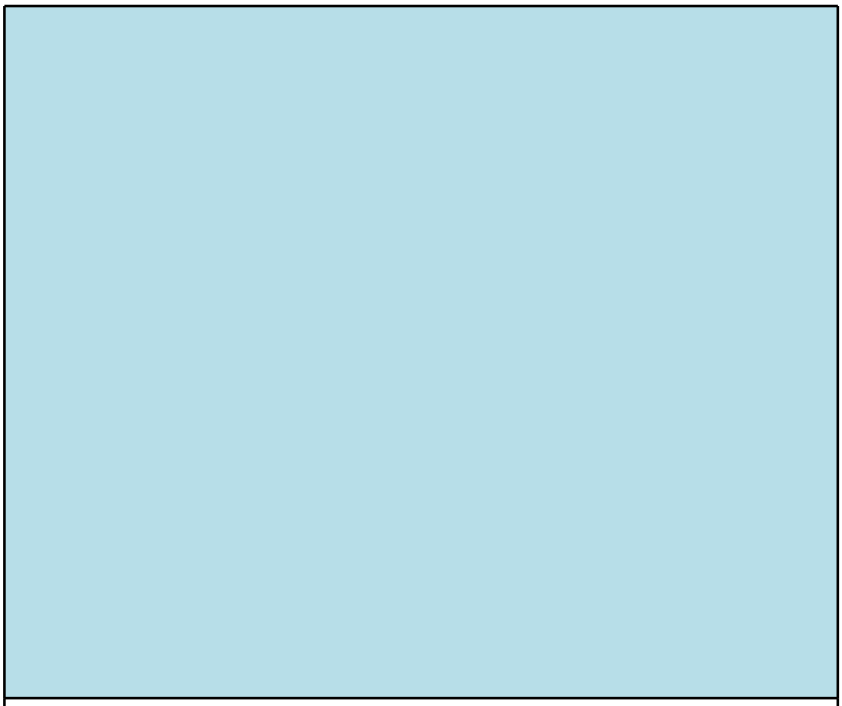




Pykälän 1 momentissa määrättäisiin turvajärjestelyjen yleisistä suunnitteluperusteista. Viittaus ydinaineiden turvajärjestelyjä koskevista toimista tehdyn yleissopimukseen 72/1989 ja sen muutokseen 19/2016 (ACPPNM) on paikallaan koska sopimus on sitovaa kansallista lainsäädäntöä. Sopimus on voimaan saatettu em. asetuksella ja lailla (asetus ydinaineiden turvajärjestelyjä koskevista toimista tehdyn yleissopimuksen voimaansaattamisesta ja sen soveltamisesta, laki ydinaineiden turvajärjestelyjä koskevista toimista tehdyn yleissopimuksen muutoksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta). Artiklan 2 a perusperiaatteisiin kuuluvat mm. uhkakuva, luokitteleva lähestymistapa ja syvyyssuuntainen puolustus. Sopimuksen liitteessä 1 on määritelty sopimuksen edellyttämät turvajärjestelyt.

Pykälän 2 momentissa määrättäisiin syvyyssuuntaisen puolustuksen toteuttamisesta. Syvyyssuuntainen puolustus on ydinlaitosten suunnitteluun ja käyttöön liittyvä kansainvälinen turvallisuuskonsepti, jonka tavoitteena on ehkäistä ja lieventää onnettomuuksia ja uhkia. Vaatimus syvyyssuuntaisesta puolustuksesta on ACPPNM-sopimuksessa kirjattu yhdeksi sen keskeisistä perusperiaatteista (ACPPNM perusperiaate I). Syvyyssuuntainen puolustus mahdollistaa useiden eri tasojen ja keinojen käytön häiriöiden tai uhkien torjumiseksi. Tämä tarkoittaa, että turvajärjestelyt eivät perustu vain yhteen toimenpiteeseen, vaan niitä toteutetaan useilla tasoilla (esim. fyysiset, teknologiset, inhimilliset) ja useissa eri paikoissa. Syvyyssuuntainen puolustus parantaa järjestelyjen resilienssiä, eli kykyä kestää ja palautua häiriöistä. Jos yksi turvaelementti epäonnistuu, muut voivat silti toimia ja estää uhkien toteutumisen. Tämä on erityisen tärkeää monimutkaisissa ympäristöissä, joissa uhkat voivat kehittyä nopeasti ja odottamattomasti.

Pykälän 3 momentissa määrättäisiin rakenteiden, järjestelmien, laitteiden ja suunnittelusta sekä toteuttamisesta siten, että ne ohjaavat turvalliseen toimintaan. Momentissa mainittujen asiakokonaisuuksien suunnittelu sekä toteutus turvallisuuslähtöisesti suojelee käyttäjiä, ja ympäristöä sekä tukee luvanhaltijan toimintaa säästäen resursseja, varmistaen myös lainmukaisuutta. Momentissa mainittujen asiakokonaisuuksien suunnittelu siten, että ne ohjaavat turvalliseen toimintaan ja ennaltaehkäisevät turvallisuutta heikentävää toimintaa on, tärkeää monesta syystä. Näistä mainittakoon mm. henkilöturvallisuus, virheiden minimointi (virheansojen välttäminen), tietoturva ja järjestelmän luotettavuus sekä säännöstöjen ja standardien noudattaminen. Esimerkkinä kriittinen päätelaite, johon ei hyväksyttyjen ulkoisten muistilaitteiden kytkeminen on estetty. Rakenteiden, järjestelmien, laitteiden ja ohjelmistojen suunnittelu turvallisen toiminnan ohjaamiseksi ja turvallisuutta heikentävän käyttäytymisen ehkäisemiseksi on keskeinen osa tehokasta riskienhallintaa ja turvallisuuden varmistamista. Hyvin suunnitellut järjestelmät voivat parantaa kokonaisturvallisuutta, torjua uhkia, vähentää onnettomuuksien riskejä ja edistää organisaation toimintakulttuuria.
Pykälän 4 momentissa määrättäisiin turvajärjestelyjen tarkoituksenmukaisesta toimeenpanosta. Tällä tarkoitetaan, että turvajärjestelyt ovat suunniteltu ja toteutettu vastaamaan tehokkaasti todellisia tarpeita ja riskien edellyttämiä hallintakeinoja ilman liiallista monimutkaisuutta tai tarpeetonta haittaa turvalliselle toiminnalle tai toimivuudelle. Tarkoituksena on, että turvajärjestelyt mitoitetaan oikein suhteessa riskeihin, jotta ne ovat mukautuvia ja voivat vastata muuttuvaan uhkaympäristöön ja vaatimuksiin.



Pykälän 1 momentissa esitettäisiin riskienhallintaa koskevia periaatteita. Riskienhallinnan määräyksenantovaltuus on YEL 126 §. Ehdotetun 1 mom. tarkoituksena on myös, että lainvastaisen toiminnan riskit tulevat osaksi riskienhallinnan kokonaisuutta ja mahdollisuuksien mukaan yhteismitallisesti arvioiduiksi. Lainvastaisella toiminnalla tarkoitetaan esimerkiksi sellaista vahingontekoa, sabotaasia tai anastusta, joka täyttää rikoksen tunnusmerkit. Momentissa tarkoitettu muu toiminta on sellaista, joka ei täytä varsinaisen rikoksen tunnusmerkkejä, mutta voisi vaarantaa turvallisuutta suoraan tai välillisesti. Kyseessä voi olla esimerkiksi ohjeiden vastainen toiminta.

Pykälän 2 momentissa määrättäisiin kyberturvallisuuden riskienhallinnasta, jonka osalta määräyksenantovaltuus tulee kyberturvallisuuslain 9 §:n 4 momentista. Poikkeamien vaikutus ydinlaitoksen ja kuljetuksen turvallisuuteen arvioidaan riskitietoisesti, jonka lisäksi keskeistä on myös tunnistaa riskiresilienssi eli riskisietoisuus. Riskienhallintaan liittyvä käytännöt perustuvat muun ohessa standardiin ISO/IEC 31000

Pykälän 3 momentissa määrättäisiin IAEA:n ja Euratomin ydinmateriaalivalvontaan kuuluvan laitteiston ja tiedonsiirron ydinlaitokseen kohdistuvan riskin huomioon ottamisesta. Luvanhaltijalla ei ole pääsyä tähän laitteistoon ja sen lähettämään tietoon, joten näihin liittyvät riskit on otettava muulla tavoin huomioon laitoksen suunnittelussa ja toteutuksessa. Kyberturvallisuuden osalta kyseessä on kyberturvallisuuslain 9 § 4 mom 1 kohdassa tarkoitettu toimialakohtainen erityispiirre. Muilta osin vaatimus perustuu ydinenergialain 80 ja 126 §:ään.

Pykälän 1 momentissa määrättäisiin turvajärjestelyjen toteuttamisesta suunnitteluperusteuhan (Design Basis Threat, DBT) mukaisesti. Säteilyturvakeskus laatii suunnitteluperusteuhan Suojelupoliisin toimittaman uhkakuvan perusteella. Suunnitteluperusteuhan julkinen osa kuvaa DBT:n laadinnan, tarkoituksen ja käytön. Turvajärjestelyjen mitoitusperusteet ja suojaustavoitteet sisältävä suunnitteluperusteuhka on salassa pidettävä ja turvallisuusluokiteltu viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 24.1 §:n 7) kohdan perusteella. Momentin tarkoitus on luetella yleisellä tasolla ne uhat, joita vastaan on suojauduttava. DBT:tä sovelletaan uusiin ydinlaitoksiin sellaisenaan ja rakenteilla olevilla ja käytössä oleville tehdään päätös, jossa voidaan hyväksyä tarvittavat poikkeamat.

Kulkuneuvo on paikasta toiseen kulkemiseen tarkoitettu laite, joka voi kuljettaa matkustajia, tavaroita tai molempia maalla, vedessä tai ilmassa.

Pykälän 2 momentissa määrättäisiin 1 momentissa esitetyssä suunnitteluperusteuhassa tarkoitetun toiminnan toteuttamisen huomioon ottamisesta.

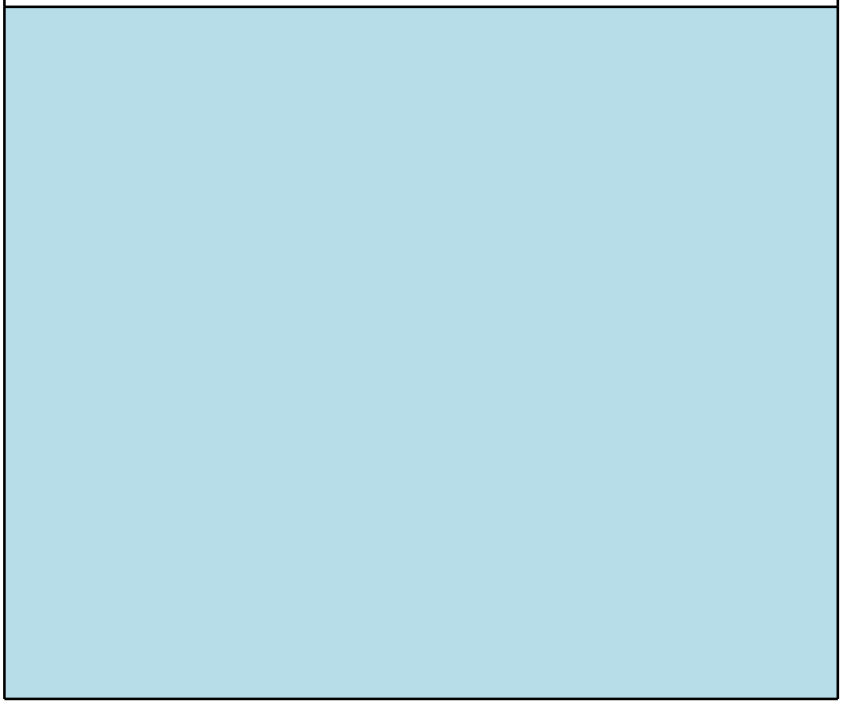
Pykälän 3 momentissa edellytettäisiin suojautumista fyysisiä uhkia, vakoilua ja vaikuttamista vastaan suunnitteluperusteuhan mukaisesti tilaturvallisuuden keinoin myös esimerkiksi toimistotilojen osalta, jos niissä käsitellään salassa pidettävää tietoa. Kyseessä on tilaturvallisuutta koskeva vaatimus rakenteelliseen suojaukseen. Vakoilua ja vaikuttamista voidaan pyrkiä tekemään salakatselun tai salakuuntelun kautta tai sähkömagneettisen säteilyn avulla. Turvakontrollit määritetään tilojen ja niissä käsiteltävän tiedon turvallisuusmerkityksen perusteella.

Pykälän 1 momentissa määrättäisiin turvajärjestelyjen suunnittelusta ja toteutuksesta siten, että turvallisuutta vaarantavan toiminnan torjuntaa varten on olemassa toisistaan riippumattomia turvallisuuden hallintakeinoja. Ei-toivottuja tapahtumia hallitaan ja viivytetään kerroksittaisilla kokonaisuuksilla, jotka voivat koostua esimerkiksi hallinnollisista, fyysisistä, teknisistä ja operatiivisista toiminnallisuuksista. Syvyyssuuntaista puolustusta käytetään sekä fyysisten turvajärjestelyjen että tietoturvallisuuden puolella. Tietoturvallisuudessa syvyyssuuntainen puolustus on monikerroksellinen suojausmalli, jossa joukko erilaisia tietoturvakontrolleja on kerrostettu kriittisten kohteiden suojaamiseksi. Tarkoituksena on se, että jos yksi kontrolli epäonnistuu, on toinen turvallisuuskontrolli tällöin myös torjumassa hyökkäystä.

Pykälän 2 momentissa määrättäisiin siitä, että ennaltaehkäisevät toimenpiteet, havaitseminen, viivytys ja vaste sekä palautuminen on toteutettava kokonaisuutena. Näiden toimenpiteiden arviointi kokonaisuutena on välttämätöntä koska yksittäisten osa-alueiden käsittely eristyksissä voi johtaa riskien ja uhkien huonoon hallintaan. Kun kaikki osa-alueet suunnitellaan ja toteutetaan synergisesti, ne tukevat toisiaan, jolloin organisaatio voi kehittää vahvemman ja kattavamman turvallisuusstrategian. Lähestymistapa parantaa organisaation kykyä reagoida uhkiin ja palautua häiriötilanteista, mikä puolestaan lisää toimintakykyä ja luotettavuutta.

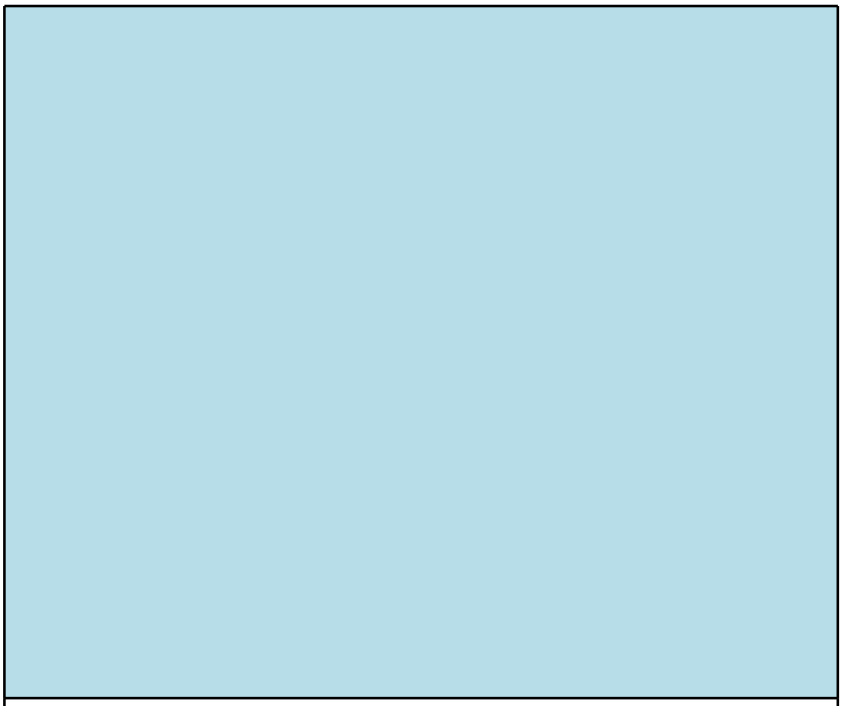
Pykälän 3 momentissa määrättäisiin, että ydinlaitoksen turvajärjestelyihin liittyvät järjestelmät ja turvallisuutta varmentavat keskeisimmät toiminnot eivät saisi olla yksinomaan ohjelmistopohjaisten järjestelmien varassa. Turvallisuuden ja uhkien hallinta ei voi olla täysin ohjelmistopohjaisten järjestelmien varassa koska ne voivat käsitellä tunnettuja ja ennalta määriteltyjä sääntöjä ja skenaarioita, mutta eivät välttämättä pysty arvioimaan tai reagoimaan uusiin tai odottamattomiin uhkiin turvallisesti. Ohjelmistopohjaisiin järjestelmiin sisältyy aina virheen tai manipulaation riski. Esimerkiksi kulunhallintajärjestelmän voisi varmentaa mekaanisilla avaimilla. Mikäli suunniteltuun tarkoitukseen ei ole saatavilla muita kuin ohjelmistopohjaisia järjestelmiä (esim. kommunikaatiojärjestelmät), niin turvallisuustasoa tulisi pyrkiä parantamaan esimerkiksi (diverssillä) varajärjestelmällä.

Pykälän 4 momentissa määrättäisiin siitä, että turvallisuuden kannalta keskeisten tietojärjestelmien tietoliikenne olisi suunniteltava ja toteutettava siten, ettei se ole langattomien yhteyksien varassa. Toiminnan ja toimintojen perustaminen langattomiin verkkoihin tekee niistä alttiimman häiriöille ja häirinnälle, signaalin heikkenemiselle ja tietoturvariskeille. Toimintavarmuuden ja turvallisuuden varmistamiseksi tulisi mahdollisuuksien mukaan hyödyntää monimuotoisia yhteysratkaisuja, jossa langattomat ja langalliset verkot täydentävät toisiaan. Tämä takaa sekä turvallisemman että luotettavamman toiminnan kaikissa tilanteissa. Kysymyksessä voi olla myös asiakokonaisuus, johon soveltuu käytettäväksi ainoastaan langallinen verkko esimerkiksi toimintavarmuusvaatimuksen tai turvallisuusmerkityksen vuoksi. Poikkeuksena vaatimukseen on puhelinjärjestelmät, jotka nykyään ovat käytännössä aina langattomia, kuten esimerkiksi turvallisuuden kannalta keskeinen Virve-järjestelmä. Laitoksen turvallisuusautomaatioon liittyvissä tietojärjestelmissä langattomat yhteydet eivät pääsääntöisesti ole sallittuja.



Pykälän 1 momentissa määrättäisiin turvajärjestelyihin liittyvästä arvioinnista turvallisuusmerkityksen ja riskin mukaisesti siten, että otetaan huomioon lainvastaisen tai muun turvallisuutta vaarantavan toiminnan mahdollisuus. Tämän tarkoitus on täydentää perinteistä safety-luokittelua siitä näkökulmasta, että turvallisuustoiminnon merkityksen ja vikaantumistodennäköisyyden lisäksi huomioidaan tahallinen vikaannuttaminen tai manipulointi. Tahallinen vikaannuttaminen tai manipulointi voisi vaikuttaa esim. rakenteiden, järjestelmien, laitteiden, ohjelmistojen ja tietojen eheyteen ja saatavuuteen. Arviointi on keskeinen askel riskienhallintaprosessissa, jonka avulla voidaan kehittää asianmukaisia turvatoimia ja varautumissuunnitelmia. Kun riskit on arvioitu, organisaatiot voivat kohdistaa rajalliset resurssit tarkoituksenmukaisesti. Riskitietoinen, luokitteleva lähestymistapa (graded approach) on myös yksi perusperiaate ACPPNM-sopimuksessa. Tietoturvallisuuden osalta voidaan hyödyntää IAEA:n Security Levelit 1 – 5, joihin liittyviä viitteitä ovat esimerkiksi Implementing Guide IAEA NSS No. 42-G (Computer Security for Nuclear Security) sekä Technical Guidance IAEA NSS No. 17-T (Computer Security Techniques for Nuclear Facilities). Huom: Ydinaineiden ja ydinjätteiden proliferaatiopohjainen luokittelu on eri asia, joka perustuu niin ikään ACPPNM-sopimukseen (ja josta säädettäneen uudessa VNA:sa).
Pykälän 2 momentissa määrättäisiin ylläpidettävän tiedon ajantasaisuudesta ja muutoksenhallinnasta. Ajantasainen ja kattava tieto mahdollistaa nopean reagoimisen mahdollisiin uhkiin tai häiriöihin. Kun tiedetään tarkasti, mitä järjestelmiä ja laitteita on käytössä, varmistetaan, että niihin liittyvät turvatoimet voivat olla tehokkaita. Kun tiedetään, mitä resursseja organisaatiolla on ja mitä niiden elinkaari kattaa, voidaan suunnitella huoltoja, päivityksiä ja tarvittaessa poistoja ennakoivasti, mikä lisää resurssien käyttöikää ja hyötyä. Muutosten jäljitettävyyttä vaaditaan, jotta voidaan palata aikaisempiin versioihin tai aloittaa selvittämään, mikä aiheutti häiriöitä. Kun kaikki muutokset on dokumentoitu, voidaan helposti selvittää, mihin muutokseen ongelmat liittyvät ja toimia sen mukaisesti.

Pykälän 3 momentissa määrättäisiin ydinlaitoksen toiminnassa ja kuljetuksissa käytettävistä rakenteista, järjestelmistä, laitteista ja ohjelmistoista. Tällä varmistetaan muun muassa, että henkilöstö ei käytä työtehtävissä omia tietokoneita, muistitikkuja ja muita älylaitteita. Hyväksymättömien rakenteiden, järjestelmien, laitteiden tai ohjelmistojen käyttö voi johtaa haitallisiin seurauksiin.



Pykälän 1 momentissa määrättäisiin turvajärjestelyjen hallintajärjestelmästä. Turvajärjestelyjen hallinta on keskeinen osa organisaation kokonaisturvallisuusstrategiaa. ACPPNM-sopimuksessa turvajärjestelyjen hallintajärjestelmää koskeva vaatimus on yksi perusperiaatteista (Perusperiaate J, jossa tosin käytetään termiä laadunhallinta). Integroimalla turvajärjestelyt luvanhaltijan johtamisjärjestelmään varmistetaan, että turvajärjestelynäkökohdat otetaan huomioon kaikessa toiminnassa ja päätöksenteossa. Turvajärjestelyjen hallintajärjestelmä mahdollistaa riskien järjestelmällisen tunnistamisen, arvioinnin ja hallinnan. Hallintajärjestelmä on prosessi, jossa parannetaan aktiivisesti ja jatkuvasti organisaatioon, ihmisiin, tiloihin ja teknologiaan kohdistuvien riskien hallintakeinoja.

Pykälän 2 momentissa määrättäisiin tietoturvallisuuden hallintajärjestelmästä. Ydinlaitokset ovat osa kansallista ja kansainvälistä kriittistä infrastruktuuria. Ne käsittelevät suuria määriä arkaluonteista tietoa, kuten ydinmateriaalin käsittelyä ja turvallisuusprosessien hallintaa. Tietoturvallisuuden hallintajärjestelmän toteuttaminen ISO/IEC 27001 -standardin tasoisesti tarjoaa kattavan ja systemaattisen kokonaisuuden tietoturvallisuuden hallintaan. ISO/IEC 27001:n mukainen hallintajärjestelmä velvoittaa huomioimaan organisaatioon, henkilöstöön, tiloihin ja teknologiaan liittyvät tietoturvariskit. Ydinlaitoksissa on tärkeää tunnistaa ja arvioida mahdollisia tietoturvauhkia, jotta voidaan toteuttaa tarvittavat suojatoimet ja vähentää riskejä. Luvanhaltijalle asetettu vaatimus standardia ISO/IEC 27001 vastaavasta turvallisuustasosta ei edellytä kyseisen standardin mukaista sertifiointia, ja myös muita vastaavia standardeja voidaan hyödyntää. Tällaisia ovat esimerkiksi COBIT (Control Objectives for Information and Related Technologies), NIST Cybersecurity Framework (National Institute of Standards and Technology) ja ITIL (Information Technology Infrastructure Library). Nämä standardit ja kehykset tarjoavat erilaisia lähestymistapoja ja käytänteitä tietoturvallisuuden hallintaan, ja organisaatiot voivat valita niistä parhaiten omiin tarpeisiinsa sopivia tai yhdistellä niitä saavuttaakseen kattavamman riskienhallinnan.

Pykälän 1 momentissa määrättäisiin turvajärjestelynäkökohdista luvanhaltijan toimintakulttuurissa. Vaatimus perustuu ACPPNM-sopimuksen perusperiaatteeseen (perusperiaate F Security Culture), joka edellyttää turvajärjestelynäkökohtien huomioon ottamista organisaation toimintakulttuurissa. Suomessa tämä näkökohta on jäänyt ”turvallisuuskulttuurin” (Safety Culture) varjoon, ja tästä Suomea on huomautettu tehdyissä kansainvälisissä IPPAS-vertaisarvioinneissa. IPPAS-suositusten mukaan vaatimus on esitettävä eksplisiittisesti STUKin määräyksessä, jotta asia saisi ansaitsemansa huomion. Turvajärjestelyjen sisällyttäminen toimintakulttuuriin ja sen arviointiin mahdollistaa tehokkaamman riskienhallinnan ja jatkuvan parantamisen. Toimintakulttuuria käsitellään myös ydinenergialain 120 §:ssä (Ydinlaitoksen henkilöstö).

Pykälän 2 momentissa määrättäisiin turvajärjestelynäkökohdista inhimillisten tekijöiden hallinnassa. Vaatimus perustuu siihen, että oikein toteutetut turvajärjestelyt voivat auttaa vähentämään inhimillisten virheiden todennäköisyyttä ja vaikutuksia sekä ehkäisemään uhkia. Kun turvajärjestelyt yhdistetään inhimillisiin tekijöihin, ne voivat lisätä työntekijöiden sitoutumista ja osallistumista turvallisuustoimiin. Turvajärjestelynäkökohtiin kuuluu sekä tahattoman että tahallisen turvallisuutta vaarantavan toiminnan huomioon ottaminen, mukaan lukien manipulointi ja hyväksikäyttö.

Pykälän 1 momentissa määrättäisiin, että luvanhaltijalla on oltava järjestelmälliset ja monialaiset menettelyt, joilla hallitaan uhkaa, joka liittyy henkilöihin, joilla on luvallinen pääsy ydinlaitokseen tai kuljetukseen taikka niiden järjestelmiin, rakenteisiin, tai laitteisiin tai niitä koskeviin tietoihin (insider-uhka). Menettelyjen olisi katettava myös toimitusketjut riskitietoisesti.

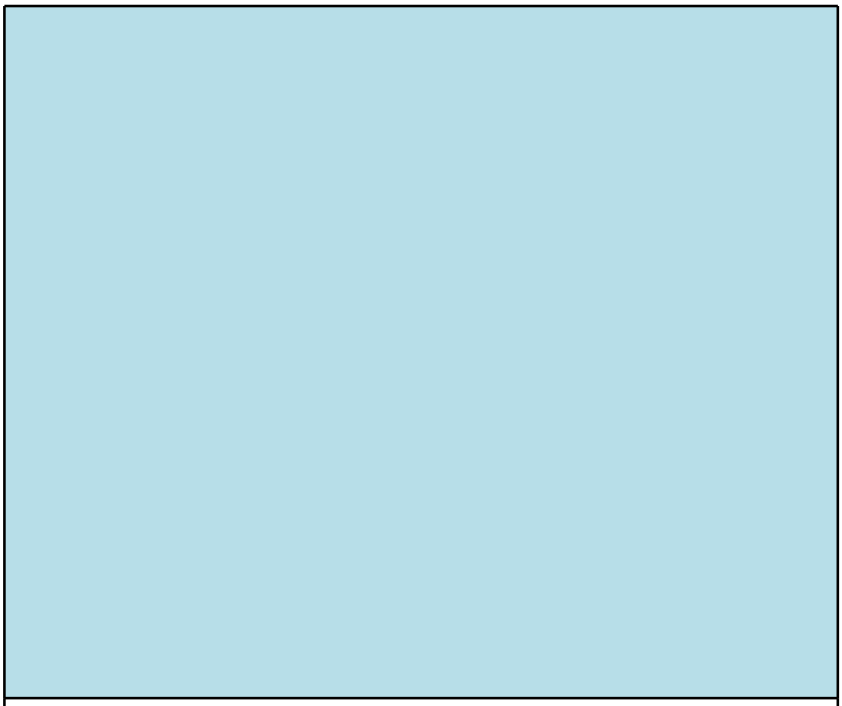
Koska määritelmällisesti insider-henkilöllä on luvallinen pääsy suojattavaan paikkaan tai tietoon (access, authority, knowledge), insider-uhka on erityisen haastava torjua. Pääsy, toimivalta ja tieto aiheuttaa tilanteen, jossa henkilöt voivat aiheuttaa merkittävää vahinkoa, joko tahallisesti tai tahattomasti. Kansainvälisissä yhteyksissä on todettu, että insider-toiminta on yleisin uhkavektori. Uhan torjuntaan kuuluu sekä hallinnollisia että teknisiä kontrolleja, rekrytointivaiheessa ja koko työsuhteen ajan. Järjestelmälliset ja monialaiset menettelyt auttavat tunnistamaan ja hallitsemaan mahdollisia riskejä, ennen kuin niistä tulee todellisia uhkia.

Monialaisilla menettelyillä tarkoitetaan esimerkiksi menettelyjä, jossa eri osa-alueiden asiantuntijat käsittelevät yhteistoiminnassa sellaiset havainnot, jotka saattavat ilmentää insider-uhan kohonnutta riskiä. Havainnot voidaan organisaatiossa yhteistoimin luokitella ja niille määritellä käsittelysäännöt ja toimenpiteet vakavuuden mukaan. Asiantuntijoihin voi kuulua henkilöstöhallintoa, esihenkilöitä, turvajärjestelyvastuuhenkilöitä ja -asiantuntijoita sekä tietohallintoa. Oleellista on varmistaa tiedon kulku ja havaintojen ja tapahtumien käsittely sekä tietosuoja.

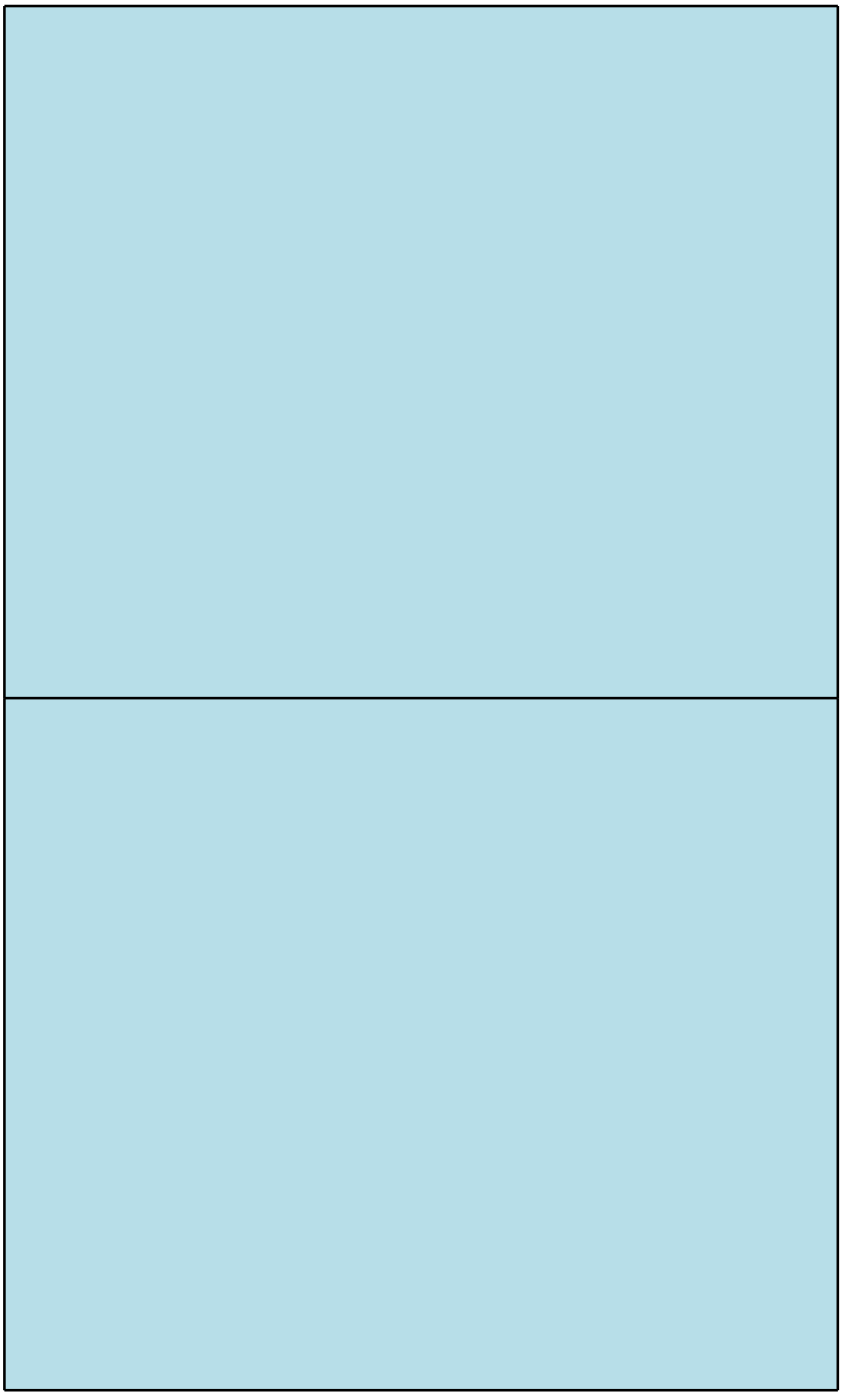
Kansainvälinen INFCIRC/908-aloite, johon Suomikin on liittynyt, tuottaa ja jakaa tietoa insider-uhkien torjuntaan liittyvistä menettelyistä. Insider-uhkien torjuntaa käsittelee myös IAEA: n ohje Preventive and Protective Measures Against Insider Threats

Pykälän 2 momentissa määrättäisiin sellaisten tehtävien tunnistamisesta, joissa yhdelle henkilölle syntyisi mahdollisuus tehdä vahinkoa tai mahdollisuus turvallisuutta vaarantaviin väärinkäytöksiin. Tällaisiin tehtäviin liittyvät riskit olisi hallittava. Väärinkäyttöä voisi olla esimerkiksi tietoturvakontrollien ohittaminen. Tällaisten tehtävien ja vastuualueiden eriyttämisellä pyritään ehkäisemään väärinkäytökset ja tietoturvakontrollien ohittamisen kannalta sellaiset työyhdistelmät, jotka voivat vaarantaa turvallisuuden. Kun sama henkilö tai tiimi on vastuussa sekä tehtävistä, joissa voidaan toteuttaa väärinkäytöksiä, että näiden tehtävien valvonnasta (tarkastus tai hyväksyntä), syntyy riski, että henkilö tai tiimi hyödyntää asemaansa väärin. Turvajärjestelyorganisaatiossa korostuu edellä 1 momentissa mainittu insider-uhka, koska organisaation henkilöstöllä yleensä on laajat pääsyoikeudet ja hyväksymisvaltuudet (mm. vieraiden tuontiin yms. liittyen). Tällöin työyhdistelmien tunnistaminen ja erottaminen auttaa ehkäisemään väärinkäytöksiä, minimoi virheitä, parantaa valvontakäytäntöjä ja lisää toimintojen luotettavuutta, mikä on tärkeää erityisesti arkaluontoisia tietoja käsittelevissä ja riskialttiissa ympäristöissä.

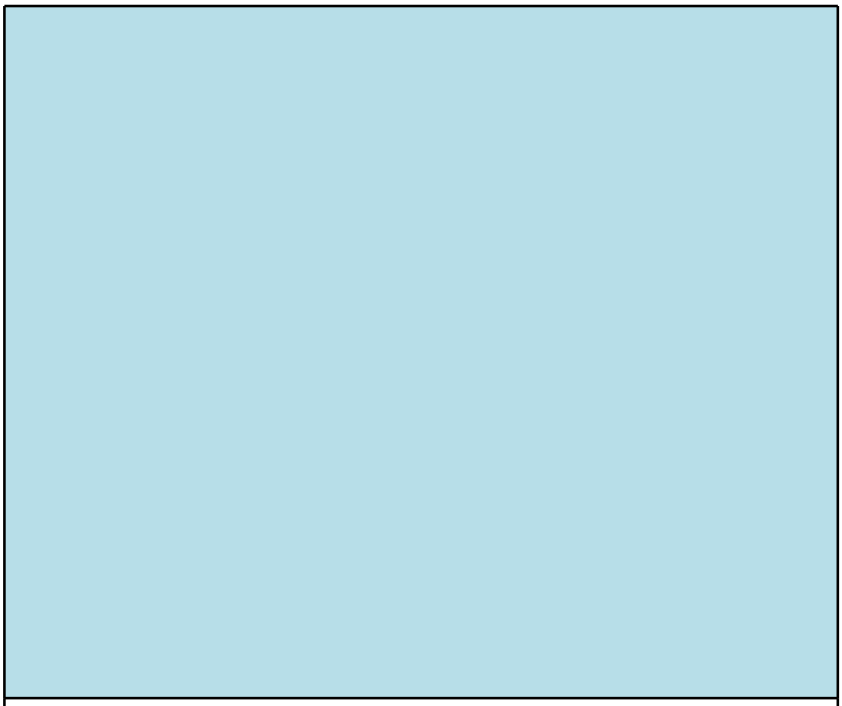
Mikäli tehtäviä ei pystytä eriyttämään, tulee ottaa käyttöön muita lisähallintakeinoja, kuten toiminnan teknistä valvontaa (esim. tapahtumien kirjaamista lokiin), kahden henkilön sääntö ja esihenkilöiden tekemää toiminnan valvontaa.



Pykälässä määrättäisiin tarvittavien fyysisten turvajärjestelyjen ja tietoturvallisuuden huomioon ottamisesta päätöksenteossa. Vaatimus perustuu siihen, että fyysiset turvajärjestelyt ja tietoturvallisuus ovat tiiviisti sidoksissa toisiinsa ja muihin turvallisuuden osa-alueisiin. Fyysiset turvajärjestelyt, kuten esimerkiksi henkilökunnan pääsynhallinta, voivat vaikuttaa digitaaliseen turvallisuuteen ja päinvastoin. Edistämällä integroituja ratkaisuja voidaan parantaa turvallisuusstrategioiden tehokkuutta. Fyysisten turvajärjestelyjen ja tietoturvallisuuden asiantuntijat tuovat päätöksentekoon omaa erityistä osaamistaan, joka on välttämätöntä nykyajan monimutkaisessa uhkaympäristössä. Heillä on syvällinen ymmärrys eri uhkista, haavoittuvuuksista ja alakohtaisista vaatimuksista, jotka voivat vaikuttaa organisaation toimintaan. Asiantuntijat tuovat käytännöllistä tietoa ja kokemusta, joka johtaa realistisiin ja toimiviin toimenpiteisiin. He voivat tunnistaa haasteita, joita päätökset saattavat aiheuttaa operatiivisesti, ja ehdottaa ratkaisuja, jotka optimoivat sekä turvallisuuden että toiminnallisuuden. Erityisesti muutosten tekeminen voi tuoda mukanaan uusia riskejä, jotka liittyvät sekä fyysisiin että tietoturvatekijöihin. Asiantuntijoiden mukanaolo varmistaa, että kaikkia mahdollisia riskejä arvioidaan ja käsitellään asianmukaisesti, mikä auttaa organisaatiota välttämään virheitä ja haitallisia seurauksia. Rajapintojen hallinta on erityisen keskeistä suunnittelussa ja muutosten hallinnassa.

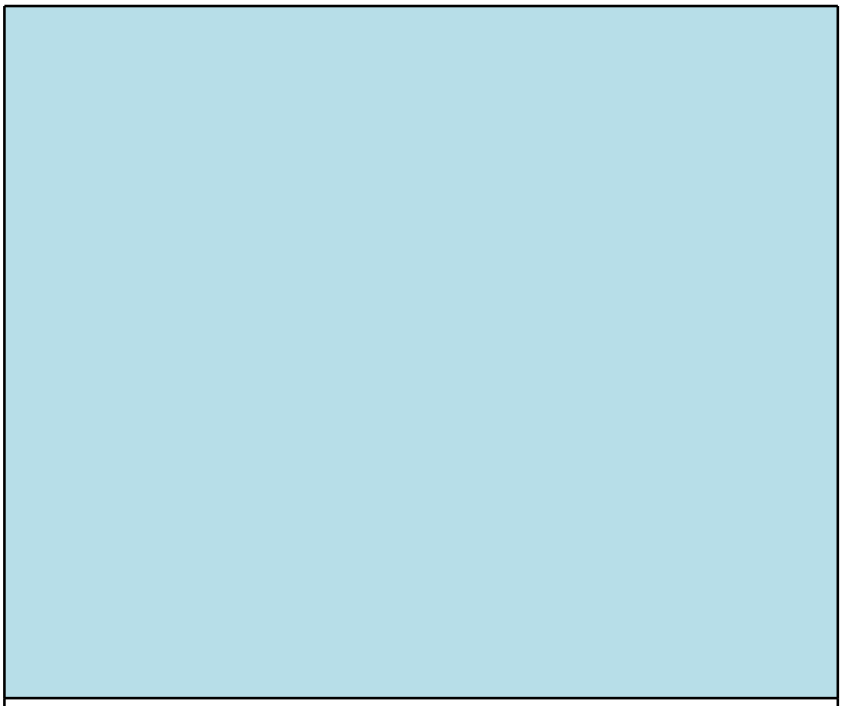


Pykälän 1 momentissa määrättäisiin turvajärjestelyihin liittyvien tehtävien, vastuiden ja valtuuksien määrittelemisestä (mukaan lukien tietoturvallisuuden parissa työskentelevät). Vaatimus perustuu siihen, että selkeä vastuunjako mahdollistaa tehokkaan riskienhallinnan, sillä silloin tiedetään, kuka vastaa mistäkin turvajärjestelytehtävästä. Tämä tarkoittaa, että riskit voidaan tunnistaa, arvioida ja hallita paremmin, mikä vähentää turvallisuusuhkien toteutumisen todennäköisyyttä. Turvahenkilöiden toimivaltuuksilla puututaan henkilöiden perusoikeuksiin, joten on keskeistä, että vastuut ja valtuudet ovat selkeästi kuvattu. Määräyksen 9 § 2 mom perusteluissa todettiin, että turvajärjestelyorganisaatiossa korostuu siinä esitetty insider-uhka koska organisaation henkilöstöllä yleensä on laajat pääsyoikeudet ja hyväksymisvaltuudet. Tämän takia luvanhaltijan olisi määriteltävä turvajärjestelyihin liittyvät tehtävät, niiden vastuut ja valtuudet sekä kuvattava ja dokumentoitava ne selkeästi. 9 § 2 mom mukaiset kriittiset työyhdistelmät ovat tällöin helpommin tunnistettavissa ja vältettävissä.
Pykälän 2 momentissa määrättäisiin turvajärjestelyjen henkilöstömitoituksesta. Vaatimus perustuu siihen, että suunnitteluperusteuhka asettaa kriteerit henkilöstömitoitukselle ja lisäksi mitoitukseen vaikuttaa ajantasainen tilannekuva. Ilman perusteellista analyysiä henkilöstömitoituksen tekeminen voi johtaa riittämättömiin tai ylimitoitettuihin resursseihin. Turvallisuustarpeet voivat muuttua ympäristön, toiminnan tai uhkien myötä. Ajantasaisen tilannekuvan ylläpitäminen auttaa organisaatiota reagoimaan muuttuviin olosuhteisiin. Tämä on tärkeää, koska nykytilanne saattaa erota alkuperäisestä suunnitelmasta, jolloin mukautuva henkilöstömitoitus on tarpeen. Kun henkilöstömitoitus perustuu ajantasaisiin tietoihin, organisaatio voi tehokkaasti minimoida riskit ja reagoida uhkiin ennaltaehkäisevästi. Henkilöstömitoitusta tulisi arvioida ennakoivasti koska turvahenkilöiden kouluttamiseen ja pätevyyksien hankkimiseen kuluu huomattavan pitkä aika.
Pykälän 3 momentissa määrättäisiin turvajärjestelyorganisaation henkilöstöstä ja johdosta. Vaatimus perustuu siihen, että YEL 155 § mukaan luvanhaltijan saa käyttää ainoastaan sellaista henkilöä turvahenkilönä, jolla on palvelussuhde luvanhaltijaan tai yksityisen turvallisuusalan elinkeinoluvanhaltijaan. Lisäksi YEL 160 § mukaan voimankäyttövälineiden on oltava luvanhaltijan tai sen lukuun toimivan hallinnoimia. Turvaohjesäännössä esitetään käytettävät voimankäyttövälineet ja turvajärjestelyorganisaation operatiivinen johtaminen ja toiminta, joiden tulee olla turvahenkilöiden palvelussuhteesta riippumatta luvanhaltijajohtoista. Vaatimus, jonka mukaan turvahenkilöiden on oltava luvanhaltijan operatiivisessa hallinnassa, liittyy siihen, että luvanhaltijalla on vastuu turvahenkilöiden toiminnasta ja organisaation turvallisuuspolitiikan, -käytäntöjen ja lainsäädännön noudattamisesta. Lisäksi kun henkilöstö on organisaation hallinnassa, voidaan reagoida nopeasti ja tehokkaasti muuttuviin tilanteisiin ja uhkiin.

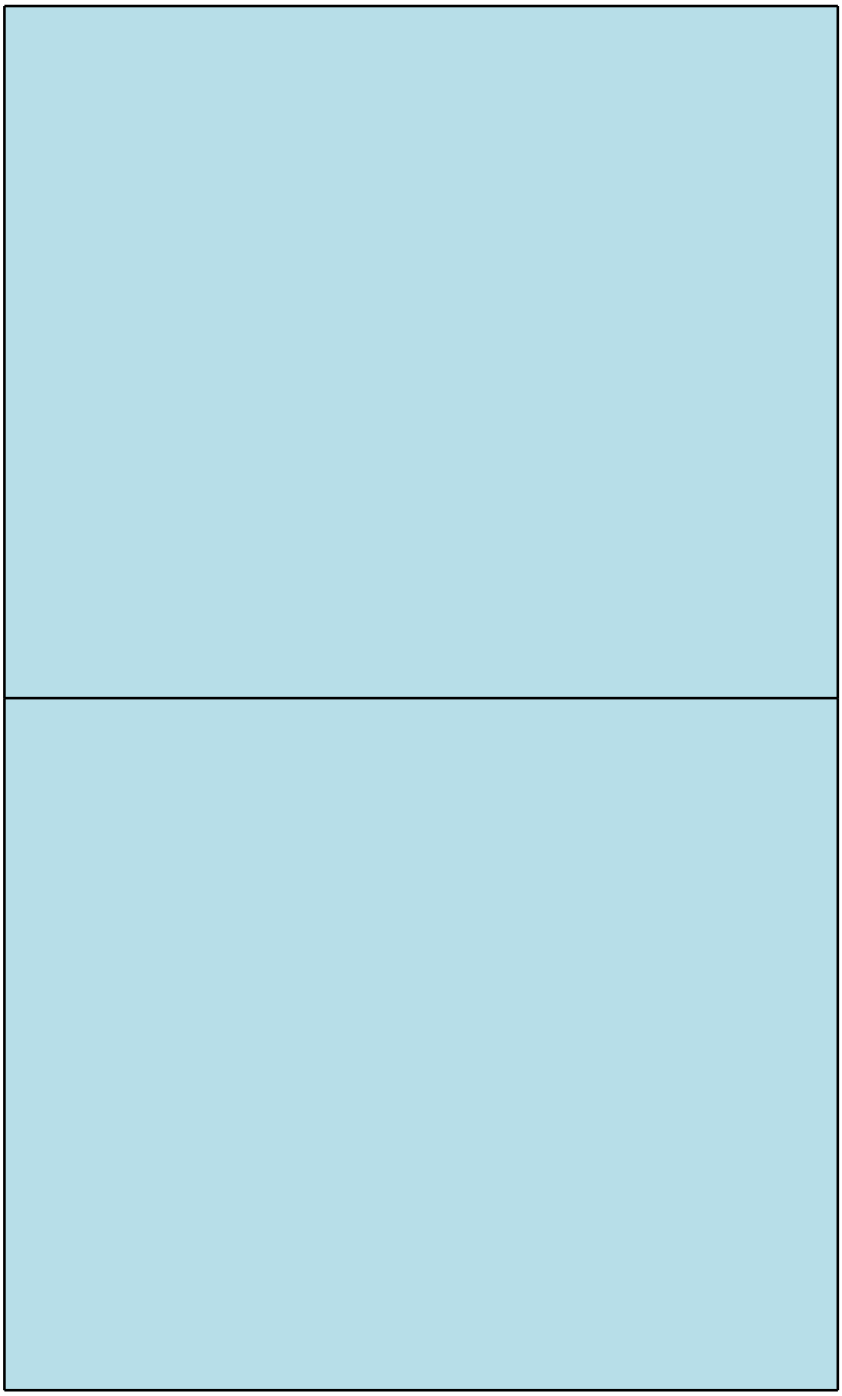


Pykälän 1 momentissa määrättäisiin turvahenkilöiden osaamisen kehittämiseen tarvittavista resursseista ja harjoitteluolosuhteista. Vaatimus perustuu siihen, että asianmukaiset koulutusresurssit, kuten kouluttajat, välineet ja harjoitteluympäristöt, ovat välttämättömiä, jotta turvahenkilöt voivat kehittää ja ylläpitää tarvittavaa ammattitaitoa. Turvahenkilöiden tehtävät ovat vaativia ja sisältävät suuren vastuun, ja vain riittävän koulutuksen kautta he kykenevät hoitamaan tehtävänsä vaikuttavasti. Harjoittelu asianmukaisissa olosuhteissa ja välineillä valmentaa turvahenkilöitä kohtaamaan todellisia tilanteita. Ampumarata on konkreettinen esimerkki eräästä tarvittavasta harjoitteluympäristöstä. Turvahenkilöt ovat osa tiimiä, joka toimii yhdessä monimutkaisissa tilanteissa. Oikeanlaiset harjoitteluolosuhteet mahdollistavat tiimityöskentelyn kehittämisen, mikä on tärkeää tehokkaan yhteistyön ja kommunikoinnin kannalta uhkatilanteissa.

Pykälän 2 momentissa määrättäisiin koko henkilöstöä koskevasta turvajärjestelykoulutuksesta ja osaamisen ylläpidosta. Vaatimus perustuu siihen, että luvanhaltijalla on velvollisuus noudattaa turvajärjestelymääräyksiä. Koulutuksen tarjoaminen koko henkilöstölle, kuten myös kuljetuksiin osallistuville (ml. kuljetuksen poliisisaattue), on olennainen osa tätä vaatimusta. Koulutus antaa henkilöstölle eväitä tunnistaa poikkeamia sekä tunnistaa, arvioida ja hallita toimintaan liittyviä riskejä. Ilman riittävää koulutusta on suurempi riski inhimillisiin virheisiin ja vahinkoihin. Työntekijät, jotka ovat saaneet asianmukaista koulutusta, ymmärtävät turvajärjestelyjen merkityksen ja ovat paremmin varustautuneita toimimaan oikealla tavalla poikkeamissa ja uhkatilanteissa. Kun organisaatio panostaa henkilöstön koulutukseen, se viestii arvoistaan ja asenteistaan sekä johdon sitoutumisesta turvajärjestelyihin, mikä voi vaikuttaa koko organisaation toimintaan ja toimintakulttuuriin.



Pykälässä määrättäisiin turvahenkilön asusta ja siinä käytettävistä tunnisteista. Turvahenkilön asusta säädetään ydinenergialakiluonnoksen 156 §:ssä, ja sen mukaan STUK voi antaa tarkempia määräyksiä turvahenkilön asusta ja siinä käytettävistä merkeistä. Turvahenkilön asua ja siinä käytettäviä merkkejä ja tunnisteita koskevat vaatimukset on tarkoitus pitää ennallaan, eli kuten määräyksessä STUK Y/3/2020. Ydinlaitoksella työskentelevän tai siellä asioivan on kyettävä tunnistamaan turvahenkilö tämän käyttämän asun ja siihen tehtyjen merkintöjen perusteella luotettavasti. Sekaantumisvaaraa turvallisuusviranomaisten käyttämiin asuihin ei saa olla. Asialla on merkitystä sekä turvahenkilön että tämän toimenpiteiden kohteeksi joutuneen henkilön oikeusturvan kannalta. Turvahenkilö käyttää tehtävässään merkittäviä, ydinenergialaissa säädettyjä toimivaltuuksia, minkä vuoksi tunnistaminen on tarpeen. Turvahenkilöä koskevissa merkinnöissä on käytetty sekä suomen että ruotsin kieltä. Koska ydinlaitoksilla työskentelee merkittävä määrä (erityisesti vuosihuoltojen aikana) muunkielisiä työntekijöitä, merkinnöissä käytetään myös englannin kieltä. Tilanpuutteen vuoksi selkämykseen tehtävissä merkinnöissä käytetään käytännössä vain kaikkien ymmärtämää englannin kieltä. Liitteen 1 mukaisten merkkien tarkkaa värikoodia ei ole määritelty, vaan käytettävän työasun perusteella merkin taustaväri tai fontin väri voivat hieman vaihdella tunnistettavuuden vaarantumatta. Taulukossa 1 on määritelty työasun ja siihen kuuluvien vaatekappaleiden pääluokat. Esimerkiksi takin sijaan käytössä voi olla joissakin tehtävissä varuste- tai heijastinliivin tyyppinen vaatekappale (pääluokka: takki). Näihin on tehtävä pääluokan mukaiset merkinnät.



Pykälän 1 momentissa määrättäisiin, että ydinlaitokselle on määriteltävä sisäkkäiset fyysiset turvajärjestelyvyöhykkeet ottaen huomioon uhkan ennalta ehkäisy, havaitseminen, viivytys ja vaste sekä vyöhykkeiden rajapintojen tasapainoinen suojaus. Tasapainoisella suojauksella tarkoitetaan sitä, että rajapinta on kokonaisuudessaan yhtä vahva, eikä siinä ole heikkoja kohtia. Fyysiset turvajärjestelyvyöhykkeet ovat osa syvyyssuuntaista puolustusta. Vyöhykkeiden rajapinnoilla ja vyöhykkeiden sisällä olevilla turvajärjestelyillä hallinnoidaan luvallista pääsyä tiloihin, materiaaleihin, järjestelmiin ja tietoihin, havaitaan ja viivytetään luvatonta pääsyä ja järjestetään poikkeaman tai uhkatilanteen mukainen vaste. Vyöhykkeet määritellään niiden sisälle suojattavien rakenteiden, järjestelmien, laitteiden, materiaalien ja tietojen turvallisuusmerkityksen mukaisesti. Vyöhykkeiden sisällä voi olla tarkoituksenmukaista määrittää erillisiä pääsynhallintakohteita. Koska insider-henkilöllä on määritelmällisesti luvallinen pääsy paikkaan tai tietoon, vyöhykkeistämisen ohella insider-uhan torjunta edellyttää erillisiä toimenpiteitä. Fyysiset turvajärjestelyvyöhykkeet perustuvat osin IAEA: n ohjeeseen Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (NSS 13).

Pykälän 2 momentissa neljä fyysistä turvajärjestelyvyöhykettä lueteltaisiin uloimmasta sisimpään: 1) sisäministeriön liikkumis- ja oleskelurajoituksista annetun asetuksen (1104/2013) liitteessä 4 määritelty liikkumis- ja oleskelurajoitusalue, 2) laitosalue, 3) suojattu alue ja 4) vitaalinen alue, ja annettaisiin niille lyhyet kuvaukset. Mikäli se olisi riskitietoisesti, turvallisuusperusteisesti perusteltua, vyöhykkeet 1) ja 2) voisivat olla käytännössä samat ja vyöhykkeiden 3) ja 4) rajapinta voisi olla osittain sama. Liikkumis- ja oleskelurajoitusalueesta käytetään joskus nimitystä voimalaitosalue.

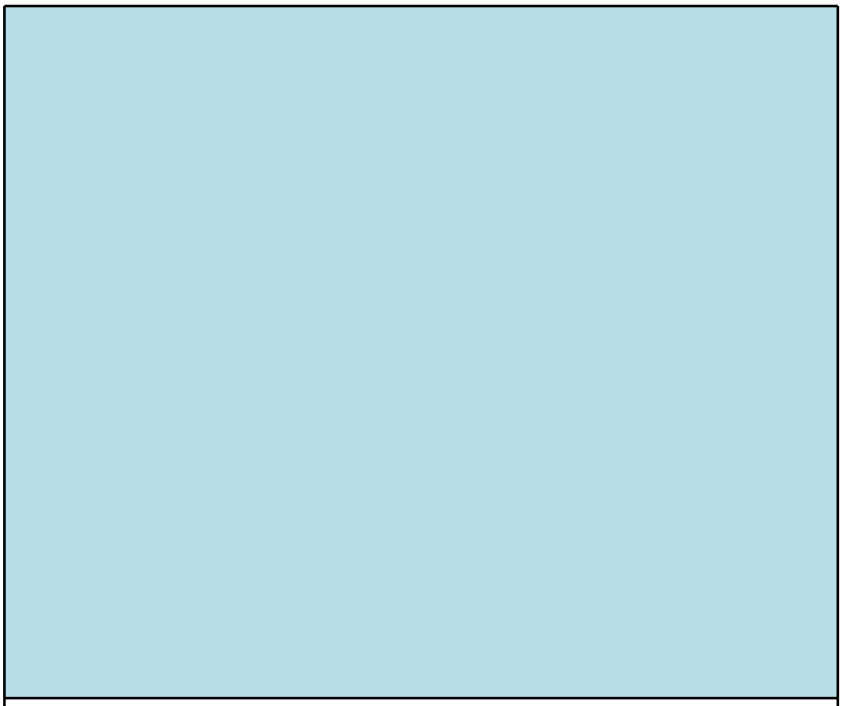
Pykälän 3 momentissa määrättäisiin suojattavien tietoverkkojen jakamisesta tietoturvavyöhykkeisiin. Tietoverkkojen jakaminen eri vyöhykkeisiin riskiarvion perusteella on olennainen osa tietoturvan ja tietoturvariskienhallinnan kokonaisuutta. Tämä käytäntö auttaa suojaamaan tietoja ja vähentämään hyökkäyksistä ja poikkeamista aiheutuvia vahinkoja. Tietoverkkojen vyöhykkeistämisessä otetaan huomioon uhkan ennalta ehkäisy, havaitseminen, viivytys ja vaste sekä vyöhykkeiden rajapintojen tasapainoinen suojaus. Tietoverkkojen vyöhykkeet ovat osa syvyyssuuntaista puolustusta. Jakamalla tietoverkot vyöhykkeisiin minimoidaan riski siitä, että hyökkäys tai poikkeama yhdessä osassa verkkoa leviää kaikkialle. Riskiarvioinnin perusteella tehdyt jaot mahdollistavat, että kriittiset kohteet voidaan sijoittaa tiukimmin suojatulle vyöhykkeelle. Jos hyökkäys esimerkiksi kohdistuu alhaisemman turvallisuustason vyöhykkeellä olevaan kohteeseen, se ei pääse ilman vyöhykerajan murtamista etenemään korkean turvallisuustason vyöhykkeelle.

Tietoverkon looginen eriyttäminen tarkoittaa tietoverkon segmentointia ja erottelua ohjelmallisesti ja hallinnollisesti, ilman fyysistä erottamista erillisiin laitteisiin tai kaapeleihin. Tyypillisiä loogisen eriyttämisen keinoja ovat esimerkiksi virtuaaliset lähiverkot, joissa sama fyysinen verkko on jaettu useisiin loogisiin langattomiin verkkoihin, sekä palomuurit ja reitityssäännöt, joilla estetään tai sallitaan liikenne verkon eri segmenttien välillä.

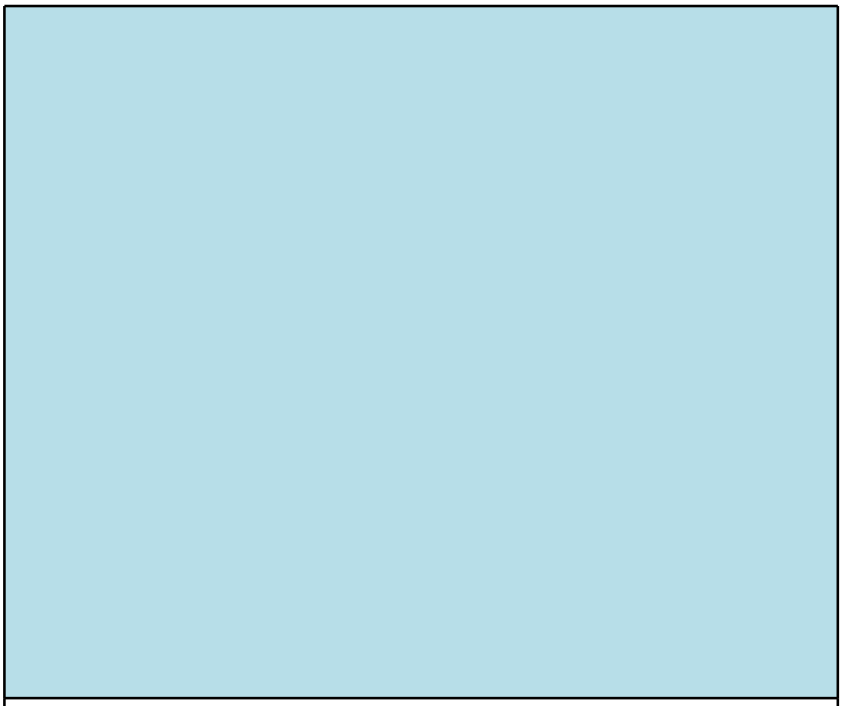
Tietoverkon fyysinen eristäminen tarkoittaa tietoverkkojen täydellistä irrottamista toisistaan fyysisellä tasolla, niin että ne eivät jaa yhteisiä verkkolaitteita, kaapeleita, reitittimiä tai muuta infrastruktuuria. Fyysisesti eristetyt verkot ovat täysin itsenäisiä ja toimivat ilman yhteyttä muihin verkkoihin, kuten internettiin tai yrityksen sisäiseen verkkoon. Tyypillisesti yrityksen toimistoverkko ja teollisuuden ohjausjärjestelmien verkko ovat täysin erillään.

Pykälän 4 momentissa määrättäisiin tärkeisiin tietojärjestelmiin liittyvästä tietoliikenteen yksisuuntaistamisesta ja ulkopuolisten yhteyksien rajoittamisesta. Tärkeiden kohteiden kohdalla tietoliikenteen fyysisen yksisuuntaistamisen ja ulkopuolisten yhteyksien rajoittamisen ja estämisen tarkoituksena on minimoida hyökkäyspinta-alaa ja estää kriittisten järjestelmien vaarantumista. Hyökkäyspinta-alalla tarkoitetaan kaikkia mahdollisia kohtia, kanavia ja mekanismeja, joiden kautta hyökkääjä voi päästä käsiksi kohteeseen. Hyökkäyspinta-alan pienentäminen on erityisen tärkeää kohteissa, joissa pienikin tietoturvapoikkeama voi aiheuttaa vakavia seuraamuksia.

Fyysinen yksisuuntaistaminen tarkoittaa, että tietoliikenne kulkee vain yhteen suuntaan, esimerkiksi kriittisestä kohteesta ulospäin, mutta ei sisäänpäin. Tämä estää hyökkääjiä käyttämästä ulkopuolisia yhteyksiä kriittisten kohteiden manipulointiin tai vahingoittamiseen. Fyysiseen yksisuuntaistamiseen käytetään esimerkiksi yksisuuntaista tiedonsiirtolaitetta (data diodi) tai yksisuuntaista valokuituyhteyttä. Palomuureilla tai muilla loogisen eriyttämisen keinoilla ei saavuteta fyysistä yksisuuntaistamista.

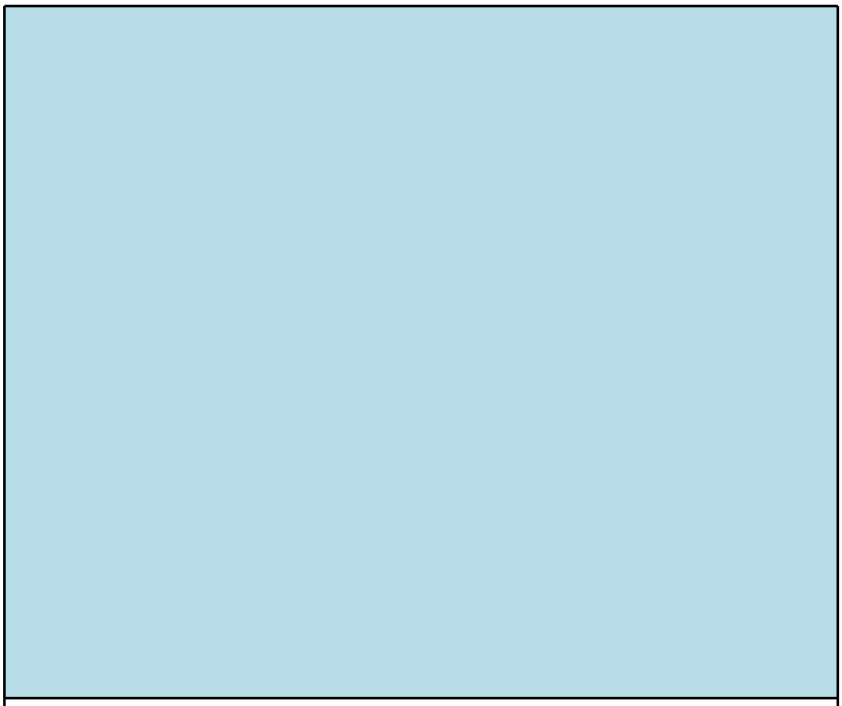


Pykälän 1 momentissa viitattaisiin määräyksen liitteeseen. Määräyksen liitteessä esitettäisiin vaatimukset ydinlaitoksen alueen merkitsemisestä sen lisäksi, mitä liikkumis- ja oleskelurajoituksista annetussa sisäministeriön asetuksen (1104/2013) 4 ja 5 §:ssä säädetään. Vaatimusten tarkoituksena on varmistaa, että ydinlaitoksen liikkumis- ja oleskelurajoitusalue on merkitty selkeästi, jotta alueelle ei voisi päätyä vahingossa rajoituksesta tietämättä. Vaatimuksella tavoitellaan myös yhdenmukaisuutta ydinlaitosten välillä. Merkintä kattaa maa- ja vesialueet mahdollisuuksien mukaan.



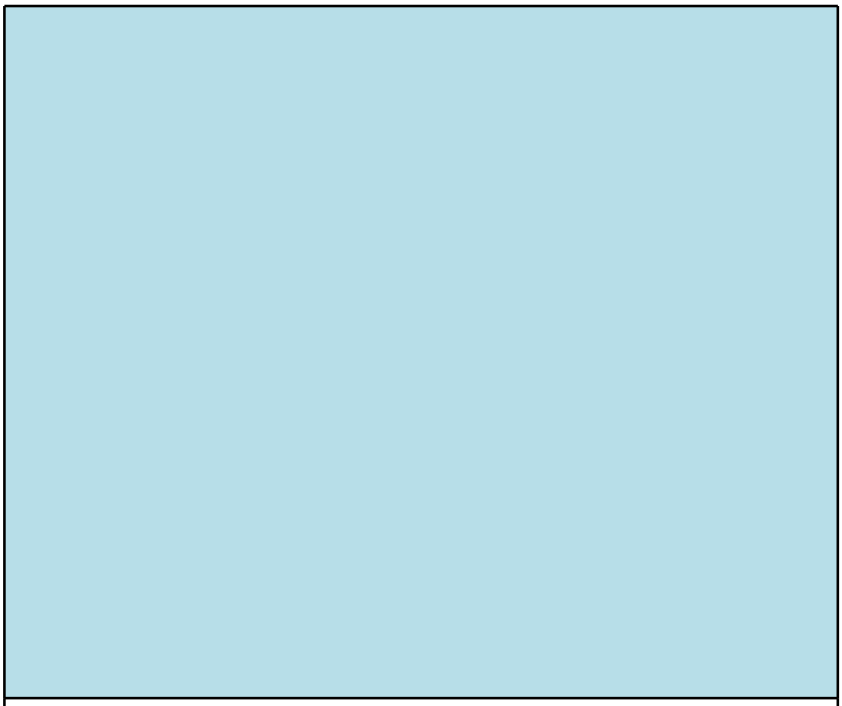
Pykälän 1 momentissa laitosalueen rajaamiseksi vaadittaisiin kaksoiseste, sen välinen riittävä eristysvyöhyke ja niiden molemmin puolin olevat alueet toisistaan riippumattomin valvontajärjestelmin sekä ajoneuvoeste. Kaksoisesteellä tarkoitetaan esimerkiksi kaksoisaitaa. Kaksoisesteen eristysvyöhykkeen ja niiden molemmin puolin olevien alueiden tarkoituksena on varmistaa luvattoman tunkeutumisen havaitseminen ja poikkeaman tai uhkatilanteen arviointi siten, että tarvittava vaste voidaan toteuttaa vaikuttavasti. Ajoneuvoesteen tarkoituksena on torjua ajoneuvolla tai siinä olevilla vaarallisilla esineillä aiheutettava uhka. Ajoneuvoesteen etäisyys kaksoisesteestä ja ajoneuvoesteen ominaisuudet määritetään riskitietoisesti ja DBT:n mukaisesti.

Pykälän 2 momentissa edellytettäisiin laitosalueelle johtavien kulkuaukkojen ja liikennereittien määrän rajaamista ja kulkujen toteuttamista yksitellen. Kulkuaukkojen ja liikennereittien lukumäärän rajaamisella optimoidaan liikenteen ja kulun valvonnan edellytyksiä ottaen huomioon myös hätäpoistumismahdollisuudet. Yksitellen tapahtuvalla kululla estetään tarkastamattomien ajoneuvojen tai henkilöiden kulkua tarkastettujen vanavedessä.



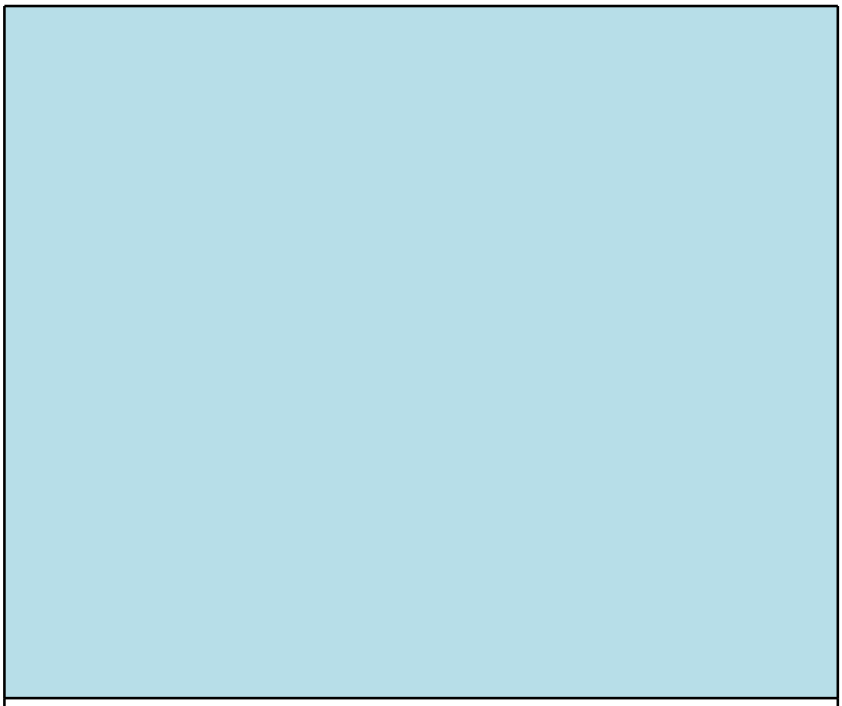
Pykälän 1 momentissa edellytettäisiin, että suojatut ja vitaaliset alueet määritellään riskitietoisesti laitoksen ominaisuuksien ja toiminnan perusteella. Syvyyssuuntaisen puolustuksen periaatteen mukaisesti turvallisuusmerkitykseltään tärkeimmät kohteet sijaitsevat vitaalisella alueella, joka sijaitsee suojatun alueen sisällä. Vitaalisen alueen määrittelyn menettely edellytettäisiin toimitettavaksi, jotta STUK voisi arvioida määrittelyn kattavuutta, kuten safety-turvallisuuden, security-turvallisuuden ja ydinmateriaalivalvonnan näkökulmien huomioon ottamista. Vitaalisten alueiden määrittelyä käsitellään asiakirjassa IAEA NSS 48-T (Identification and Categorization of Sabotage Targets, and Identification of Vital Areas at Nuclear Facilities).

Pykälän 2 momentissa edellytettäisiin, että suunnittelussa otettaisiin huomioon vitaalisella alueella liikkumisen ja oleskelun rajoitus turvallisuusperusteiseen minimiin. Tällä tarkoitetaan, että ydinlaitos suunnitellaan siten, ettei vitaaliselle alueelle ole tarvetta sijoittaa järjestelmiä ja laitteita, jotka eivät sinne turvallisuusmerkityksensä puolesta kuulu, jotta esim. niiden huoltamisesta ja seurannasta ei aiheudu turvallisuuden kannalta tarpeetonta kulkua ja oleskelua vitaalisella alueella.



Pykälän 1 momentissa edellytettäisiin valvontaa teknisin menetelmin ja partioimalla. Teknisiä turvavalvontajärjestelmiä ja -menetelmiä käytetään siinä määrin, kun se on käytännöllisin toimenpitein mahdollista. Henkilöiden tekemät havainnot eivät korvaa teknisiä menettelyjä, vaan täydentävät niitä. Toki myös partioinnissa käytetään teknisiä menetelmiä, kuten drooneja, lämpökameroita ja pimeänäkölaitteita.

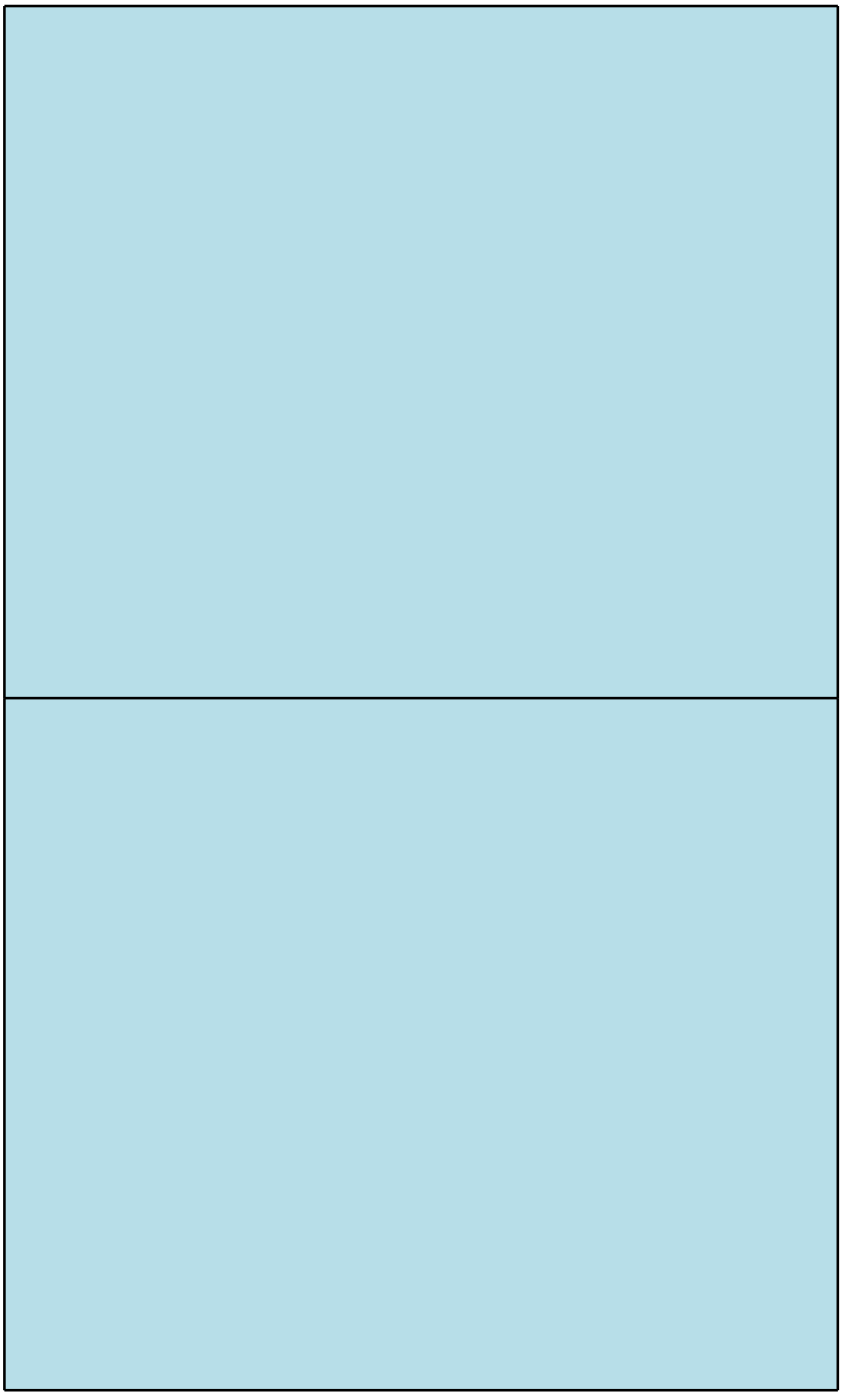
Pykälän 2 momentissa turvajärjestelyvyöhykkeillä edellytettäisiin turvavalvontajärjestelmiä, jotka kokonaisuutena täyttäisivät momentissa luetellut vaatimukset. Turvavalvontajärjestelmien kokonaisuutta koskevien vaatimusten tarkoituksena on, että poikkeamat ja uhkatilanteet pystytään havaitsemaan ja arvioimaan oikea-aikaisesti, jotta vaste voidaan toteuttaa vaikuttavasti. Tapahtumatallenteiden avulla pyritään turvaamaan tapahtumien selvittämisen ja tutkinnan, ml. viranomaistutkinnan, edellytykset.
Pykälän 3 momentissa edellytettäisiin, että turvavalvontajärjestelmien, kuten kameravalvontajärjestelmän, olisi oltava mahdollisimman katveettomia laitosalueella. Turvavalvontajärjestelmien katveettomuudella pyritään tasapainoiseen havaitsemiseen ja oikea-aikaiseen tilanteen arviointiin.



Pykälän 1 momentissa määrättäisiin tietoverkkojen ja -järjestelmien normaalin toiminnan määrittämisestä ja poikkeavan toiminnan havaitsemisesta sekä sen kiistattoman tutkinnan mahdollistamisesta. Tietoverkkojen ja -järjestelmien normaalitila on ymmärrettävä, jotta mahdolliset poikkeamat voidaan ylipäätään havaita. Kun poikkeamat havaitaan, niihin on pystyttävä reagoimaan oikea-aikaisesti ja vaikuttavasti.

Tietoverkoista ja -järjestelmistä on kerättävä tietoa poikkeamien havaitsemiseksi ja luotettavan tutkinnan mahdollistamiseksi. Kiistattomat ja kattavat loki- sekä muut valvonnan tukena olevat tiedot ovat todisteita poikkeamien tutkinnassa, mikä helpottaa syiden selvittämistä ja vastuullisten tunnistamista koko tapahtumaketjun elinkaaren ajalta. Kiistattomat ja kattavat tiedot ovat erityisen merkityksellisiä, jos poikkeamat johtavat juridisiin toimiin, kuten riitatilanteisiin ja rikostutkintaan.

Pykälän 2 momentissa määrättäisiin tietojen riittävästä suojaamisesta. Tietojen eheyden ja saatavuuden varmistaminen sekä tietojen luvattoman käsittelyn estäminen ovat keskeisiä periaatteita tietoturvallisuudelle. Tietojen tulee olla saatavilla silloin kun niitä tarvitaan, sillä niiden puuttuminen voi keskeyttää kriittiset prosessit ja toiminnan. Tietojen virheettömyys ja oikeellisuus takaavat, että toiminta ja päätöksenteko perustuu luotettavaan ja ehyeen tietoon. Ilman asianmukaisia menettelyjä tiedot voivat joutua sisäisten tai ulkoisten tahojen luvattomaan käyttöön, jolloin tietojen luvaton käsittely voi johtaa tietovuotoihin, väärinkäytöksiin ja jopa toiminnan ja turvallisuuden vaarantumiseen.



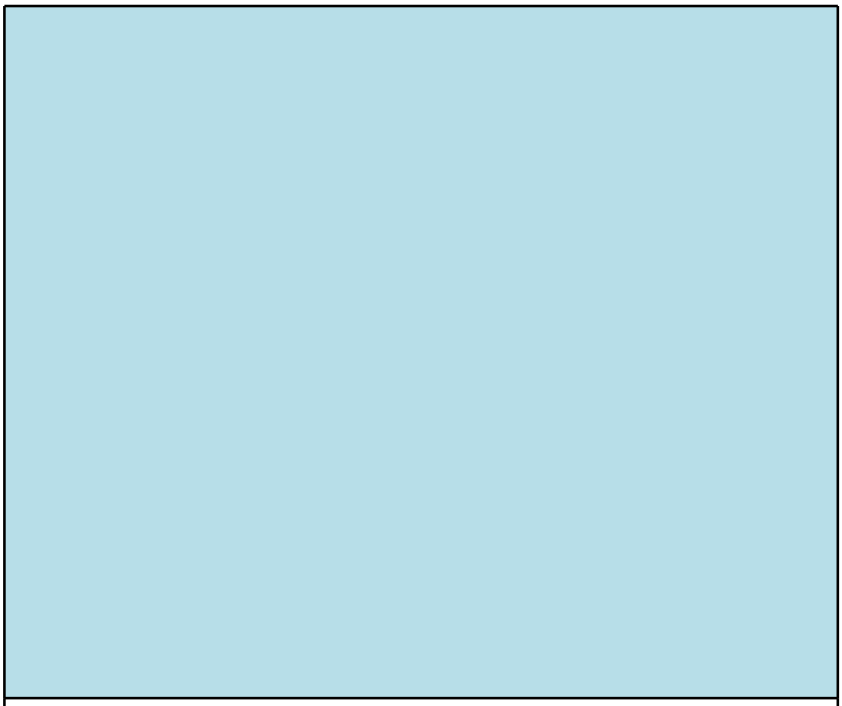
Pykälän 1 momentissa edellytettäisiin, että luvanhaltija varmistaa riittävän viivytyksen rakenteellisin ja teknisin järjestelyin. Vaatimuksen tarkoitus on, että asia tulee huomioiduksi täysimääräisesti laitoksen layoutin, rakenteiden sekä toiminnan ja tietoturvallisuuden suunnittelussa nimenomaan rakenteellisten ratkaisujen muodossa, jotta saadaan aikaan viivettä tukemaan turvaorganisaation ja viranomaisten operatiivisen vasteen edellytyksiä ja vaikuttavuutta.

Pykälän 2 momentissa edellytettäisiin, että turvajärjestelyjen kannalta merkitykselliset järjestelmät on erotettava ja suojattava rakenteellisesti ja teknisesti. Suojauksella tarkoitetaan esim. aitauksia, rakennuksia, huonetiloja, suojakaappeja ja -koteloita, lukituksia, sinetöintejä, murto- ja sabotaasihälytyksiä ja suojauksia sähkömagneettista häirintää, vakoilua tai kyberuhkia vastaan. Teknisiä menettelyjä ovat myös mm. tietoliikenneyhteyden häiriöstä tai sähkön menetyksestä aiheutuvat hälytykset ja järjestelmien ja laitteiden itsediagnostiikkahälytykset. Rakenteellisella erottamisella tarkoitetaan esimerkiksi riittävää etäisyyttä. Tietyt turvajärjestelyjärjestelmät ovat itsessään suojaavia rakenteita.

Pykälän 1 momentissa määrättäisiin, että henkilöitä, ajoneuvoja ja tavaraliikennettä on valvottava ydinlaitokselle sisään ja sieltä ulos mentäessä.

Pykälän 2 momentissa määrättäisiin, että turvallisuudelle haitallisten ja vaarallisten esineiden pääsy ydinlaitokseen ja kuljetukseen on estettävä ja että ydinaineiden, ydinjätteiden ja muiden radioaktiivisten aineiden vienti laitokseen tai laitoksesta on estettävä. Tarkoituksena on estää vaarallisten esineiden vienti ydinlaitokseen tai kuljetukseen sekä torjua anastusuhkaa. Sanaa ”luvaton” käytetään yleiskielen merkityksessä, eikä sillä viitata tiettyyn lupamenettelyyn.

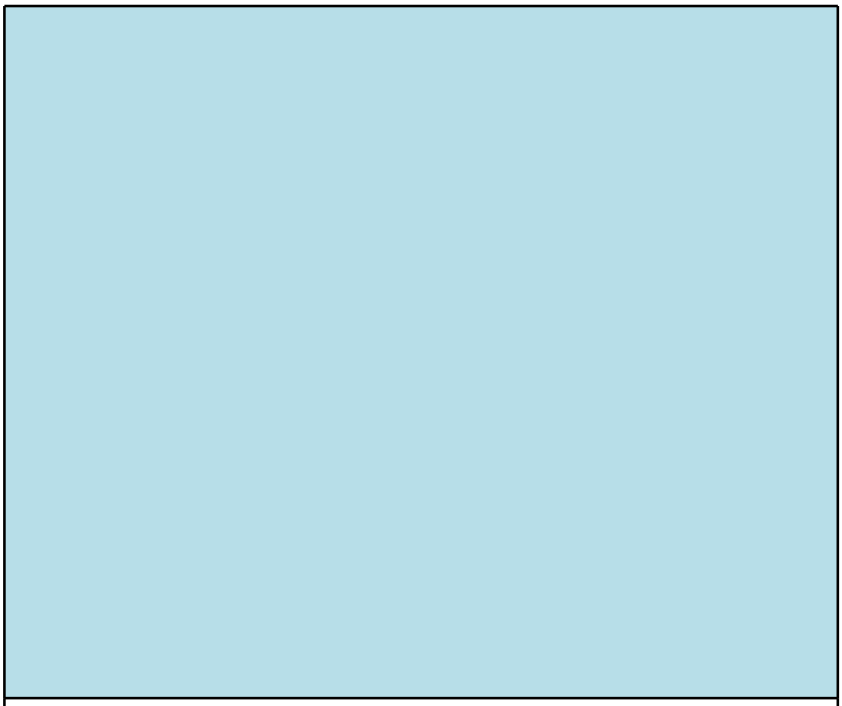
Pykälän 3 momentissa edellytettäisiin, että ajoneuvojen turvallisuustarkastus suoritetaan ns. sulutuksessa, mikä yleensä edellyttää kiinni olevaa porttia sekä ajoneuvon edessä että takana. Luvanhaltija voi tehdä ajoneuvotarkastuksia myös laitosalueelta ulos menevälle liikenteelle. Olisi siis estettävä tarkastuksen kohteena olevan vielä tarkastamattoman ajoneuvon sisään- tai ulosajo sekä muiden tarkastamattomien ajoneuvojen tai henkilöiden kulku kulkuaukosta samaan aikaan.



Pykälän 1 momentissa edellytettäisiin, että pääsyoikeudettomien henkilöiden pääsy ydinlaitokseen tai kuljetukseen on estettävä ja että ydinlaitoksessa asioivien ja kuljetukseen osallistuvien henkilöllisyydestä on varmistuttava. Kyseessä on kulun rajoittamista ja valvontaa käsittävä perusvaatimus, jolla on myös safety-turvallisuuteen liittyvä vaikutus, jotta esim. onnettomuustilanteissa tiedetään, keitä paikalla on, eikä paikalla oleskella tarpeettomasti.

Pykälän 2 momentissa määrättäisiin laitosalueelle tapahtuvaan henkilökulkuun ja turvallisuustarkastuksiin liittyvistä menettelyistä, joilla varmistetaan kulku yksitellen ja ehkäistään vaarallisten esineiden vientiä laitokseen sekä radioaktiivisten aineiden vientiä pois laitoksesta. Turvallisuustarkastajaa itseään ei koske vaatimus kohdassa 4), joka muiden kohdalla edellyttää, että turvallisuustarkastetut ja -tarkastamattomat henkilöt eivät kohtaa toisiaan. Muut vaatimuskohdat koskevat myös turvahenkilöitä. Vaatimuskohdan 4) tarkoituksena on estää tarkastamatonta henkilöä välttämästä vaarallisen esineen havaitsemista luovuttamalla se jo tarkastetulle. Käytännössä vaatimuksen voi täyttää linjastotyyppisillä tarkastuspisteillä, joilla edetään yksi kerrallaan yhteen suuntaan.

Pykälän 3 momentissa edellytettäisiin, että liikkuminen ydinlaitoksessa ja kuljetuksen välittömässä läheisyydessä on oltava tarkoituksen mukaan rajoitettua ja valvottua. Kyseessä on kulun rajoittamista ja valvontaa käsittävä perusvaatimus, joka liittyy niin outsider- kuin insider-uhankin torjuntaan ja jolla on myös safety-turvallisuuteen liittyvä vaikutus, jotta säteilylähteiden läheisyydessä ei oleskella tarpeettomasti. Liikkumista rajoitetaan tehtäväperusteisesti ja valvotaan, että rajoituksia noudatetaan.
Pykälän 4 momentissa edellytettäisiin, että henkilöiden liikkumista sekä tavaroiden säilytystä ja siirtoa on valvottava, ja muita kuin itsenäiseen liikkumiseen hyväksyttyjen henkilöitä on saatettava. Vaatimuksen tarkoitus on varmistaa, että liikkuminen, säilytys ja siirto tapahtuu hyväksytysti ja turvallisesti. Muiden kuin itsenäiseen kulkuun luvitettujen henkilöiden lisäksi pääsy voi olla tarpeen henkilöille, joille ei ole tehty samantasoisia taustaselvityksiä ja muita luotettavuusselvityksiä, joten heidän on liikuttava saatettuina. Tässä yhteydessä valvonnalla ei tarkoiteta yksittäisten henkilöiden ja tavaroiden jatkuvaa 100 %:sta seurantaa.
Pykälän 4 momentissa edellytettäisiin, että poistumistiet on toteutettava rakenteellisesti ja teknisesti siten, että voidaan poistua vaara-alueelta turvallisesti, mutta että hätäpoistumisteitä ei voi käyttää tunkeutumisreitteinä. Tarkoituksena on ehkäistä tilanne, jossa vaikkapa onnettomuuden tai aiheettoman hälytyksen aiheuttamalla saataisiin aikaan tilanne, jossa hätäpoistumisteiden kautta voisi ilman kulkuoikeutta päästä sisään jollekin turvajärjestelyvyöhykkeelle tai sen sisällä olevaan tilaan. Vaatimuksen tarkoituksena on myös suojata laitoksen turvallisuusjärjestelmien rinnakkaisuusperiaatetta (redundanssia).



Pykälän 1 momentissa määrättäisiin pääsynhallinnasta turvallisuuden kannalta keskeisiin tietoihin ja muihin pääsynhallintaa vaativiin kohteisiin. Luvanhaltijan olisi hallittava, todennettava ja valvottava pääsyä fyysisiin kohteisiin, tietojärjestelmiin ja tietoon turvallisuusmerkityksen perusteella. Hallinta koskisi henkilöitä ja ohjelmistoja. Vaatimus tarkentaisi pääsyn rajoittamisen, hallinnan ja valvonnan periaatetta.

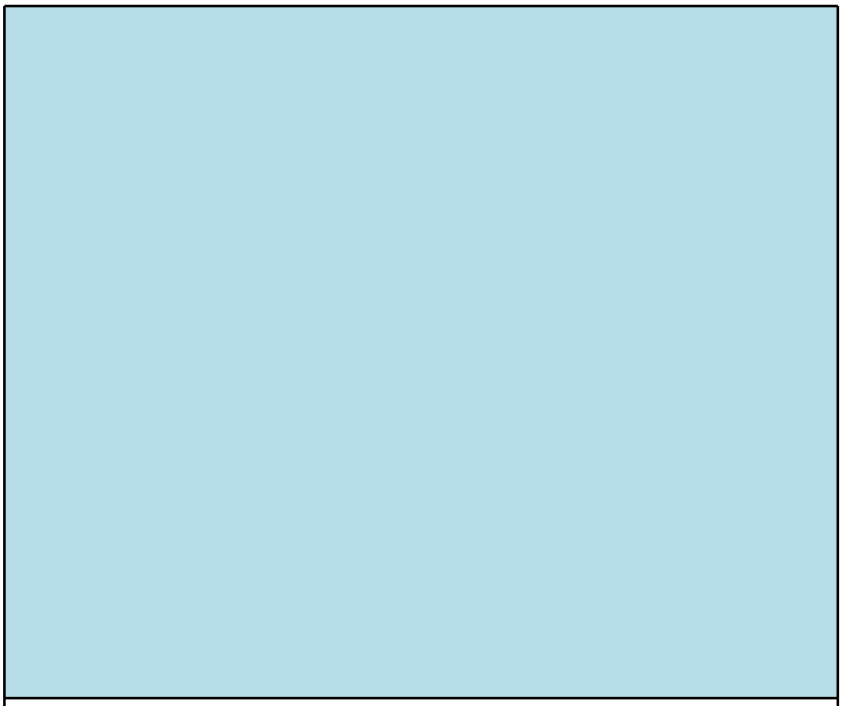
Pykälän 2 momentissa määrättäisiin pääsynhallinnan tavoitteeksi vain sallittujen, turvalliseksi todettujen järjestelmien, rakenteiden, laitteiden ja ohjelmistojen hyväksytty, luvallinen ja valvottu käyttö. Vaatimuksessa on kyse fyysisten turvajärjestelyjen ja tietoturvallisuuden toimenpiteiden yhdistämisestä rajapinnan hallinnassa.

Pykälän 3 momentissa määrättäisiin käyttöoikeuksien rajauksesta pienimpien oikeuksien periaatteen mukaisesti ja tehtäväperusteisesti. Tällä tarkoitetaan sitä, että jokaisella käyttäjällä ja käyttäjätunnuksella olisi vain tehtävän kannalta välttämättömät vähimmäisoikeudet. Työtehtävää ei tulisi suorittaa sen vaatimia laajemmilla oikeuksilla. Käyttäjätunnusten ja valtuuksien laajuudet tulisi ottaa huomioon järjestelmien, sovellusten ja tietoverkkojen toiminnallisissa määrittelyissä.

Käyttäjätunnuksien ja salasanojen hallintamenettelyjen tulisi kattaa käyttäjätunnusten ja salasanojen koko elinkaari. Tähän kuuluu esimerkiksi henkilökohtaisten, koneellisten sekä yhteiskäyttöisten käyttäjätunnusten ja salasanojen hyväksyntä, luominen, jakelu, käyttö, tarkastaminen ja päivittäminen. Käyttäjätunnuksilla ja salasanoilla tulisi olla omistaja, joka vastaa niiden asianmukaisesta käytöstä ja hallinnasta. Yhteiskäyttötunnuksia tulisi käyttää vain erityistapauksissa, joissa yksilöllisiä tunnuksia ei voida hyödyntää.

Käyttöoikeudet tulisi tarkastaa säännöllisin määräajoin, esimerkiksi vuosittain tai puolivuosittain. Pääkäyttäjävaltuudet tulisi tarkastaa useammin kuin peruskäyttäjien oikeudet. Pääsy- ja käyttöoikeudet sekä niihin tehdyt muutokset ja tarkistukset tulisi dokumentoida. Jos käyttäjän rooli tai vastuut muuttuvat, niihin liittyvät oikeudet tulisi päivittää vastaavasti.

Pykälän 4 momentissa edellytettäisiin henkilöiden tunnistukseen käytettävän tarkoitukseen soveltuvia pääsynhallintajärjestelmiä yhdessä luotettavan tunnistusteknologian kanssa. Luotettava ja tarkoitukseen soveltuva pääsynhallinta sekä tunnistusteknologia varmistavat, että vain valtuutetut henkilöt pääsevät heille hyväksyttyihin kohteisiin. Tarkoituksena on myös teknologian kehityksen hyödyntäminen pääsynhallinnan ylläpidossa ja parantamisessa.

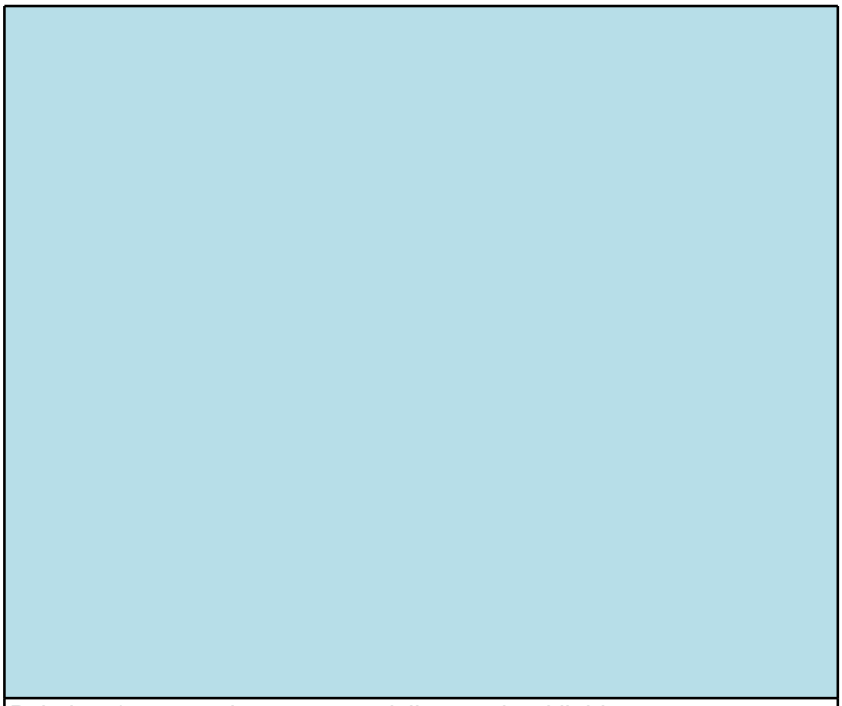


Pykälän 1 momentissa edellytettäisiin avainten ja tunnisteiden hallinnointia mahdollisimman reaaliaikaisesti ja turvallisesti. Tarkoituksena on teknologian kehityksen ja tietoturvallisuuden hyvien käytäntöjen hyödyntäminen pääsynhallinnan ylläpidossa ja parantamisessa. Esimerkkejä hallinnoinnista olisivat hyvät salasanakäytännöt ja että avainten ja tunnisteiden tilatiedot ovat ajantasaiset. ISO/IEC 27000 -standardisarjan mukainen hyvä käytäntö on ulotettu määräyksessä koskemaan myös fyysisiin turvajärjestelyihin liittyviä avaimia ja tunnisteita.

Reaaliaikainen hallinta mahdollistaa esimerkiksi avainten ja tunnisteiden nopean mitätöinnin tai vaihdon, jos ne vaarantuvat tai ovat paljastuneet. Tunnistetietojen, kuten käyttäjätunnusten ja salasanojen turvallinen hallinta varmistaa, että vain valtuutetut käyttäjät pääsevät järjestelmiin ja tietoihin.

Pykälän 2 momentissa edellytettäisiin käytettäväksi ajantasaiseen teknologiaan perustuvia menettelyjä avainten ja tunnisteiden hallinnassa väärinkäytön mahdollisuuden minimoimiseksi. Tunnisteita voivat olla esimerkiksi käyttäjätunnukset, biometriset tunnisteet, PIN-koodit ja evästeet. Väärinkäyttöä olisi esimerkiksi avainten luvaton kopiointi tai salausavainten puutteellinen salaaminen. Tarkoituksena on teknologian kehityksen hyödyntäminen pääsynhallinnan ylläpidossa ja parantamisessa. Esimerkiksi ohjelmoitavien avainten käyttö perinteisten mekaanisten avainten sijaan mahdollistaa tiettyjä turvatekijöitä.

Nykyaikaiset hallintamenettelyt järjestelmineen, kuten esimerkiksi salausavainten keskitetty hallinta ja automaattinen kierrätys sekä -jakelu vähentävät inhimillisiä virheitä, jotka voivat johtaa avainten ja tunnisteiden vuotamiseen. Järjestelmät tarjoavat kattavan valvonnan, joka mahdollistaa tapahtumien ja väärinkäytösten nopean havaitsemisen sekä myös automaattisia toimintoja.



Pykälän 1 momentissa määrättäisiin turvahenkilöiden tietoturvallisesta ja luotettavasti viestinnästä keskenään sekä viranomaisten kanssa. Luvanhaltijan olisi huolehdittava tietoturvallisen ja kattavan viestintäverkon käytettävyydestä ydinlaitoksella, jotta se olisi toimintakuntoinen, tietoturvallinen ja riittävä käyttötarpeisiin nähden. Huolehtiminen sisältää verkon valvontaa, huoltoa, kapasiteetin suunnittelua, tarvittaessa tietoliikenteen salaamista, turvallista elinkaarenhallintaa, kyberturvallisuusriskien torjuntaa sekä nopeaa reagointia mahdollisiin häiriöihin. Tietoturvallinen, häiriönkestävä viestintä on keskeinen osa turvajärjestelyissä onnistumista.

Viestinnän tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden ja eheyden varmistamista siten, että viestiyhteys on myös aina käytettävissä tarvetilanteessa. Tämä koskee normaalitilannetta sekä poikkeama- ja uhkatilanteita. Erityisesti poikkeama- ja uhkatilanteissa voidaan joutua priorisoimaan jotakin em. kolmesta osa-alueesta.

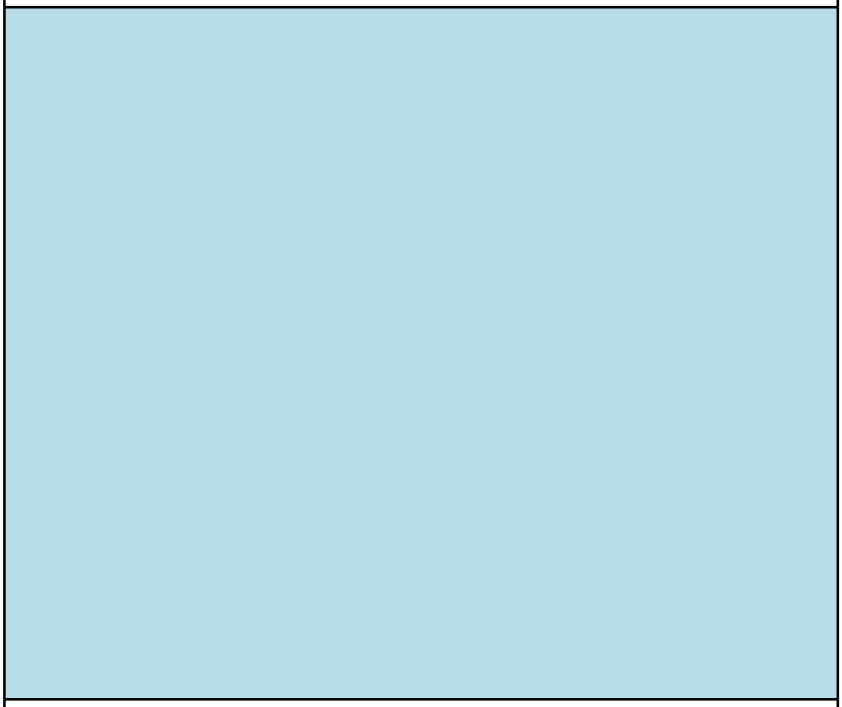
Ydinlaitoksessa olisi otettava huomioon sähkö- ja automaatiojärjestelmien ja viestintäjärjestelmien yhteensopivuus. Pääviestintäjärjestelmän häiriöiden, kuten kyberhyökkäysten, laitevikojen tai yhteyskatkosten varalta tarvitaan luotettava varajärjestelmä, joka varmistaa kommunikaation jatkumisen kriittisissä tilanteissa, joissa nopeus ja tiedon luotettavuus ovat olennaisia.

Pykälän 2 momentissa määrättäisiin, että turvahenkilöt voivat kommunikoida keskenään ja viranomaisen kanssa tietoturvallisesti. Viestintäjärjestelyille on oltava varajärjestelmä, jota voidaan käyttää, jos ensisijainen järjestelmä ei ole käytettävissä.

Pykälän 3 momentissa määrättäisiin viestiyhteyksistä kuljetuksissa. Tavoitteena on, että luvanhaltija ja tarvittaessa poliisi olisivat tietoisia kuljetuksen tilanteesta ja sijainnista, ja että nämä tiedot eivät olisi vapaasti ulkopuolisten saatavissa. Vaatimus koskee sekä puheviestintään käytettäviä välineitä että mahdollisia ajoneuvojen seurantavälineitä. Kuljetuksen tietojen tietoturvallisuudesta olisi huolehdittava (IAEA NSS 13, INFCIRC/225/Rev. 5).

Pykälän 1 momentissa edellytettäisiin asianmukaisia tiloja, välineitä, viestintäyhteyksiä ja henkilöitä turvajärjestelyjen operatiivista johtamista varten, sekä näille järjestelyille varajärjestelyitä. Varajärjestelyjen olisi oltava erotettu varsinaisista järjestelyistä siten, ettei niitä menetetä samanaikaisesti samasta syystä. Syy voisi olla esimerkiksi onnettomuus tai uhkatilanne, ja erottaminen voitaisiin tehdä esimerkiksi varmistamalla riittävä fyysinen etäisyys sekä fyysinen ja kybersuojaus. Vaatimus koskee sekä normaalitilannetta että poikkeamia ja uhkatilanteita. Ei käytettäisi termiä johtokeskus, kuten nykyisessä määräyksessä, vaan jätettäisiin enemmän vapauksia suunnitella ja toteuttaa johtamisen edellytykset laitoksen ominaisuuksiin ja johtamiseen sopiviksi.
Pykälän 2 momentissa edellytettäisiin turvajärjestelyjen operatiiviseen johtamiseen varattujen tilojen suojaamista erilaisissa onnettomuus- ja uhkatilanteissa. Vaatimus koskisi tilojen fyysistä suojaamista ja kybersuojausta. Tiloissa olisi oltava mahdollista työskennellä ilman suojavarusteita sekä normaalin käytön että onnettomuus- ja uhkatilanteiden aikana. Tarkoituksena on varmistaa tärkeälle johtamistoiminnolle hyvät toimintaedellytykset myös suunnitteluperusteuhan mukaisissa uhkatilanteissa ja onnettomuustilanteissa.
Pykälän 3 momentissa edellytettäisiin poliisin käyttöön osoitetun sellaisen tilan varustelua, josta poliisi voi johtaa uhkatilanteen torjumista. Vaatimuksessa ei oteta kantaa siihen, missä tila sijaitsisi tai minkälaisesta tilasta ja sen varustuksesta olisi kyse. Tarkoituksena olisi, että luvanhaltija selvittäisi poliisilta, millainen ja missä sijaitseva tila olisi tarkoituksenmukaisin. Vaatimuksessa SYT-3958 esitetään luvanhaltijalle yleisempi vaatimus, jonka mukaan on varattava poliisille mahdollisuus osallistua uhkatilanteita koskevien turvajärjestelysuunnitelmien ja -toimenpiteiden valmisteluun.

Pykälän 4 momentissa määrättäisiin, ettei sama henkilö saa toimia samanaikaisesti sekä turvajärjestelyjen operatiivisesta johtamisesta että hälytysten käsittelystä vastaavana henkilönä. Tällä pyritään varmistamaan, että nämä kaksi keskeisen tärkeää tehtävää saavat molemmat sen asiantuntemuksen, huomion ja keskittymisen, joka niiden suorittamiseen vaaditaan.



Pykälän 1 momentissa edellytettäisiin, että turvavalvonnan hälytykset ja turvaorganisaatiolle tulevat ilmoitukset olisi käsiteltävä ja arvioitava oikea-aikaisesti. Tavoitteena on hyvän tilannekuvan muodostaminen ja ylläpitäminen ja oikean vasteen järjestäminen. Hälytykset ja ilmoitukset olisi tarpeen mukaan priorisoitava.

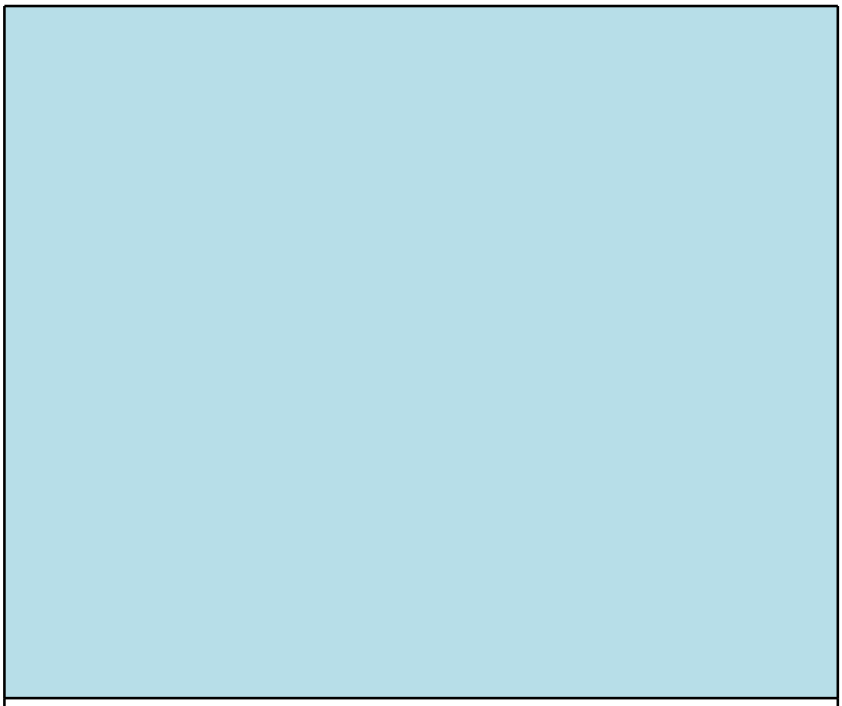
Pykälän 2 momentissa edellytettäisiin, että hälytyskeskuksessa ja varahälytyskeskuksessa olisi järjestelmät hälytysten käsittelyä ja arviointia varten sekä varmennetut, tietoturvalliset yhteydet poliisiin, operatiiviseen johtamiseen tarkoitettuihin tiloihin, henkilöihin (ks. SYT-4036) ja valvomoon. Tarkoituksena on teknologian kehityksen hyödyntäminen hälytysten käsittelyssä ja arvioinnissa turvahenkilön asiantuntemuksen apuna. Tietoturvallisilla yhteyksillä tavoitellaan viestinnän luottamuksellisuuden, eheyden ja saatavuuden varmistamista.

Pykälän 3 momentissa edellytettäisiin hälytyskeskusten suojaamista vastaavasti kuin johtamiseen varattuja tiloja. Hälytyskeskuksen olisi sijaittava suojatulla alueella. Varahälytyskeskus voisi näin ollen sijaita muuallakin, myös oleskelu- ja liikkumisrajoitusalueen ulkopuolella, mikäli sen osoitettaisiin olevan turvajärjestelyjen ja safety-turvallisuuden kannalta edullista. Hälytyskeskus olisi itsessään todennäköisesti vitaalinen tila.

Tarkoituksena on varmistaa tärkeälle hälytysten käsittelylle ja arvioinnille hyvät toimintaedellytykset myös suunnitteluperusteuhan mukaisissa uhkatilanteissa ja onnettomuustilanteissa.

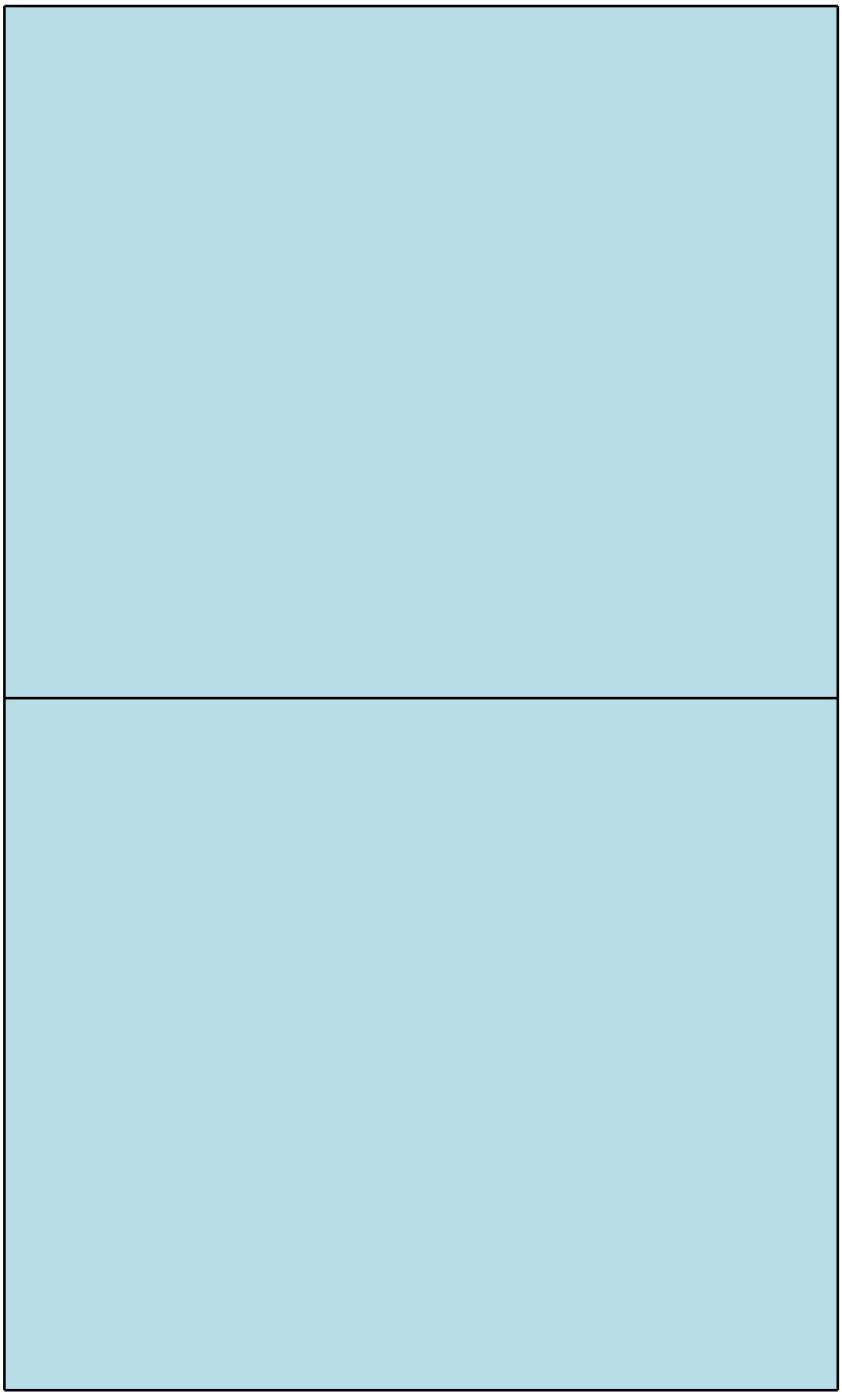
Pykälän 4 momentissa edellytettäisiin, että hälytyskeskusten sähkönsyötölle on oltava varajärjestelmät. Varmistukseen voidaan käyttää keskeytymättömiä virransyöttölaitteistoja (UPS), akustoja, rinnakkaisia sähkönsyöttöjärjestelyjä, varavoimadieseleitä tms. järjestelmiä.

Pykälän 5 momentissa määrättäisiin, että hälytyskeskuksessa on aina oltava vähintään kaksi turvahenkilöä. Vaatimus liittyy sekä insider-uhan torjuntaan että tapaturmaan tai vastaavaan varautumiseen. Määrättäisiin hälytyskeskusten olosuhteista siten, että ne mahdollistavat turvajärjestelyjen tehokkaan toteutumisen. Tällä tarkoitetaan turvahenkilöiden työskentelyolosuhteita: työvälineitä, valaistusta, äänimaailmaa, lämpötilaa, tauotusta, muuta ergonomiaa, sosiaalitiloja, eli teknisten järjestelmien ja järjestelyjen tarjoamaa tukea hälytyskeskusturvahenkilön asiantuntijatehtävän suorittamiseen.
Pykälän 6 momentissa määrättäisiin, että varahälytyskeskuksen olisi oltava erotettu varsinaisesta hälytyskeskuksesta siten, ettei niitä menetetä samanaikaisesti samasta syystä. Syy voisi olla esimerkiksi tekninen häiriö, onnettomuus tai uhkatilanne. Erottaminen voitaisiin tehdä esimerkiksi varmistamalla riittävä fyysinen etäisyys sekä fyysinen ja kybersuojaus. Vaatimus koskee sekä normaalitilannetta että onnettomuuksia, muita poikkeamia ja uhkatilanteita. Määrättäisiin, että hälytyskeskuksesta olisi tarvittaessa pystyttävä siirtymään varahälytyskeskukseen turvallisesti. Tarve voisi syntyä, jos katsottaisiin, että onnettomuudessa, muussa poikkeamassa tai uhkatilanteessa olisi tarkoituksenmukaista jatkaa hälytysten käsittelyä ja arviointia varahälytyskeskuksessa. Samalla sijaintipaikalla sijaitsevilla ydinlaitoksilla voisi olla yhteinen hälytyskeskus. Siirtymistä varahälytyskeskukseen ei tarvittaisi, jos varahälytyskeskuksessa olisi pysyvästi laitoksen turvajärjestelyihin koulutettu osaava henkilöstö sekä muutoin riittävä, vaatimusten mukainen varustelu. Tässäkin tapauksessa poistuminen tarvittaessa varsinaisesta hälytyskeskuksesta olisi pystyttävä toteuttamaan turvallisesti.



Pykälän 1 momentissa määrättäisiin, että valvomot sijaitsevat vitaalisella alueella. Uhka- tai onnettomuustilanteessa valvomotyöntekijöiden olisi myös kyettävä siirtymään mahdollisimman nopeasti ja turvallisesti varavalvomoon, jotta ydinlaitoksen turvallinen tila voidaan taata mahdollisimman luotettavasti. Siirtymän aikana on tarvittaessa käytettävä henkilösuojaimia. Ydinlaitoksen valvomoilla tarkoitetaan ydinlaitoksen valvomoa ja varavalvomoa tai vastaavaa tilaa, mutta ei mahdollisia muita ohjauspaikkoja. Erilaiset ohjauspaikat ja niiden suojaustarpeet arvioidaan niiden riskimerkityksen perusteella.

Pykälän 2 momentissa määrättäisiin ohjaus- ja valvontapaikkojen ja niiden tietoliikenneyhteyksien suojaamisesta rakenteellisesti ja teknisesti. Rakenteellisella suojauksella tarkoitetaan fyysisiä turvajärjestelyjä, kuten esimerkiksi rakenteellisia esteitä. Teknisellä suojaamisella tarkoitetaan esimerkiksi turvavalvontajärjestelmiä sekä suojautumista kyberuhkia vastaan. Laitosalueen ulkopuolella sijaitsevat ohjaus- ja valvontapaikat ja niiden tietoliikenneyhteydet voivat olla alttiita häiriöille, vahingoille ja kyberhyökkäyksille, kuten haittaohjelmille, tietomurroille tai palvelunestohyökkäyksille. Näiden hyökkäysten seurauksena ohjaus- ja valvontajärjestelmiin voisi päästä luvattomasti käsiksi, jolloin voitaisiin manipuloida laitoksen toimintoja tai estää turvallinen toiminta.



Pykälän 1 momentissa määrättäisiin turvajärjestelyiden ylläpitämisestä ydinlaitoksen ja sen rakenteiden, järjestelmien, laitteiden sekä niitä koskevan tiedon koko elinkaaren ajan. Elinkaariajattelu on olennaista turvajärjestelyiden kannalta, koska riskit muuttuvat ajan myötä ja uusia riskejä voi ilmetä. Turvajärjestelyistä tulisi huolehtia aktiivisesti jokaisessa elinkaaren vaiheessa.

Pykälän 2 momentissa edellytettäisiin, että turvavalvontajärjestelmiä koestettaisiin määräajoin niiden luotettavan toiminnan varmistamiseksi. Turvavalvontajärjestelmien toiminta voi heikentyä ajan myötä kulumisen, ohjelmistovirheiden tai muiden tekijöiden vuoksi. Koestus varmistaa, että rakenteelliset ja tekniset turvajärjestelyt, toimivat suunnitellusti ja reagoivat oikein ja luotettavasti mahdollisiin poikkeamiin. Turvajärjestelyjen vaikuttavuuden varmistamiseksi turvavalvontajärjestelmille ja rakenteellisille turvajärjestelyille olisi oltava ennakkohuolto-ohjelma. Varaosien saatavuus on välttämätöntä turvavalvontajärjestelmien luotettavan ja turvallisen toiminnan varmistamiseksi. Varaosien saatavuus varmistaa turvajärjestelmän nopean palauttamisen toimintaan mahdollisten vikojen jälkeen, estää käyttökatkoksia ja tukee järjestelmän elinkaaren hallintaa.

Pykälän 3 momentissa edellytettäisiin, että turvavalvontajärjestelmien suunnittelussa ja toteutuksessa on huomioitava redundanttisuus ja diversifiointi. Tämä tarkoittaa, että järjestelmissä, rakenteissa, laitteissa ja ohjelmistoissa on otettava huomioon vikojen ja tahallisen vahingoittamisen tai manipuloinnin mahdollisuus eikä yksittäinen vikaantuminen saa vaikuttaa järjestelmän kokonaisvaltaiseen vaikuttavuuteen. Turvajärjestelyjen olisi turvallisuuden takaamiseksi oltava toimintakykyisiä myös mahdollisissa onnettomuustilanteissa. Tähän varautumiseen kuuluu myös turvavalvontajärjestelmien varasähkön varmistaminen.

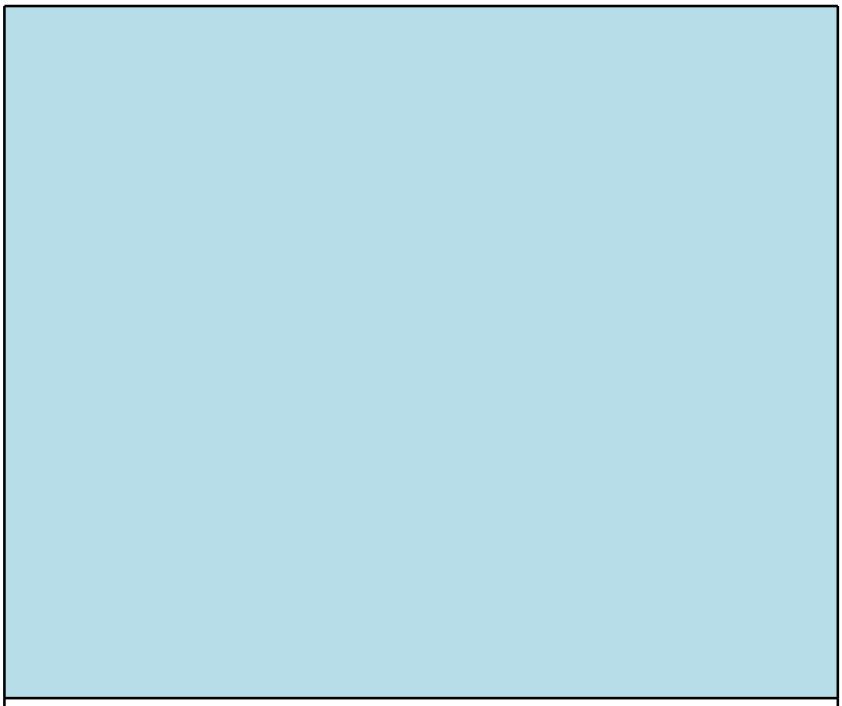
Pykälän 4 momentissa edellytettäisiin, että turvajärjestelyistä on huolehdittava myös tilanteissa, joissa turvajärjestelyjen ensisijaiset menettelyt eivät ole käytettävissä. Korvaavat menettelyt varmistavat, että turvajärjestelyjen taso voidaan säilyttää, vaikka ensisijaiset turvajärjestelymenettelyt, esimerkiksi vikaantumisen takia, eivät olisi väliaikaisesti käytettävissä. Luvanhaltijan tulisi palata ensisijaisiin menettelyihin niin nopeasti kuin käytännöllisin toimenpitein on mahdollista.

Pykälän 5 momentissa määrättäisiin tietojärjestelmiin liittyvästä haavoittuvuuksien hallinnasta. Tietojärjestelmiin liittyviä riskejä tulisi hallita mm. päivittämällä järjestelmät ajantasaisiksi ja varmistamalla, että järjestelmien kovennukset, valvonta sekä pääsynhallinta on järjestetty riittävällä tavalla riskimerkitys huomioon ottaen. Tietojärjestelmiin kuuluvat kaikki laitoksen tietojärjestelmät mukaan lukien fyysisiin turvajärjestelyihin liittyvät järjestelmät (mm. ohjelmistopohjaiset avainjärjestelmät).

Luvanhaltijan on hankittava tietoa käytössään olevien tietojärjestelmien teknisistä haavoittuvuuksista ja arvioitava riskejä avoimille haavoittuvuuksille. Luvanhaltijan olisi toteutettava asianmukaisia toimenpiteitä avoimien haavoittuvuuksien hallitsemiseksi. Jotta luvanhaltija voi hallita avoimia teknisiä haavoittuvuuksia ja niihin liittyviä riskejä, edellyttää tämä käytännössä, että sillä on kattava ja ajantasainen tieto käytössä olevista teknologiasta sekä niiden tarkoista versioista. Haavoittuvuuksiin liittyvien riskien hallintaan kuuluu jäännösriskin määrittäminen, hyväksyminen ja dokumentointi.

Pykälän 6 momentissa määrättäisiin tietojärjestelmiin liittyvästä haavoittuvuuksien hallinnasta. Tietojärjestelmiin liittyviä riskejä tulisi hallita mm. päivittämällä järjestelmät ajantasaisiksi ja varmistamalla, että järjestelmien kovennukset, valvonta sekä pääsynhallinta on järjestetty riittävällä tavalla riskimerkitys huomioon ottaen. Tietojärjestelmiin kuuluvat kaikki laitoksen tietojärjestelmät mukaan lukien fyysisiin turvajärjestelyihin liittyvät järjestelmät (mm. ohjelmistopohjaiset avainjärjestelmät).

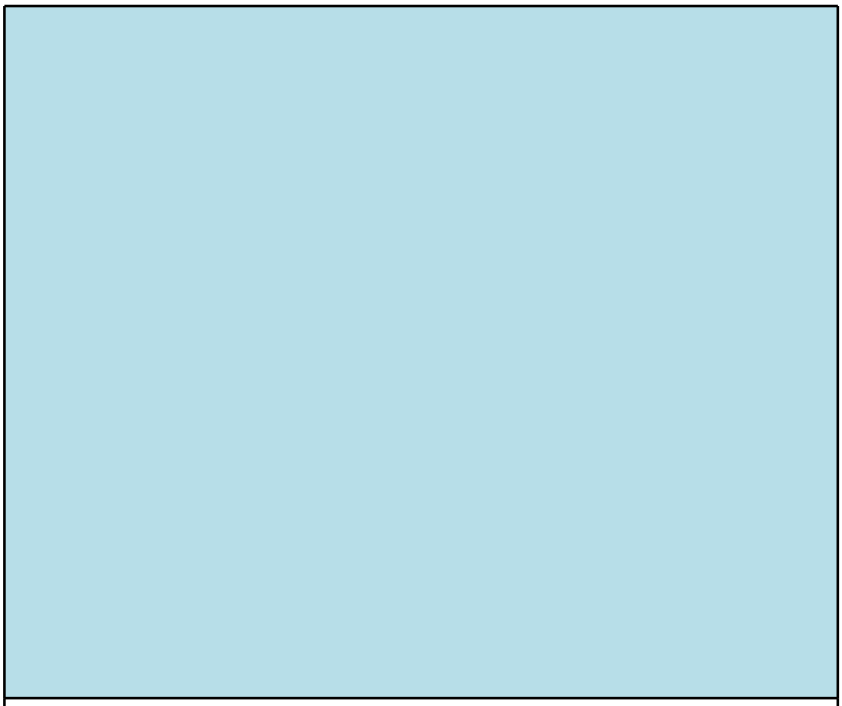
Luvanhaltijan on hankittava tietoa käytössään olevien tietojärjestelmien teknisistä haavoittuvuuksista ja arvioitava riskejä avoimille haavoittuvuuksille. Luvanhaltijan olisi toteutettava asianmukaisia toimenpiteitä avoimien haavoittuvuuksien hallitsemiseksi. Jotta luvanhaltija voi hallita avoimia teknisiä haavoittuvuuksia ja niihin liittyviä riskejä, edellyttää tämä käytännössä, että sillä on kattava ja ajantasainen tieto käytössä olevista teknologiasta sekä niiden tarkoista versioista. Haavoittuvuuksiin liittyvien riskien hallintaan kuuluu jäännösriskin määrittäminen, hyväksyminen ja dokumentointi.



Pykälän 1 momentissa määrättäisiin turvallisuudelle tärkeiden rakenteiden (esim. ovet, portit), järjestelmien, laitteiden ja ohjelmistojen päivitettävyydestä toiminnan suunnittelun lähtökohtana. Päivitettävyys on keskeinen tekijä pitkäaikaisen toimivuuden ja turvallisuuden kannalta. Päivitettävyys mahdollistaa vanhentuneen tekniikan korvaamista, mahdollisten haavoittuvuuksien hallintaa ja uusimpien tietoturvapäivitysten käyttöön ottamista. Teknologia kehittyy nopeasti ja joskus on pystyttävä mukautumaan uusiin uhkiin ja vaatimuksiin. Päivitettävyys myös parantaa kohteen luotettavuutta sekä toiminnan jatkuvuutta. Tavoitteena olisi, että päivitettävyys koskisi yhä enemmän myös ohjausjärjestelmiä, joita perinteisesti on pidetty haastavina päivittää.

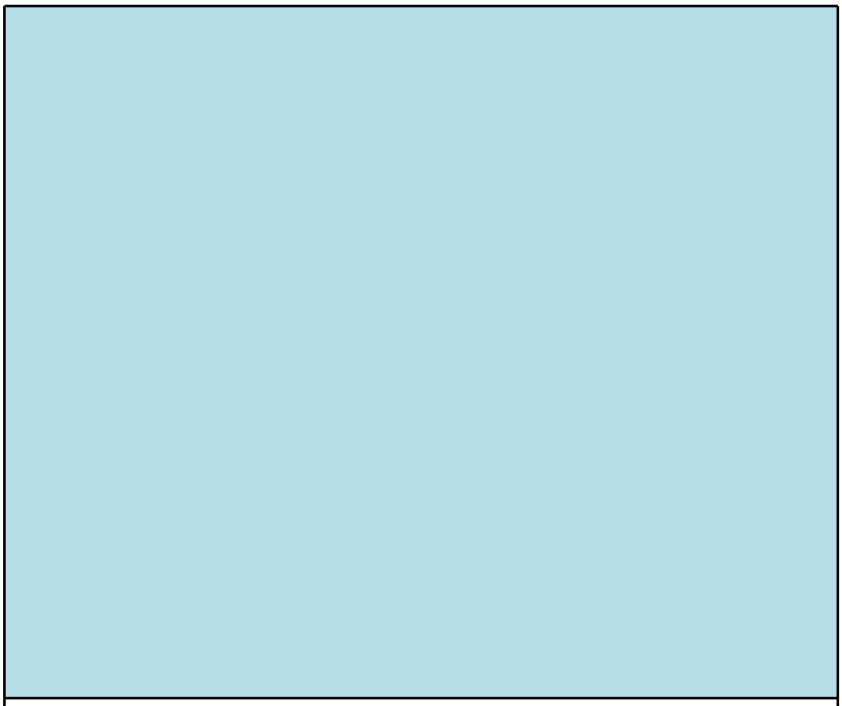
Pykälän 2 momentissa määrättäisiin järjestelmällisten muutostenhallinnan menettelyjen noudattamisesta turvallisuuden ja jäljitettävyyden varmistamiseksi. Turvajärjestelyjen kannalta merkittävät muutokset ja niihin liittyvät päätökset olisi dokumentoitava niiden jäljitettävyyden varmistamiseksi. Järjestelmällinen muutosten hallinta edellyttää riskien arviointia jo ennen muutokseen ryhtymistä. Ilman huolellista muutoksen hallintaa on vaikeaa arvioida, miten muutos vaikuttaa muihin järjestelmiin, prosesseihin ja niiden rajapintoihin.

Rajapintojen hallinnalla pyritään sovittamaan turvallisuuden eri osa-alueet yhteen siten, että vältetään ristiriitoja ja hyödynnetään synergioita.



Pykälän 1 momentissa määrättäisiin tietoturvallisuustestauksesta suunnittelun, käyttöönoton ja muutosten yhteydessä. Riskitietoinen testaus varmistaa, että tietoturvaratkaisut ja hallintakeinot ovat oikeassa suhteessa mahdollisiin haitallisiin vaikutuksiin. Kaikkiin riskeihin ei ole mahdollista tai järkevää varautua samassa laajuudessa, joten riskitietoinen lähestymistapa auttaa priorisoimaan riskit, uhat ja haavoittuvuudet. Suunnitteluvaiheessa toteutettava testaus edes auttaa sitä, että tietoturva ja tarvittavat hallintakeinot on sisäänrakennettu jo alusta alkaen (security by design). Käyttöönoton yhteydessä tapahtuvassa tietoturvatestauksessa tarkistetaan ovatko riskien ja hallintakeinojen tarpeet muuttuneet, ja päivitetään tarvittaessa hallintakeinot ja varmistetaan, että testattava kohde toimii suunnitellusti. Muutoksen yhteydessä tehdään suunnittelu- ja käyttöönottovaihetta vastaavat testaukset tarvittavilta osin.

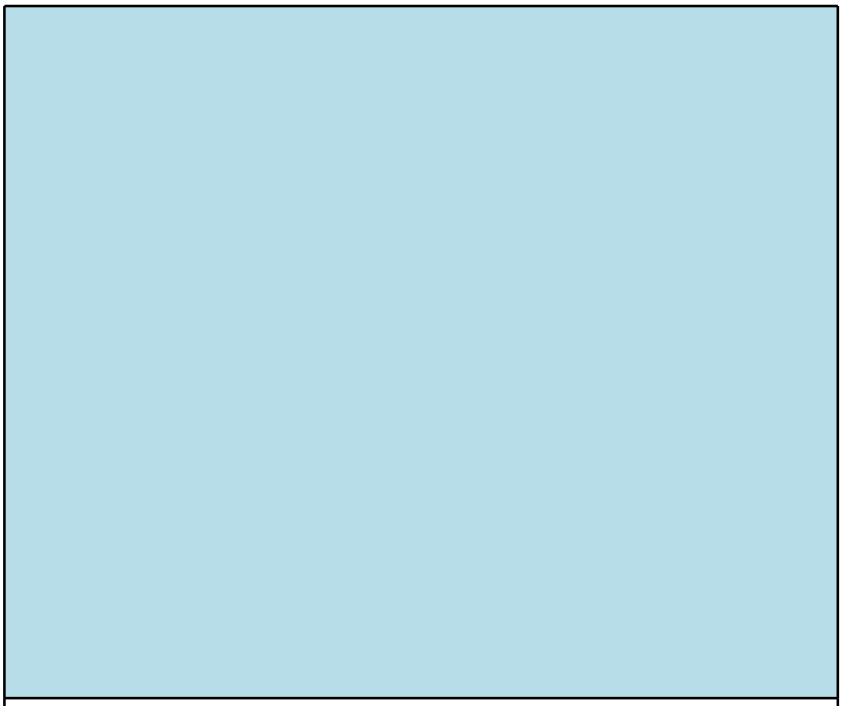
Pykälän 2 momentissa määrättäisiin järjestelmien tietoturvallisuudesta testauksessa. Tietoturvallisuuden varmistamiseen kuuluu tuotanto-, testaus- ja kehitysvaiheiden ympäristöjen ja tietosisältöjen suojaaminen ja eriyttäminen riittävällä tasolla ja ohjelmistojen ja laitteiden siirtäminen kehitys-, testaus- ja tuotantotilaan määritetysti, dokumentoidusti ja valvotusti. Muutokset tuotantojärjestelmiin testataan lähtökohtaisesti tarkoitukseen soveltuvassa testi- tai koeympäristössä. Mikäli testaus joudutaan suorittamaan tuotantoympäristössä, se tehdään ainoastaan ennalta määritellyissä ja hyväksytyissä olosuhteissa. Mikäli salassa pidettävää tietoa viedään kehitys- tai testausympäristöön, ympäristöjä hallitaan ja suojataan samantasoisilla keinoilla, kuin tuotantoympäristöä.



Pykälän 1 momentissa määrättäisiin turvallisen elinkaaren hallinnan menettelyistä. Järjestelmän elinkaaren eri vaiheissa on erilaisia turvallisuusriskejä, joita vahingolliseen toimintaan ryhtyvä taho voisi kyetä hyödyntämään. Turvallisen elinkaaren hallinnan menettelyt kattavat kaikki vaiheet järjestelmän suunnittelusta käytöstä poistoon. Suunnitteluvaiheessa integroidaan eri turvallisuusnäkökohdat suoraan järjestelmään (security by design). Käyttöönoton ja käytön yhteydessä tarkistetaan ovatko riskit ja hallintakeinojen tarpeet muuttuneet, ja päivitetään tarvittaessa hallintakeinot ja varmistetaan, että kohde toimii suunnitellusti. Muutoksen yhteydessä tehdään suunnittelu- ja käyttöönottovaihetta vastaavat testaukset tarvittavilta osin. Käytöstä poiston yhteydessä huolehditaan erityisesti siitä, että kaikki järjestelmässä olleet tiedot hävitetään hyvien tietoturvallisuuskäytänteiden mukaisesti.

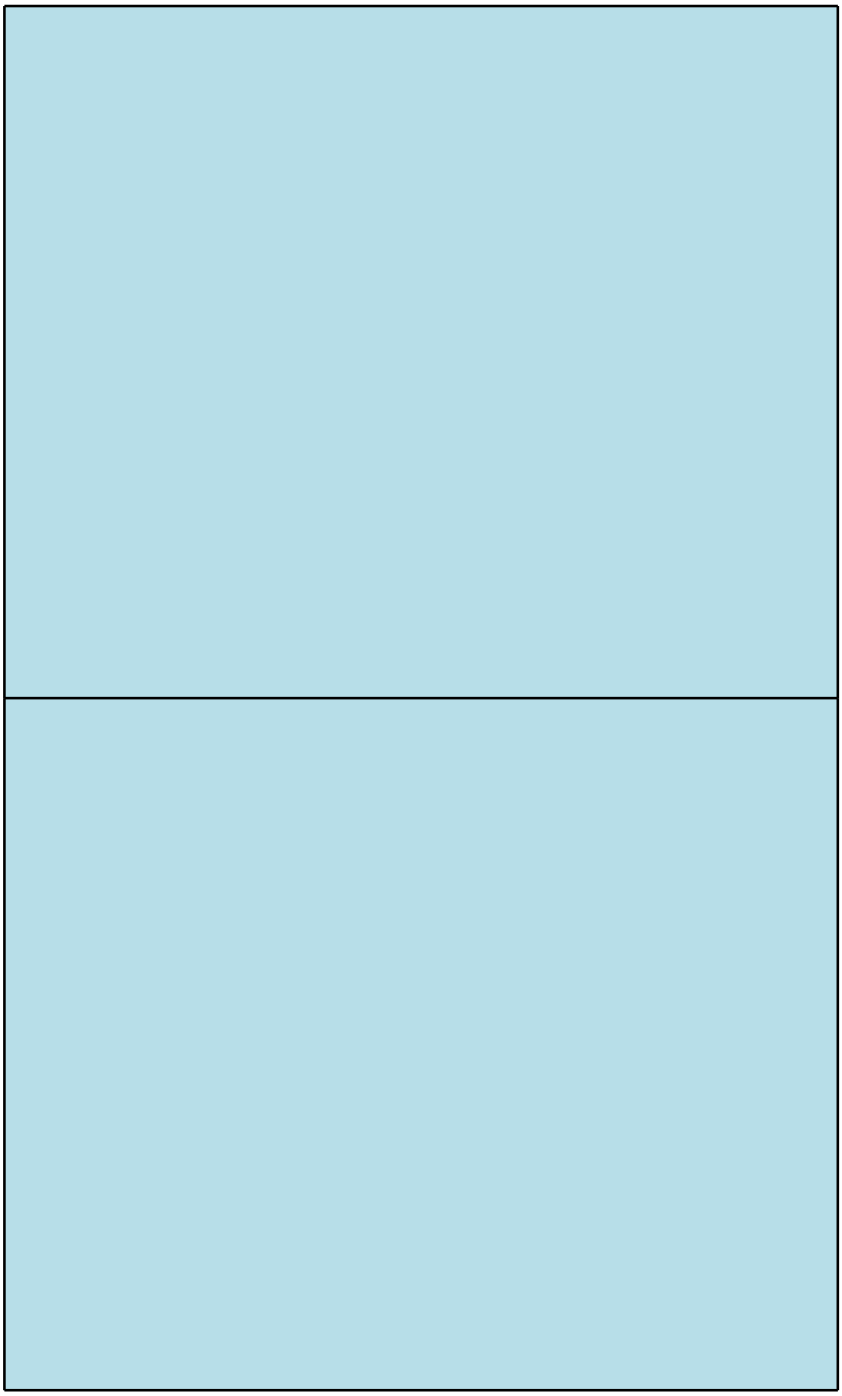
Pykälän 2 momentissa määrättäisiin palveluiden hallintamenettelyistä. Ulkoisten palveluiden ja alihankkijoiden käyttöön liittyy turvajärjestelyriskejä (esim. insider-uhka, kuten pääsy salassa pidettävään tietoon tai logistiikkaketjuun tunkeutuminen), jotka luvanhaltijan tulisi tunnistaa ja joita sen tulisi hallita. Hallintaprosessi pyrkii varmistamaan, että ulkoisten palvelujen ja alihankkijoiden turvallisuustaso on sama kuin luvanhaltijalla palveluun liittyvän turvallisuusmerkityksen mukaisesti.

Hallintamenettelyihin liittyy vastuista ja velvollisuuksista, immateriaalioikeuksista ja kriittisten tietojen omistajuudesta sopiminen.



Pykälän 1 momentissa määrätäisiin siitä, että luvanhaltija varaa poliisille mahdollisuuden osallistua uhkatilanteita koskevien turvajärjestelysuunnitelmien ja -toimenpiteiden valmisteluun. Vaatimus perustuu siihen, että poliisi toimii ulkopuolisena vasteena uhkatilanteissa ja poliisin osallistuminen uhkatilanteita koskevien turvajärjestelysuunnitelmien ja -toimenpiteiden valmisteluun edesauttaa suunnitelmien toimivuutta ja vaikuttavuutta uhkatilanteissa, erityisesti poliisin ja turvaorganisaation yhteistoiminnan kannalta Poliisilla on asiantuntemusta, hyviä käytäntöjä, laajaa kokemusta uhkatilanteiden hallinnasta, jotka ovat luvanhaltijalle hyödyksi.

Pykälän 2 momentissa määrättäisiin velvollisuudesta luoda ja ylläpitää yhteistyömenettelyitä tarvittaviin toimivaltaisiin viranomaisiin sekä sidosryhmiin. Yhteistyön tavoitteena on tilannekuvan ylläpito, hyvien käytäntöjen jakaminen, käyttökokemustoiminta ja benchmarking. Luvanhaltijoille tärkeitä turvajärjestelyihin liittyviä viranomaistahoja ovat poliisiviranomaiset, pelastuslaitokset, Suojelupoliisi, Rajavartiolaitos, Kyberturvallisuuskeskus ja Puolustusvoimat ja mahdolliset muut viranomaiset, joilla on rooli ydinturvallisuuden ja turvajärjestelyjen toteutumisessa. Toimialan sidosryhmiä ovat esimerkiksi muut kotimaiset sekä ulkomaalaiset ydinalan luvanhaltijat, joiden kanssa tietojen ja hyvien käytäntöjen vaihto hyödyttää turvajärjestelyjen kehittämistä.



Pykälän 1 momentissa määrättäisiin poikkeamien ennalta ehkäisemiseen ja havaitsemiseen liittyvistä menettelyistä. Asianmukaiset menettelyt ja niitä tukevat järjestelmät auttavat estämään poikkeamien syntymistä, havaitsemaan ja rajoittamaan niiden vaikutusta. Esimerkiksi laitevikoja voidaan ennalta ehkäistä säännöllisillä huolloilla, päivityksillä ja tarkastuksilla, ja poikkeamia voidaan havaita reaaliaikaisella valvonnalla. Muun muassa tietoympäristöjen erityispiirteet tulisi huomioida menettelyjä luotaessa ja käytettäessä. Esimerkiksi monet IT-palvelujen menetelmät ja työvälineet eivät ole suoraan käytettävissä OT-palvelujen poikkeamien hallinnassa.

Tavoite asianmukaiselle vasteelle määritetään etukäteen erilaisiin poikkeamiin ja uhkatilanteisiin liittyen. Määrityksen pohjalta voidaan mitoittaa tarvittavat resurssit.

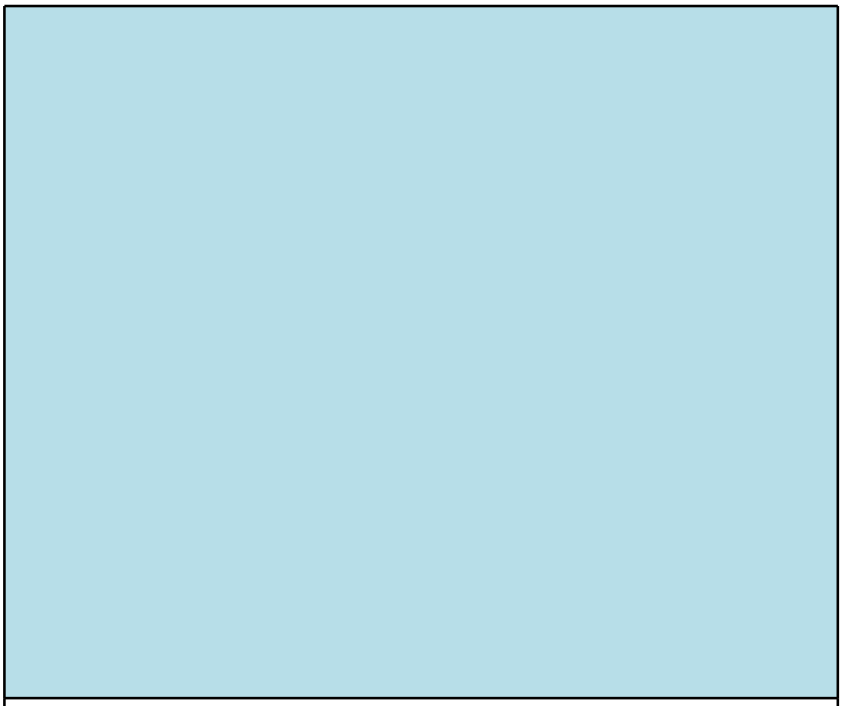
Pykälän 2 momentissa määrättäisiin tietojen keräämisestä, suojaamisesta ja säilyttämisestä poikkeamien ja uhkatilanteiden tutkinnan edellytysten varmistamiseksi. Tietoihin kuuluvat turvavalvontajärjestelmillä ja muilla tietojärjestelmillä kerätyt tiedot, kuten kameratallenteet, lokit ja tietojärjestelmien muut käyttötiedot. Tietojen tallennuksessa ja hallinnassa otetaan huomioon tietojen säilytysaika- ja paikka, tietojen suojaaminen, käyttötarkoitus, käsittelyoikeudet ja mahdolliset muut laeista seuraavat velvoitteet.

Pykälän 1 momentissa määrättäisiin, että poikkeamissa ja uhkatilanteissa on ryhdyttävä tilanteen vaativiin toimenpiteisiin viipymättä. Tarkoituksena on varmistaa vasteen oikea-aikaisuus ja vaikuttavuus. Poikkeamiin ja uhkatilanteisiin (erityistilanteisiin) olisi varauduttava. Tarvittaviin toimenpiteisiin kuuluu turvallisuutta vaarantavan toiminnan pysäyttäminen, erityistilanteen hallintaan saattaminen, seurausten estäminen ja rajoittaminen.

Pykälän 2 momentissa määrättäisiin viranomaisten hälyttämisestä ja tilannekuvan välittämisestä, jotta viranomainen saa tiedon tapahtumasta ja voi käynnistää viranomaisvasteen. Ensi-ilmoituksen lisäksi tapahtumaa koskevaa tilannekuvaa, kuten mitä on tapahtunut ja mihin toimenpiteisiin on ryhdytty, olisi toimitettava vasteviranomaiselle jo ennen tämän saapumista paikalle, jotta se voi organisoida omaa toimintaansa uhkaa vastaan.

Pykälän 3 momentissa määrättäisiin luvanhaltijan velvollisuudesta tukea poliisia uhkatilanteessa. Tarkoituksena on varmistaa, että poliisi pystyy johtamaan tilannetta turvallisuusmerkityksen perusteella, kuten priorisoimaan toimenpiteiden keskinäistä järjestystä moniulotteisissa tilanteissa.

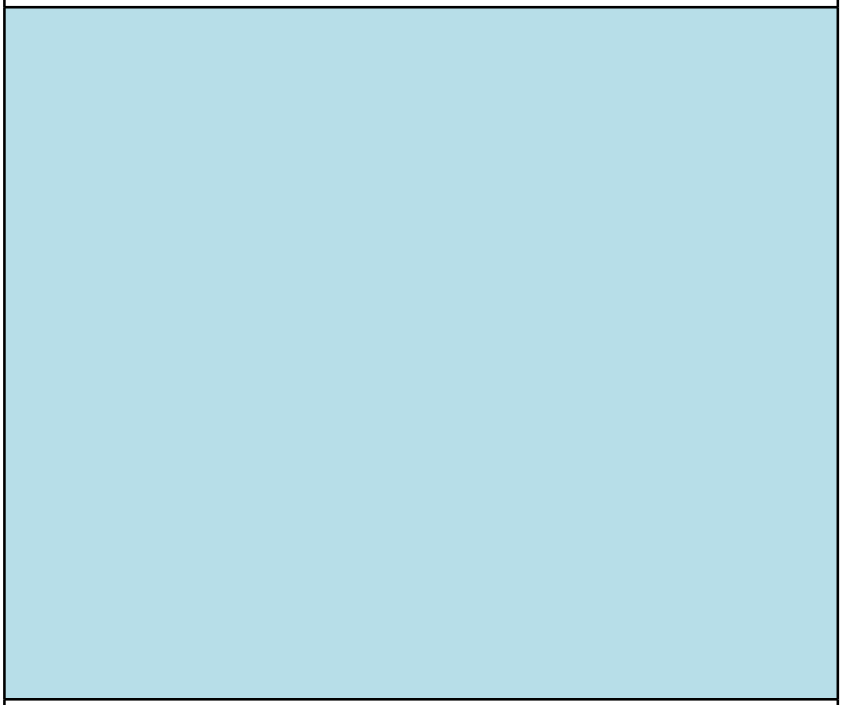
Ydinlaitosten tilat voivat aiheuttaa ylimääräistä säteilyaltistusta henkilöille, joilla ei ole aiempaa kokemusta ydinlaitoksella työskentelystä. Myös voimankäyttöön ydinlaitoksen alueella tulee kiinnittää erityistä huomiota, jotta turvallisuus ei vaarannu vastetoiminnan seurauksena. Säteilyannosten ja -päästöjen minimoimiseksi luvanhaltijan tulisi tukea poliisia ja muita viranomaisia tarvittavissa määrin ydinlaitoksen erityispiirteet huomioon ottaen, jotta vastetoimintaan liittyvät riskit saadaan minimoitua.



Pykälän 1 momentissa määrättäisiin luvanhaltijan velvollisuudesta toimittaa STUKille tietoja turvajärjestelyihin liittyvästä poikkeamasta tai uhkatilanteesta, jotta STUK pystyy arvioimaan tilanteen turvallisuusmerkityksen ja antamaan tarvittaessa suosituksia muille viranomaisille sekä viestimään tilanteesta viranomaisten kanssa ja yleisölle.

Pykälän 2 momentissa määrättäisiin turvajärjestelyihin liittyvästä poikkeamasta ja uhkatilanteesta raportoimisesta. Tällä tavoin STUK voi arvioida miten toiminnanharjoittaja kehittää toimintaansa poikkeamista ja uhkatilanteista saatujen kokemusten perusteella.

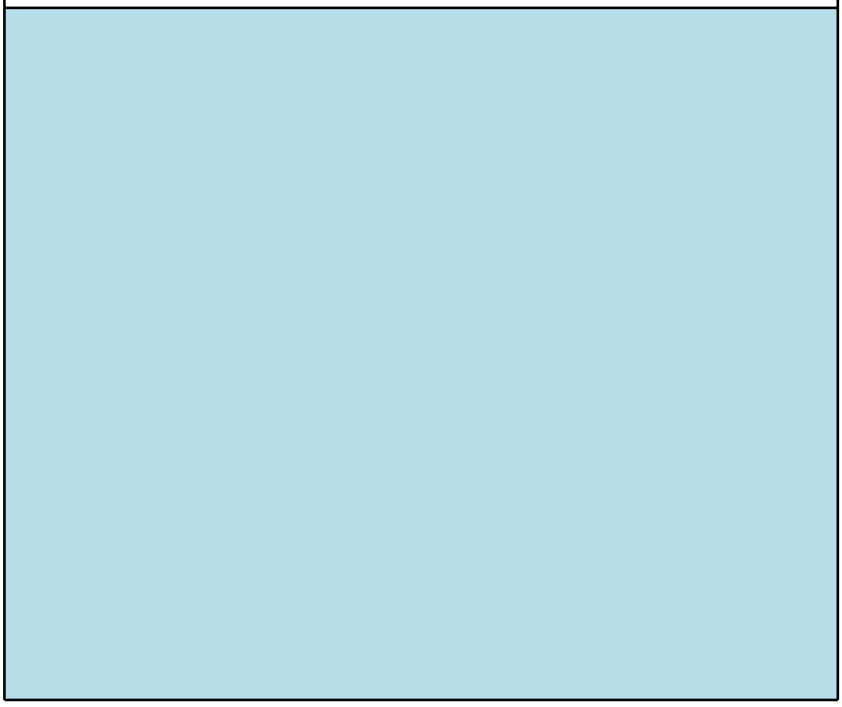
Pykälän 3 momentissa säädetään kyberturvallisuutta koskevien poikkeamien ilmoittamisesta viittauksella kyberturvallisuuslakiin.

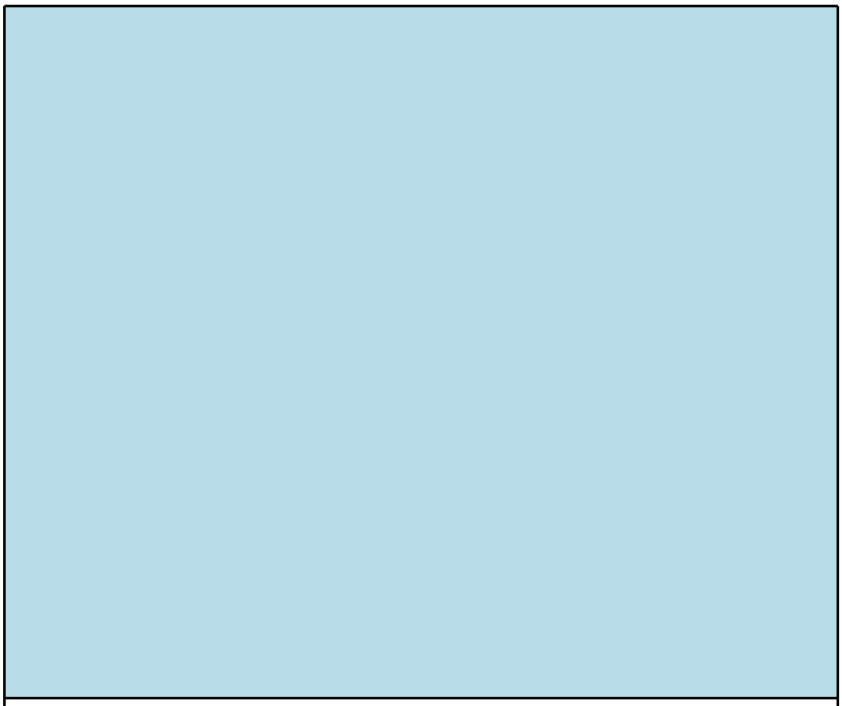


Pykälän 1 momentissa säädetään jatkuvuuden hallinnasta turvajärjestelyjen osalta. Jatkuvuuden hallintamenettelyjen avulla luvanhaltija kykenee ylläpitämään turvajärjestelyjen vaikuttavuutta riippumatta muuttuvasta uhkasta, henkilövaihdoksista tai muista tekijöistä, joilla on vaikutusta turvajärjestelyiden toteutukseen. Kysymyksessä on standardia ISO/IEC 27002 vastaava kontrolli, joka tulisi sovellettavaksi myös fyysisiin turvajärjestelyihin. Testaamisen tarkoituksena on varmistaa, että tarvittavat tiedot ja turvajärjestelyjen toiminta pystytään palauttamaan oikea-aikaisesti. Riittävät taloudelliset- ja henkilöresurssit mahdollistavat henkilöstön riittävyyden sekä turvajärjestelyjen kehittämisen jatkuvan parantamisen periaatteiden mukaisesti.

Pykälän 2 momentissa määrättäisiin järjestelmien ja varmuuskopioiden hallinnasta jatkuvuusvaatimusten ja riskiarvion mukaisesti. Riskiarvio auttaa tunnistamaan kriittiset järjestelmät ja tiedot, joiden toiminnan ja säilyttämisen häiriintyminen voi aiheuttaa merkittäviä haittoja toiminnalle ja sen turvallisuudelle. Jatkuvuusvaatimukset määrittävät, kuinka nopeasti järjestelmien on toivuttava häiriöstä (RTO, Recovery Time Objective) ja kuinka tuoretta tiedon on oltava varmuuskopioissa (RPO, Recovery Point Objective). Huonosti hallitut järjestelmät ja puutteelliset varmuuskopiot voivat johtaa toiminnan keskeytymiseen, tiedon menetyksiin ja toiminnan palautumisen vaikeutumiseen. Varmuuskopioiden suojaaminen ja säilyttäminen turvallisuusmerkityksen mukaisesti mahdollistaa riittävien hallintakeinojen suunnittelun ja toteuttamisen suhteessa riskeihin. Tästä esimerkkinä sellaiset kriittiset varmistukset, joita täytyy säilyttää eristettynä kaikista muista ympäristöistä (ns. offline-tilassa tai ilmaraon takana) ja tämän takia hyökkääjä ei pääse niihin tietoverkkoja hyödyntäen vaikuttamaan.

Tietojen palautusta on syytä testata, jotta varmuus tietojen palauttamisen onnistumisesta voidaan varmistaa. Varmuuskopioiden olemassaolo ei takaa niiden toimivuutta. Testaamalla palautusta voidaan arvioida, kuinka nopeasti ja kuinka tuoreisiin tietoihin voidaan päästä häiriön sattuessa. Käytännön testit auttavat henkilöstöä tutustumaan palautusprosesseihin ja harjoittelemaan niiden suorittamista stressittömässä ympäristössä.





Pykälän 1 momentissa määrättäisiin turvajärjestelyjen dokumentoinnista, siten että luvanhaltija pystyy osoittamaan itselleen ja STUKille, että turvajärjestelyt ovat vaatimusten mukaiset. Uhkatilanteiden dokumentoinnit ovat tärkeitä mahdollisen poliisitutkinnan edellytysten varmistamiseksi. Dokumentointi auttaa myös luvanhaltijaa kehittämään toimintaansa jatkuvan parantamisen periaatteen mukaisesti.

Pykälän 2 momentissa määrättäisiin turvajärjestelyjen kannalta keskeisten tietojen ja tallenteiden suojaamisesta. Turvajärjestelyjen keskeisten tietojen ja tallenteiden oikeudeton paljastuminen voi aiheuttaa vahinkoa turvajärjestelyjen vaikuttavuudelle. Tietojen suojaus tulisi tehdä hyvien tietoturvallisuuskäytänteiden mukaisesti. Luvanhaltijan tulisi myös huomioida salassa pidettävien viranomaisaineistojen asianmukainen suojaus siten, että luvanhaltijalla on käytössään tilat, välineet ja järjestelmät, joissa salassa pidettäviä aineistoja kyetään käsittelemään turvallisesti.

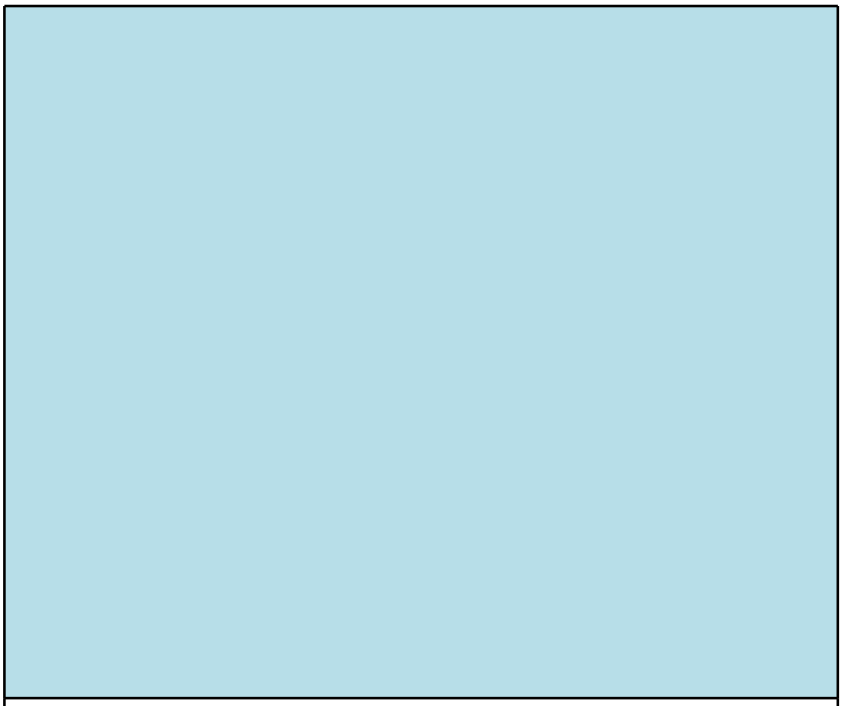
Pykälän 3 momentissa määrättäisiin tiedon luokittelun ja merkitsemisen periaatteista ja toteuttamisesta. Tiedon turvallisuuden varmistaminen edellyttää sitä, että tietoa käsitellään ja suojellaan sen luonteen ja turvallisuusmerkityksen mukaan. Kun tiedot on luokiteltu, luvanhaltija voi asettaa asianmukaiset menettelyt pääsyoikeuksille, tiedon käsittelylle, säilytykselle, jakelulle, arkistoinnille ja tuhoamiselle

Pykälän 4 momentissa määrättäisiin tietojen käsittelyn ja tietojärjestelmien käytön ohjeista. Ohjeiden tarkoituksena on varmistaa, että henkilöstö osaa käsitellä tietoja ja käyttää tietojärjestelmiä oikealla ja turvallisella tavalla. Ohjeet opastavat henkilöstöä esimerkiksi rooleista ja vastuista, siitä, miten tiedot suojataan, miten turvalliset salasanat luodaan ja säilytetään. Ohjeiden selkeys, käytettävyys ja saatavuus ovat keskeisiä periaatteita. Ohjeet edesauttavat toiminnan yhdenmukaisuutta. Osa ohjeista koskee kolmansia osapuolia.

Pykälän 1 momentissa määrättäisiin viranomaisen turvallisuusluokitteleman ja muun salassa pidettävän tiedon käsittelystä. Koska viranomaiset luovuttavat luvanhaltijoille tiettyjä salassa pidettäviä tietoja, katsotaan tarkoituksenmukaiseksi, että niiden tietoturvallisuudesta huolehdittaisiin saman tasoisesti kuin asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetussa valtioneuvoston asetuksessa (1101/2019) määrätään, vaikka asetus ei sinällään koske kuin viranomaisia.

Pykälän 2 momentissa määrättäisiin viranomaisen salassa pidettävän tiedon tai siitä johdettua tietoa sisältävän aineiston luovuttamisesta kolmannelle osapuolelle. Ennen kyseisen tiedon luovuttamista kolmannelle osapuolelle luvanhaltijan on otettava yhteys Säteilyturvakeskukseen tai kyseisen tiedon laatineeseen muuhun viranomaiseen sen varmistamiseksi voidaanko tietoa miltä osin ja millä edellytyksillä mahdollisesti luovuttaa tai onko tiedon uudelleen luokittelu kenties mahdollista.

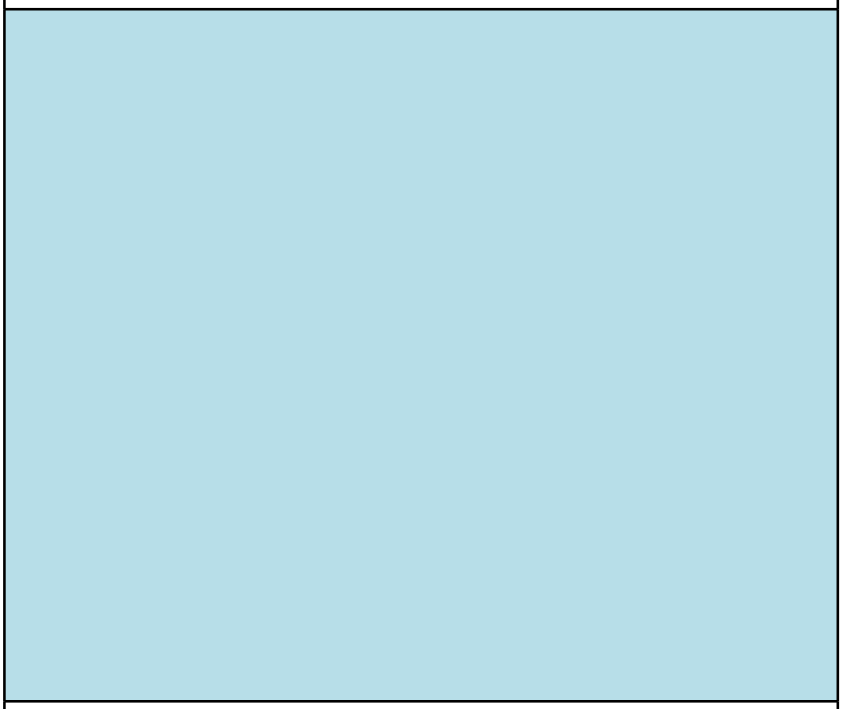
Tällaisen salassa pidettävän tiedon oikeudeton käyttö tai paljastuminen voi aiheuttaa haittaa turvajärjestelyjen toteuttamiselle ja turvallisuudelle yleensäkin.



Pykälän 1 momentissa määrättäisiin palvelutasojen ja -vaatimusten määrittämisestä, toteuttamisesta sekä valvonnasta. Turvajärjestelyjen palvelutasot ja -vaatimukset tulisi olla selkeästi määritelty, jotta turvajärjestelyjen tehokkuutta voidaan arvioida ja havaita niissä mahdollisesti tapahtuvia poikkeamia. Palvelutasovaatimus tarkoittaa esimerkiksi sitä, että sisäinen tai ulkoinen palveluntarjoaja kykenee tuottamaan palvelun sovitun mukaisena ja ajantasaisena. Palvelun laadulle ja suorituskyvylle määritetään vähimmäisvaatimukset, jotka palveluntarjoajan tulee täyttää. Palvelutasovaatimus koskisi mm. turvavalvontajärjestelmien käytettävyyttä ja korjausaikavastetta.

Pykälän 2 momentissa määrättäisiin turvajärjestelyjen vaatimuksenmukaisuuden arvioinnista. Turvajärjestelyjen vaatimustenmukaisuuden arvioinnin tarkoituksena on selvittää, ovatko turvajärjestelyt riittävät ja tunnistaa mahdolliset parannuskohteet ja edesauttaa jatkuvaa parantamista. Arvioinnissa tulisi huomioida ydinlaitoksen koko elinkaari, mukaan lukien kuljetukset. Arvioinnissa mahdollisesti havaitut puutteet turvajärjestelyissä tulisi korjata tarkoituksenmukaisesti. Ydinenergialakiluonnoksen 123 §:ssä käsitellään sisäistä valvontaa.

Pykälän 3 momentissa määrättäisiin turvajärjestelyjen itsearvioinneista ottaen huomioon uhkakuvassa ja riskienarvioinneissa tapahtuneet muutokset ja turvallisuustapahtumat. Itsearvioinnin tarkoitus on havaita mahdollisia kehityskohteita turvajärjestelyissä sekä tämän pohjalta kehittää niitä jatkuvan parantamisen periaatteella. Turvajärjestelyjen yhteensopivuus luvanhaltijan valmiusjärjestelyihin ja poliisin toimintasuunnitelmiin olisi tarkoituksenmukaista arvioida samassa yhteydessä. Hyvä käytäntö on, että turvajärjestelyjen itsearvioinnit sisältyisivät muiden sisäisten arviointien tai auditointien prosessiin.

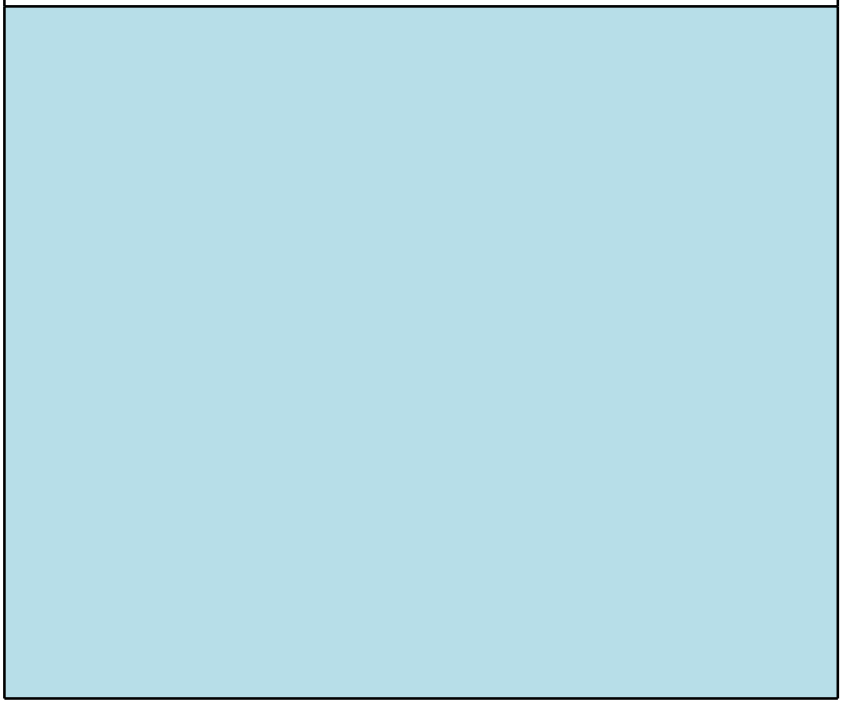


Pykälän 1 momentissa määrättäisiin turvajärjestelyharjoituksista, jotka ovat oleellisia turvajärjestelyiden vaikuttavuuden osoittamisen sekä turvajärjestelyjen jatkuvan parantamisen kannalta. Turvajärjestelyjen tason varmistamiseksi turvahenkilöiden harjoittelua tarvitaan säännöllisesti asiaa koskevien luvanhaltijan asiakirjojen mukaisesti.

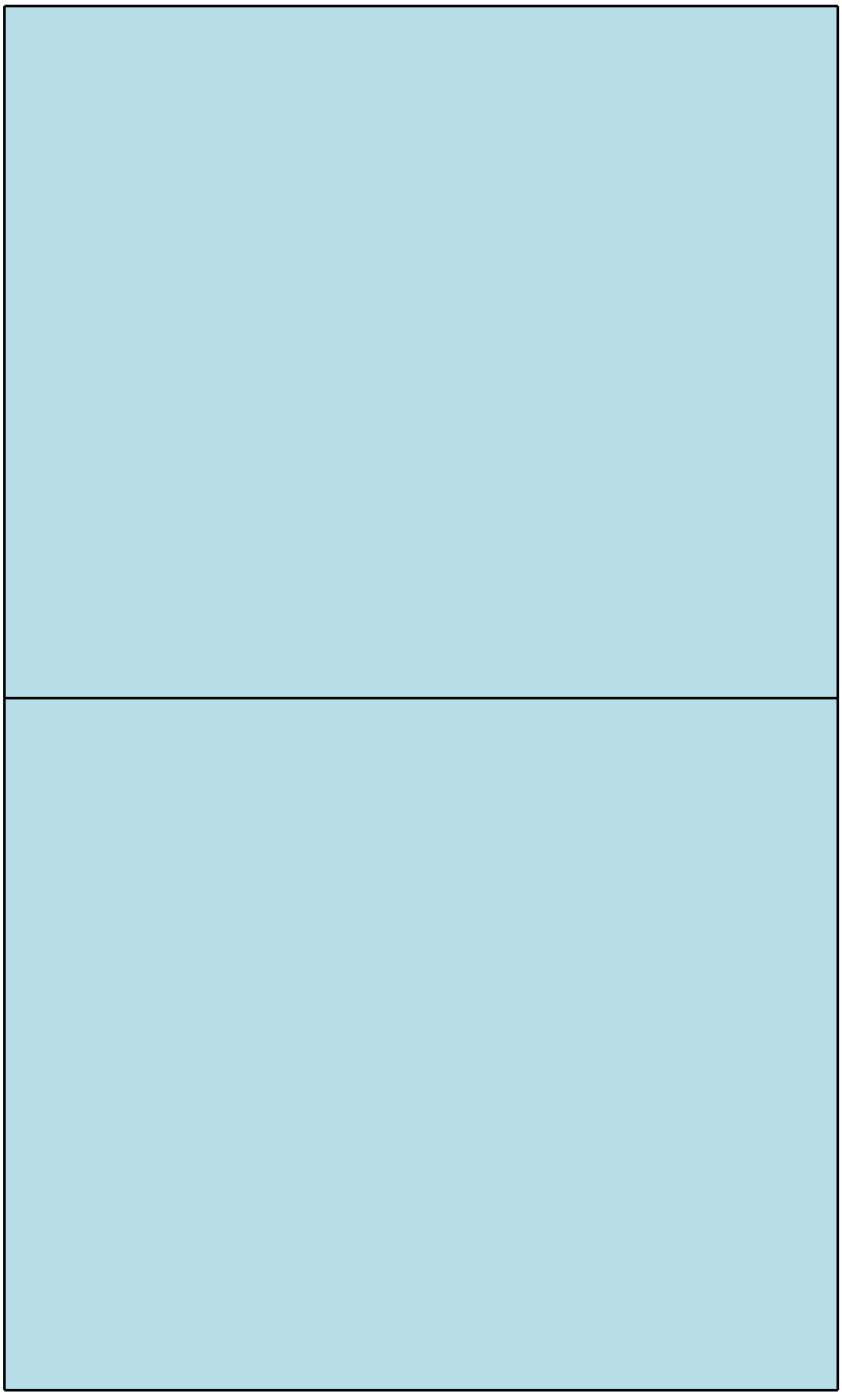
Onnettomuuksien, fyysisten uhkien, tietoturvallisuusuhkien ja poikkeamien yhdistäminen harjoittelussa on keskeistä, sillä vakavimmat skenaariot todennäköisesti ovat näiden uhkien yhdistelmiä.

Pykälän 2 momentissa määrättäisiin harjoitusten sisällöstä. Koska suunnitteluperusteuhkaa on käytettävä turvajärjestelyjen suunnittelun ja arvioinnin perusteena, on perusteltua, että harjoitukset sisältäisivät suunnitteluperusteuhan mukaisia skenaarioita. Skenaarioiden kautta suojaustavoitteiden täyttyminen voidaan osoittaa. Harjoittelun avulla kyetään havainnoimaan ja korjaamaan mahdollisia puutteita. Harjoittelun on myös sisällettävä turvajärjestelyjen havainnointi- ja vastekyvykkyyden testausta. Turvaorganisaation havainnointi- ja vastekyky muodostavat keskeisen elementin, jolle uhkien ajantasainen ja tehokas torjunta perustuu.

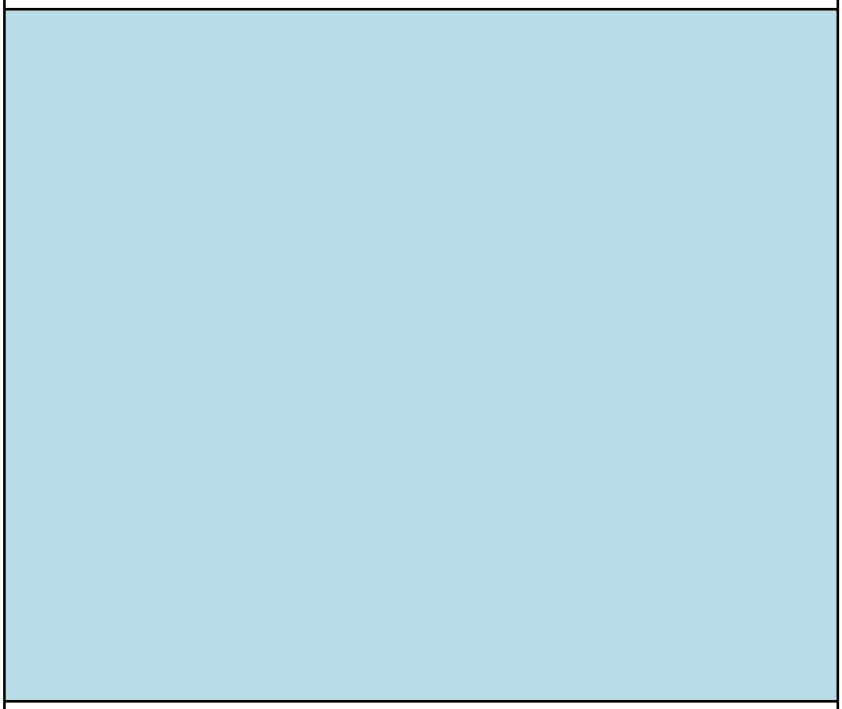
Pykälän 3 momentissa määrättäisiin viranomaisten mahdollisuudesta osallistua harjoituksiin. Toimivaltaisten viranomaisten osallistuminen harjoituksiin ja niiden suunnitteluun on keskeistä, koska erityisesti vakavissa uhkatilanteissa yhteistoiminta turvallisuusviranomaisten kanssa korostuu. Harjoituksia olisi tarpeen suunnitella yhteistyössä asianomaisten viranomaisten kanssa. Yhteistyö koskisi myös harjoitustoiminnan perusteella tunnistettuja parannustoimenpiteitä jatkuvan parantamisen periaate huomioiden.



Pykälän 1 momentissa määrättäisiin turvajärjestelyjen vaikuttavuudesta poikkeamia ja uhkatilanteita vastaan. Luvanhaltijan on osoitettava, että laitoksella on varauduttu erilaisten uhkatilanteiden varalle ja että turvajärjestelyihin liittyvät järjestelmät, rakenteet, laitteet ja toimenpiteet ovat riittäviä estämään tai viivyttämään riittävän kauan vahingontekijää aiheuttamasta laitoksen, sen henkilökunnan tai ympäristön turvallisuutta vaarantavaa tilannetta. Vaikuttavuuden osoittamiseksi on käytettävä erityyppisiä osoittamiskeinoja. Vaikuttavuuden keskeinen osoitusmuoto on harjoitusten käyttäminen.
Pykälän 2 momentissa määrättäisiin turvajärjestelyjen koekäyttöjaksoista. Koekäyttö on suunniteltava ja se on dokumentoitava. Turvajärjestelyiden koekäytön avulla turvajärjestelyitä kyetään testaamaan, osoittamaan sen mahdolliset puutteet sekä tekemään tarvittavat korjaavat toimenpiteet ennen turvajärjestelyjen varsinaista operatiivista käyttöönottoa.
Pykälän 3 momentissa määrättäisiin turvajärjestelyjen testaamiseen liittyvästä järjestelmällisestä ohjelmasta. Järjestelmällisellä ohjelmalla voidaan osoittaa ja varmistaa turvajärjestelyjen sekä tietojärjestelmien toimivuus ennen käyttöönottoa sekä käytön aikana. Ohjelmalla varmistetaan, että kaikki turvajärjestelyjen ja tietojärjestelmien osa-alueet testataan riittävän kattavasti ja varmistetaan niiden toimivuus käyttövaiheessa.

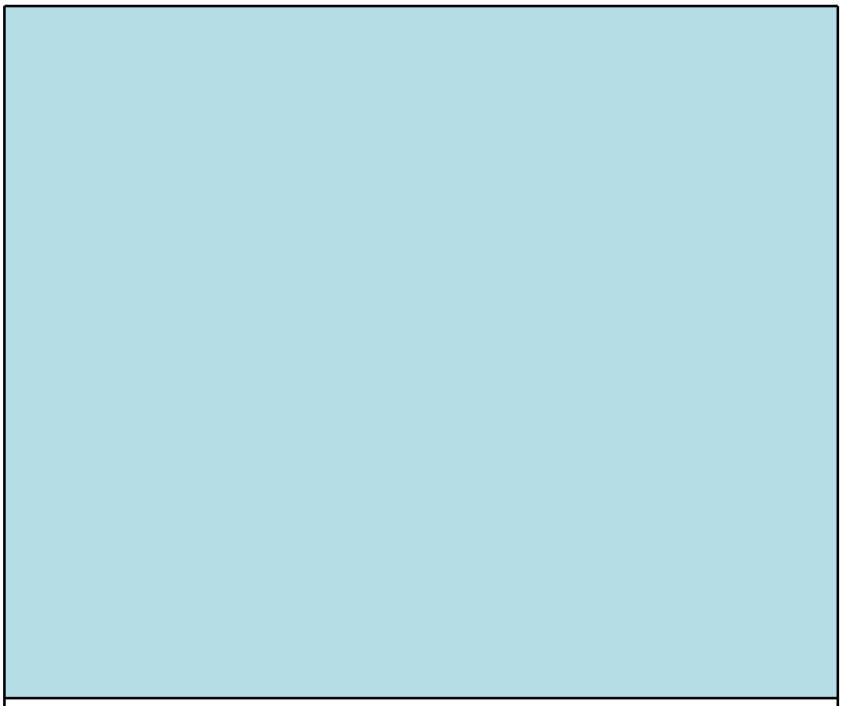


Luvussa 11 määrättäisiin turvajärjestelyistä kuljetuksissa. Kuljetusten turvajärjestelyiden tavoitteena on turvata kuljetus lainvastaiselta toiminnalta. Keskeisenä tavoitteena on varautua torjumaan anastus- ja sabotaasiuhka. Kuljetusten turvaamisen osa-alueet ovat lainvastaisen toiminnan ennalta ehkäiseminen, havaitseminen ja viivyttäminen sekä vaste lainvastaiseen toimintaan. Vasteeseen kuuluvat lainvastaisen toiminnan pysäyttäminen, tilanteen hallintaan saattaminen, seurausten estäminen ja rajoittaminen. Toiminnanharjoittajan on avustettava viranomaisia erityistilanteessa erityisesti säteilyseurausten estämisessä ja rajoittamisessa sekä kadonneen tai varastetun ydinaineen tai -jätteen takaisin saamisessa. Kansainvälisiin kuljetuksiin sovelletaan ACPPNM-sopimuksen määräyksiä. Pykälässä esitettäisiin soveltamisala. Vaatimuksia sovelletaan myös kuljetukseen liittyvään tilapäiseen säilytykseen aivan kuten VAK-lainsäädännössä. ACPPNM-sopimuksen liite 1 (Annex I) sisältää myös vaatimuksia, jotka koskevat tilapäistä säilytystä.



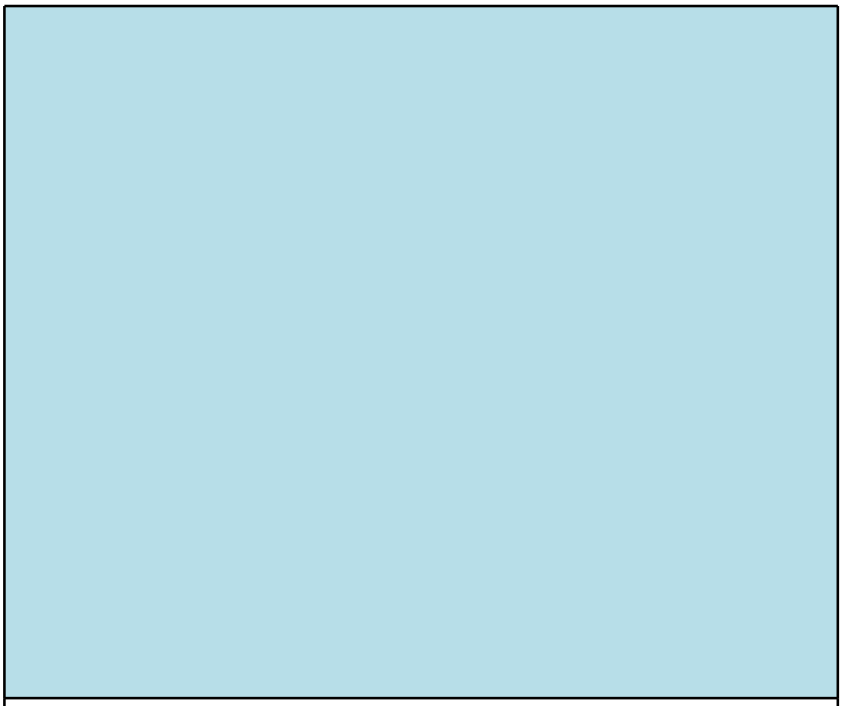
Pykälän 1 momentissa määrättäisiin vastaanottajan valmiudesta vastaanottaa kuljetus. Vastaanottajan valmiudesta on varmistuttava, jotta tähän liittyvät vastaanottajan roolit ja vastuut ovat selkeät. Vaatimus perustuu kansainvälisiin suosituksiin (IAEA NSS 13, INFCIRC/225/Rev. 5).

Pykälän 2 momentissa määrättäisiin kuljetukseen liittyvistä ilmoituksista sekä tiedosta kuljetuksen kulusta. Luvanhaltijalla on oltava ajantasainen tieto kuljetuksen sijainnista mahdollisten kuljetukseen liittyvien poikkeamien havaitsemiseksi ja poikkeamaan liittyvien toimenpiteiden käynnistämiseksi. Vaatimus liittyy valtioiden välisiin toimivaltakysymyksiin kansainvälisissä kuljetuksissa (ACPPNM).
Pykälän 3 momentissa määrättäisiin kuljetuksen yhteyskeskuksesta. Ydinaineen ja ydinjätteen kuljetukset ovat erityistilanteita (liikkuva tilanne), minkä vuoksi reaaliaikaisen yhteydenpidon varmistamisen tarve korostuu (erityisesti uhkatilanteissa). Yhteyskeskuksen suojauksella varmistetaan, että mahdollisen kuljetukseen kohdistuvan lainvastaisen toiminnan yhteydessä yhteyskeskuksen toimintakyky säilytetään ja kuljetuksen paikantaminen ja yhteydenpito mahdollistuu (IAEA NSS 13, INFCIRC/225/Rev. 5).
Pykälän 5 momentissa määrättäisiin kuljetusvälineiden turvallisuustarkastuksesta mahdollisen kuljetukseen kohdistuvan lainvastaisen toiminnan ehkäisemiseksi ja paljastamiseksi. Rajatulla alueella tehdyllä turvallisuustarkastuksella, lastauksella, purulla ja tilapäisellä säilytyksellä pyritään ehkäisemään kuljetukseen liittyviä uhkia muodostamalla suojavyöhyke turvattavalle kuljetukselle. Rajattu alue mahdollistaa myös asiattomien henkilöiden havainnoinnin ja näiden toimintaan puuttumisen.



Pykälän 1 momentissa määrättäisiin suunnitelmista poikkeamiseen liittyvistä toimenpiteistä, jotta viranomaiset saavat poikkeamisesta tiedon oikea-aikaisesti (IAEA NSS 13, INFCIRC/225/Rev. 5).

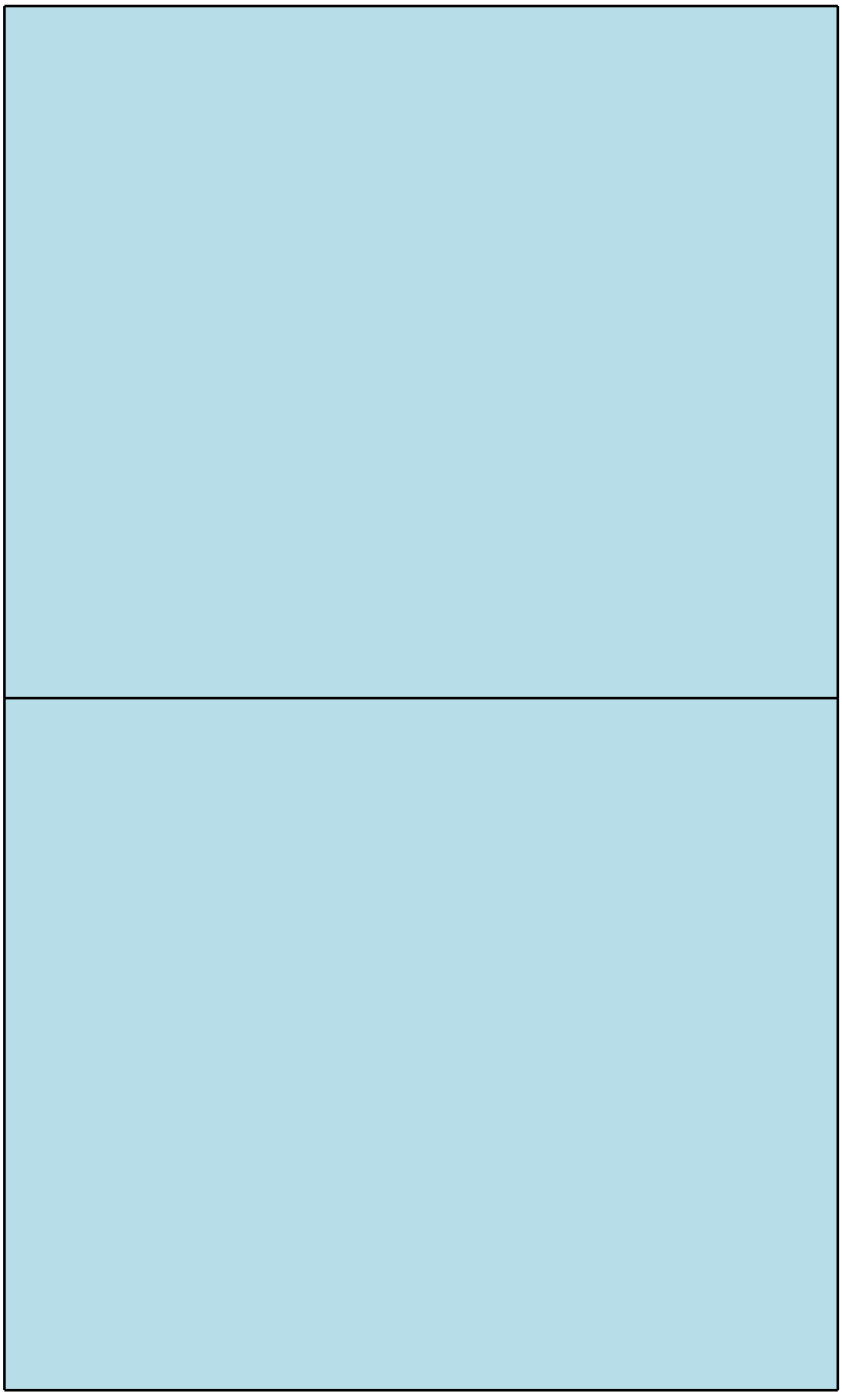
Pykälän 2 momentissa määrättäisiin edellytyksistä, joiden mukaan kuljetuksen olosuhteita tulisi harkita uudelleen. Tällaisia edellytyksiä ovat erityisesti (tiedustelu)tiedot kuljetukseen mahdollisesti kohdistuvasta turvallisuusuhasta tai tiedot kuljetuksen reittiä koskevista sää- tai muista olosuhteista, joiden vuoksi muutoksia kuljetukseen tulisi arvioida. Kuljetuksella olisi oltava ennalta suunniteltuja varareittejä, jotka turvaavat kuljetuksen perille saapumisen, mikäli ensisijaisen reitin havaitaan turvallisuusuhkien tai muun syyn takia olevan sellainen, että se ei ole käytettävissä (IAEA NSS 13, INFCIRC/225/Rev. 5).



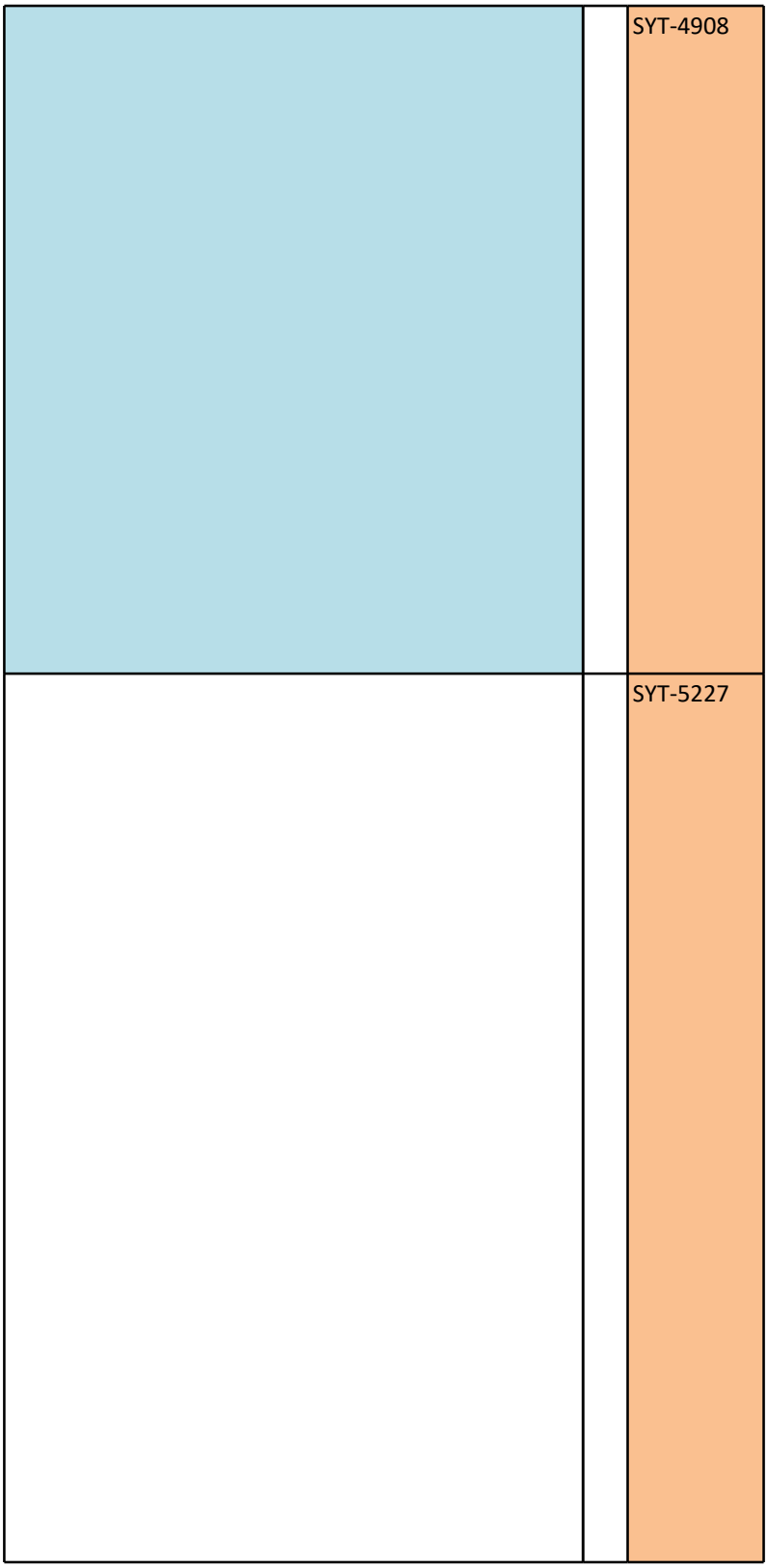
Pykälän 1 momentissa määrättäisiin kuljetusvälineen luvattoman käytön estämisestä teknisillä menetelmillä. Tekninen ajonestojärjestelmä estää kuljetusvälineen käynnistämisen ja/tai muuten sen liikkeelle saattamisen sekä mahdollistaa luvattoman käyttöyrityksen havaitsemisen ja toimintaan puuttumisen. Se on osa syvyyspuolustusta operatiivisen vasteen lisäksi (IAEA NSS 13, INFCIRC/225/Rev. 5).

Pykälän 2 momentissa määrättäisiin käytetyn ydinpolttoaineen ja muun suojaluokkien II ja I ydinaineen kuljetusten erityisvaatimuksista. Nämä vaatimukset perustuvat kansainvälisiin suosituksiin (IAEA NSS 13, INFCIRC/225/Rev. 5). Yksinkäytössä tarkoittaa yhdeltä lähettäjältä tulevaa kuormaa, jonka lähettäjä lähettää yksinomaan käyttöönsä varatussa ajoneuvossa tai kontissa. Se ei välttämättä ole kuljetusvälineen ainoa lasti, mikä edellytetään suojaluokan I ydinaineelle.

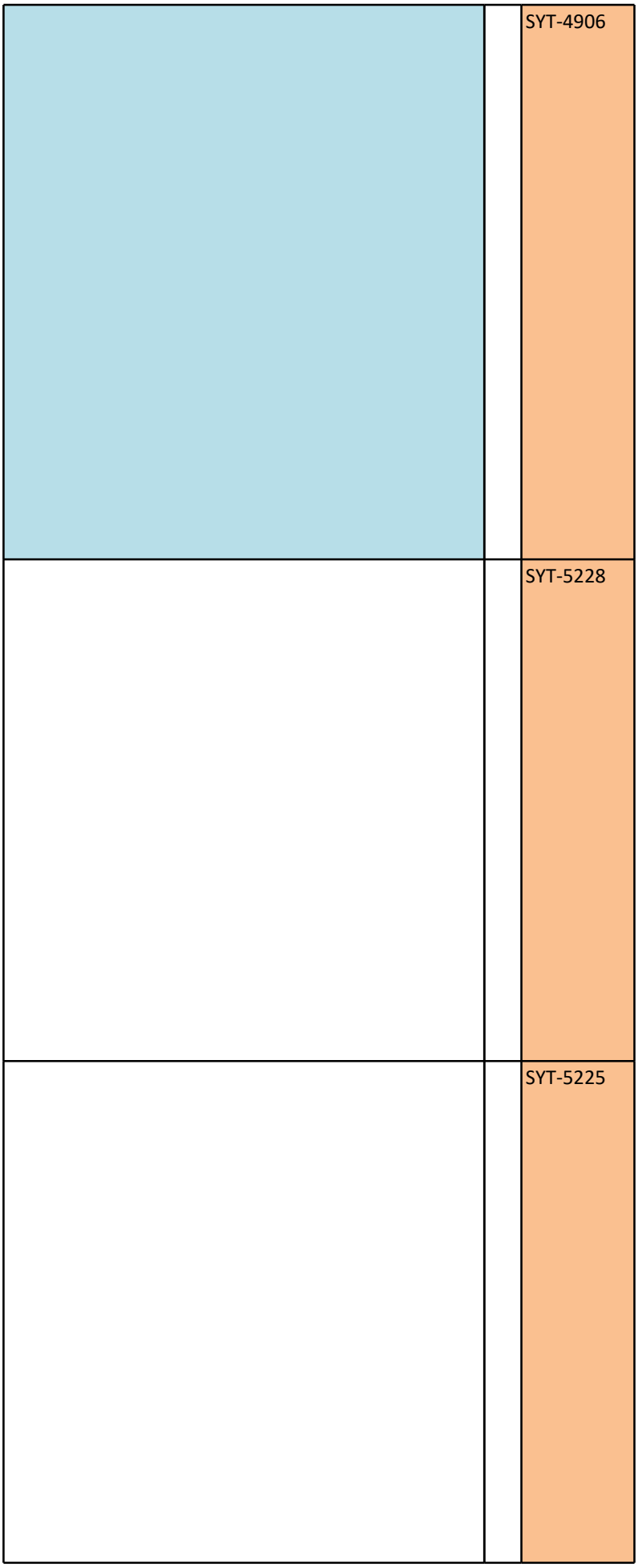
Pykälän 3 momentissa määrättäisiin suojaluokan I ydinaineen kuljetusta koskevasta ilmoitusvelvollisuudesta Säteilyturvakeskukselle. Ajantasaisen tilannekuvan ylläpitämiseksi ja muiden velvoitteiden täyttämiseksi on tärkeätä, että Säteilyturvakeskus on tietoinen suojaluokan I ydinaineen kuljetuksista. Vaatimus perustuu kansainvälisiin suosituksiin (IAEA NSS 13, INFCIRC/225/Rev. 5).



Poikkeama-/siirtymäsäännöstarve		ID
		SYT-4909
		SYT-4910

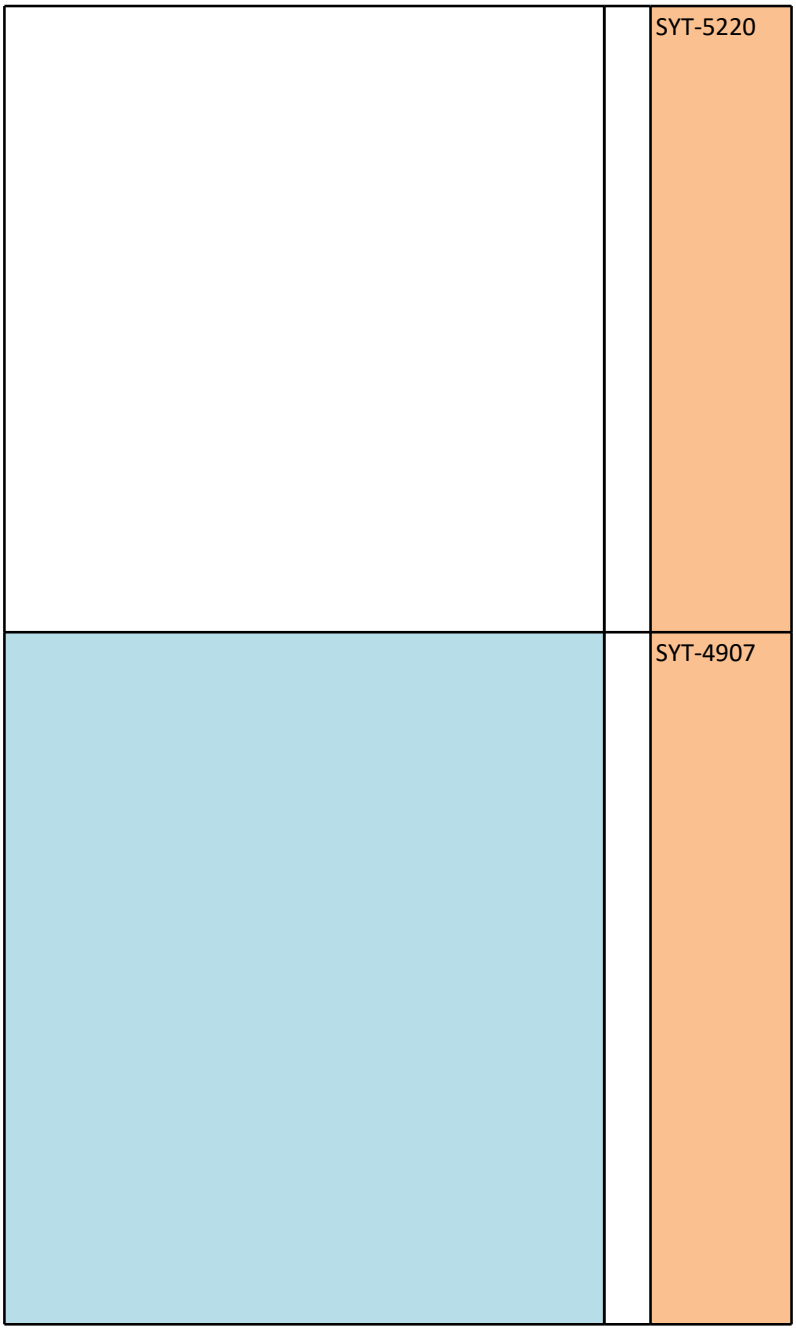

SYT-4908
SYT-5227

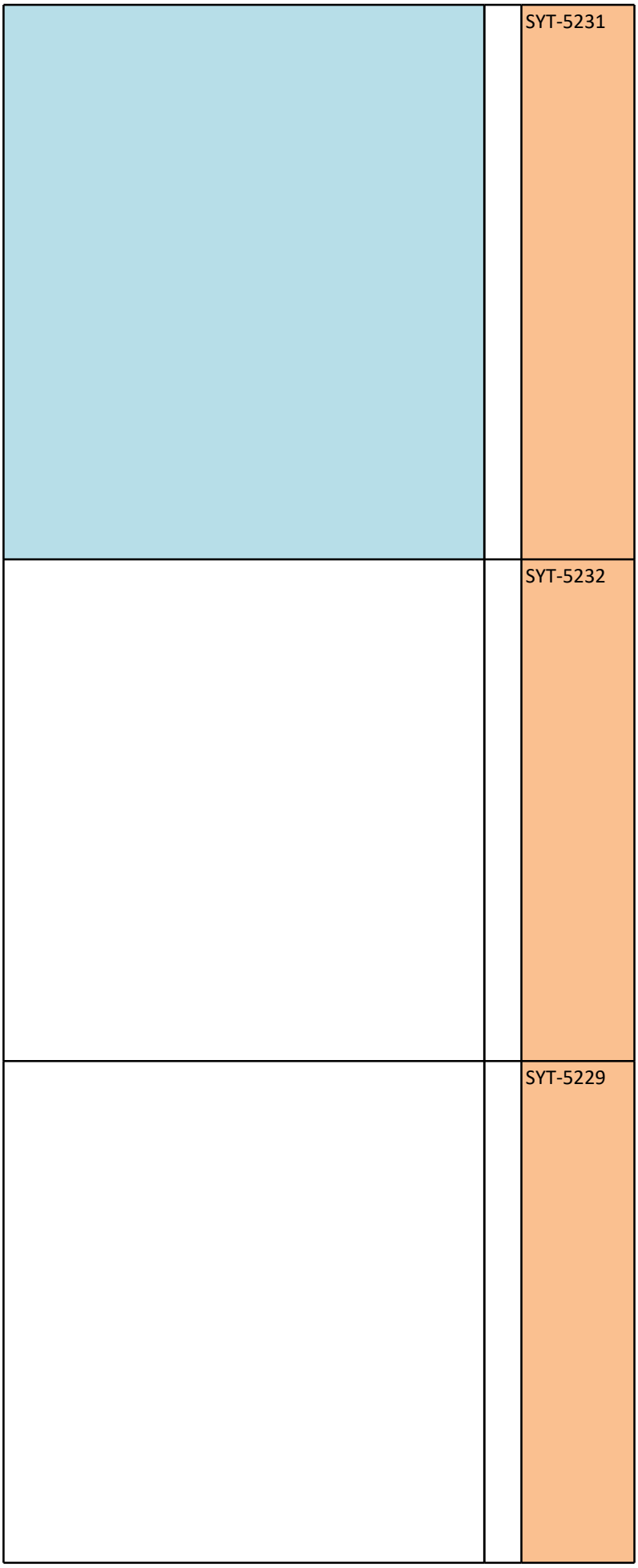
		SYT-6089
		SYT-6090
		SYT-6088

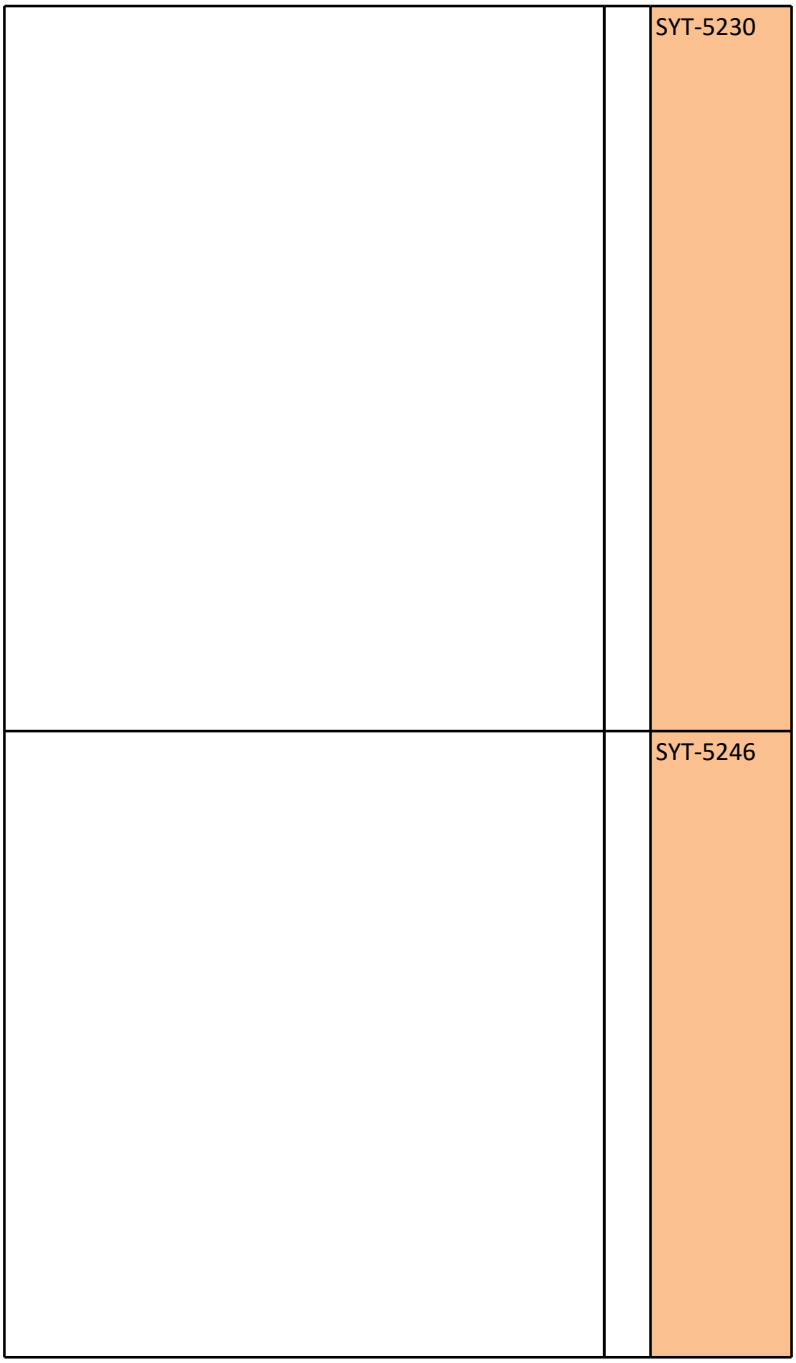

SYT-4906
SYT-5228
SYT-5225

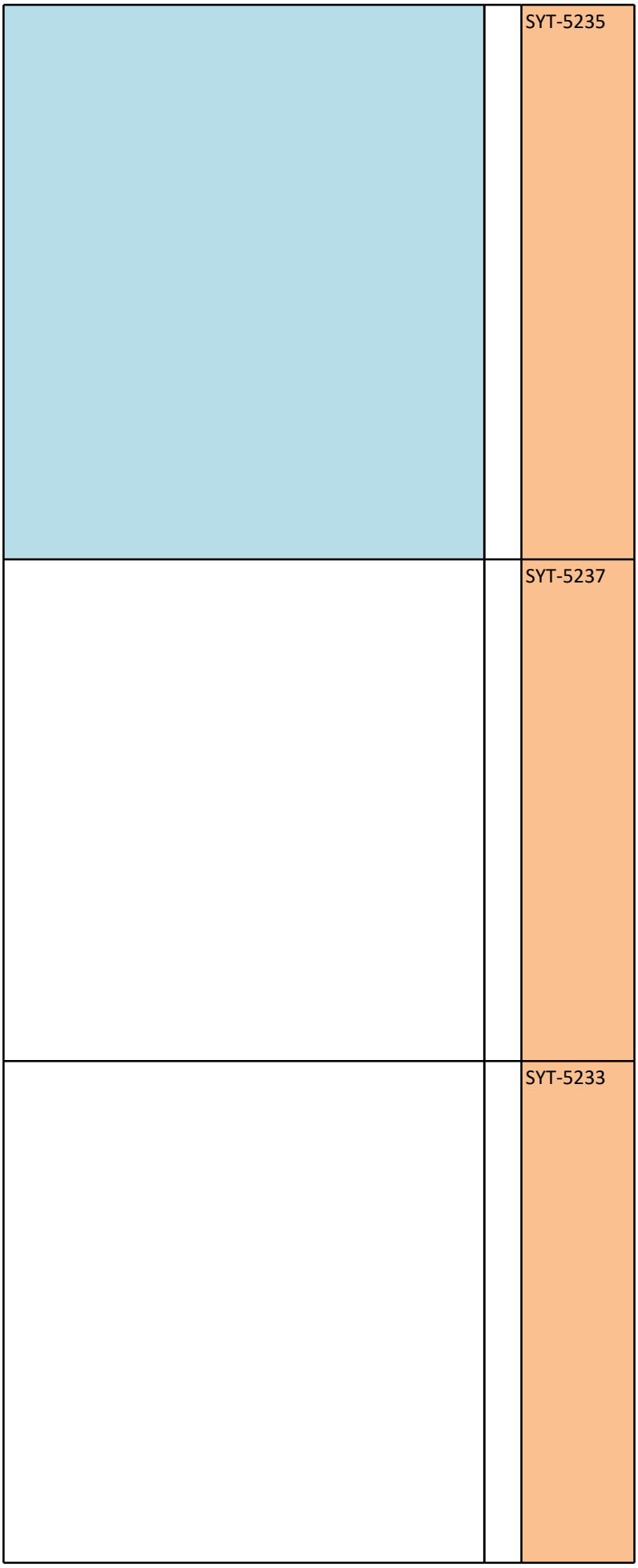
		SYT-5226
		SYT-5223
		SYT-5224

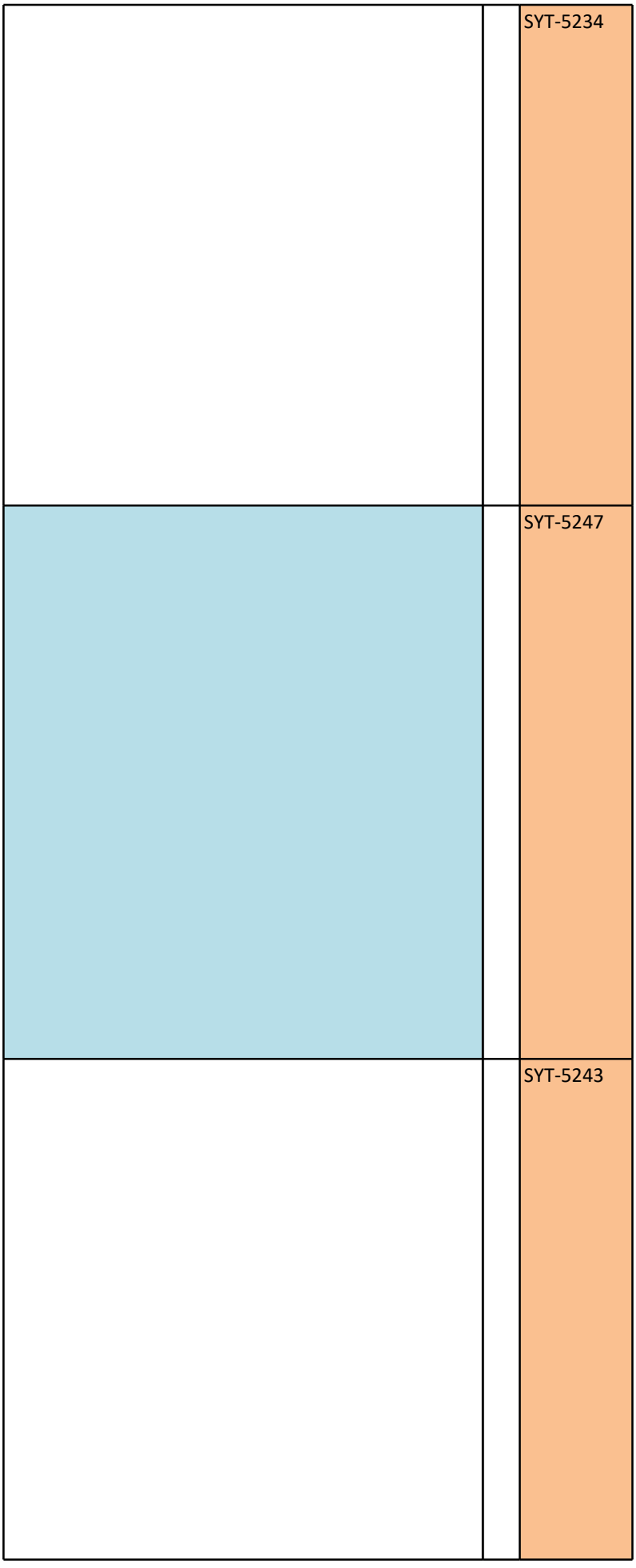
		SYT-5221
		SYT-5222
		SYT-5219

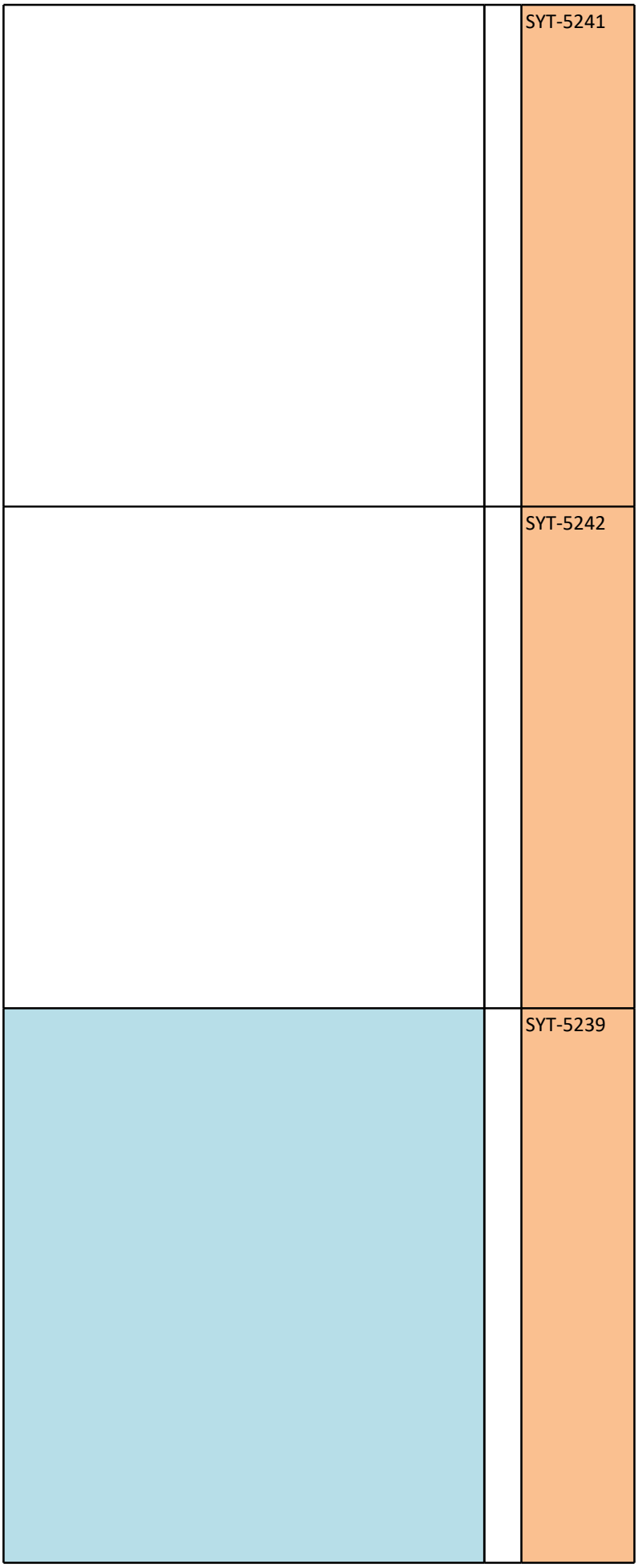

SYT-5220
SYT-4907


SYT-5231
SYT-5232
SYT-5229

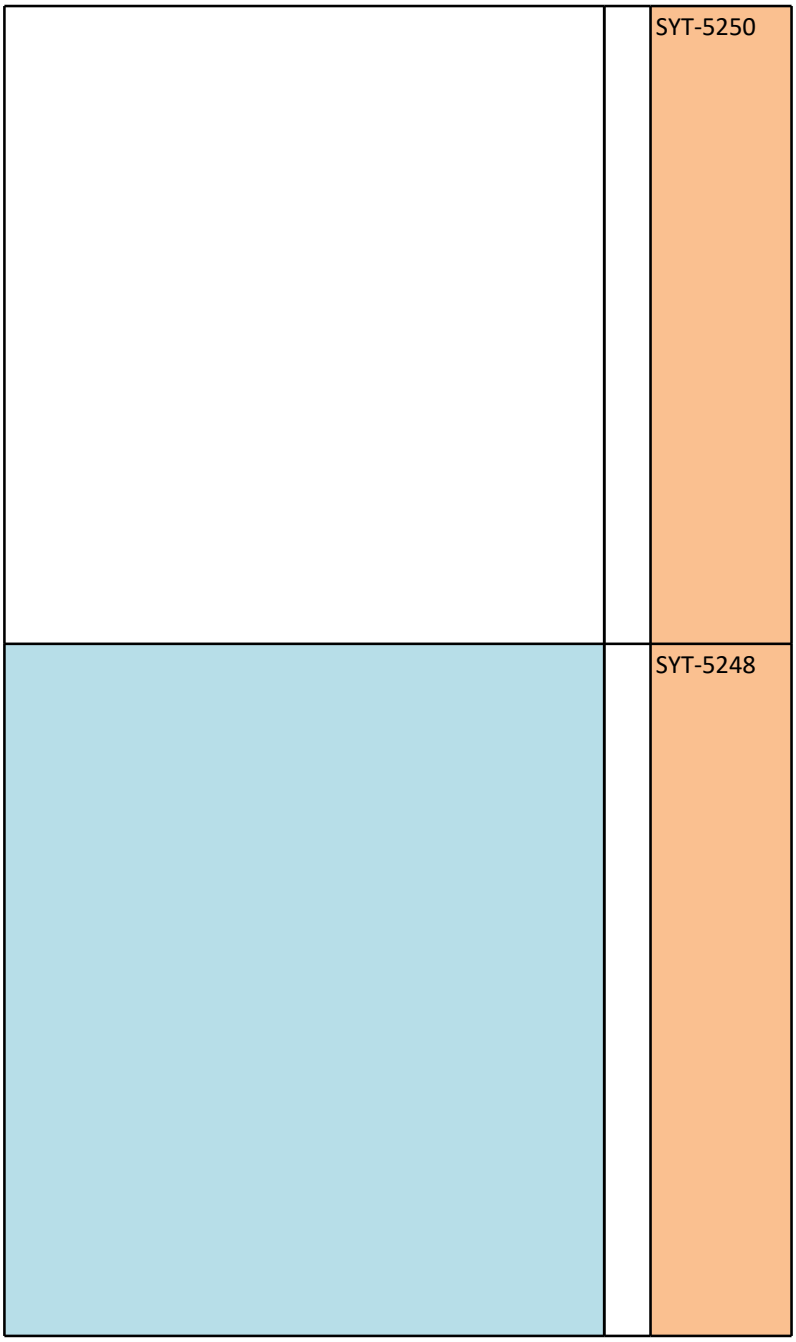

SYT-5230
SYT-5246

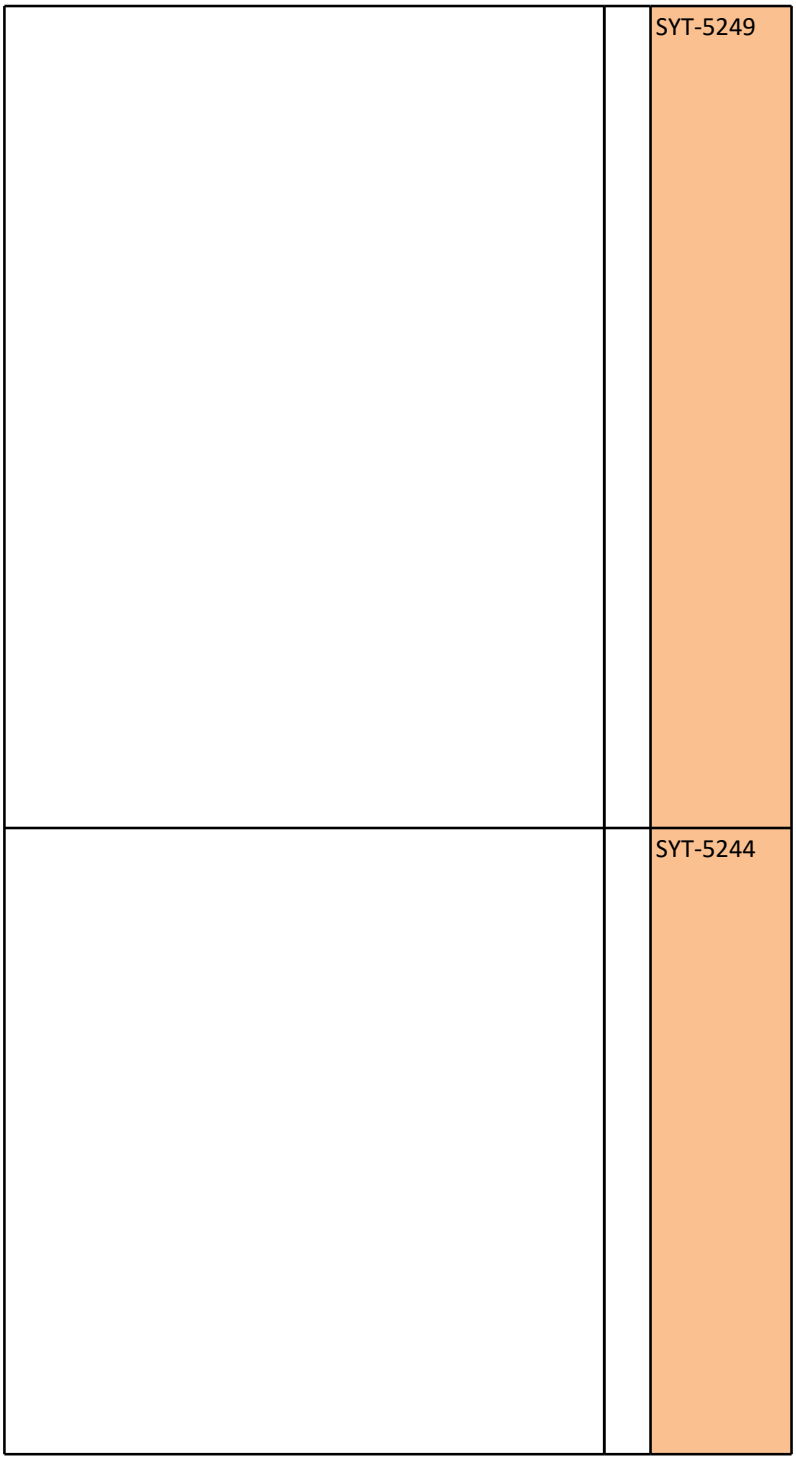

SYT-5235
SYT-5237
SYT-5233

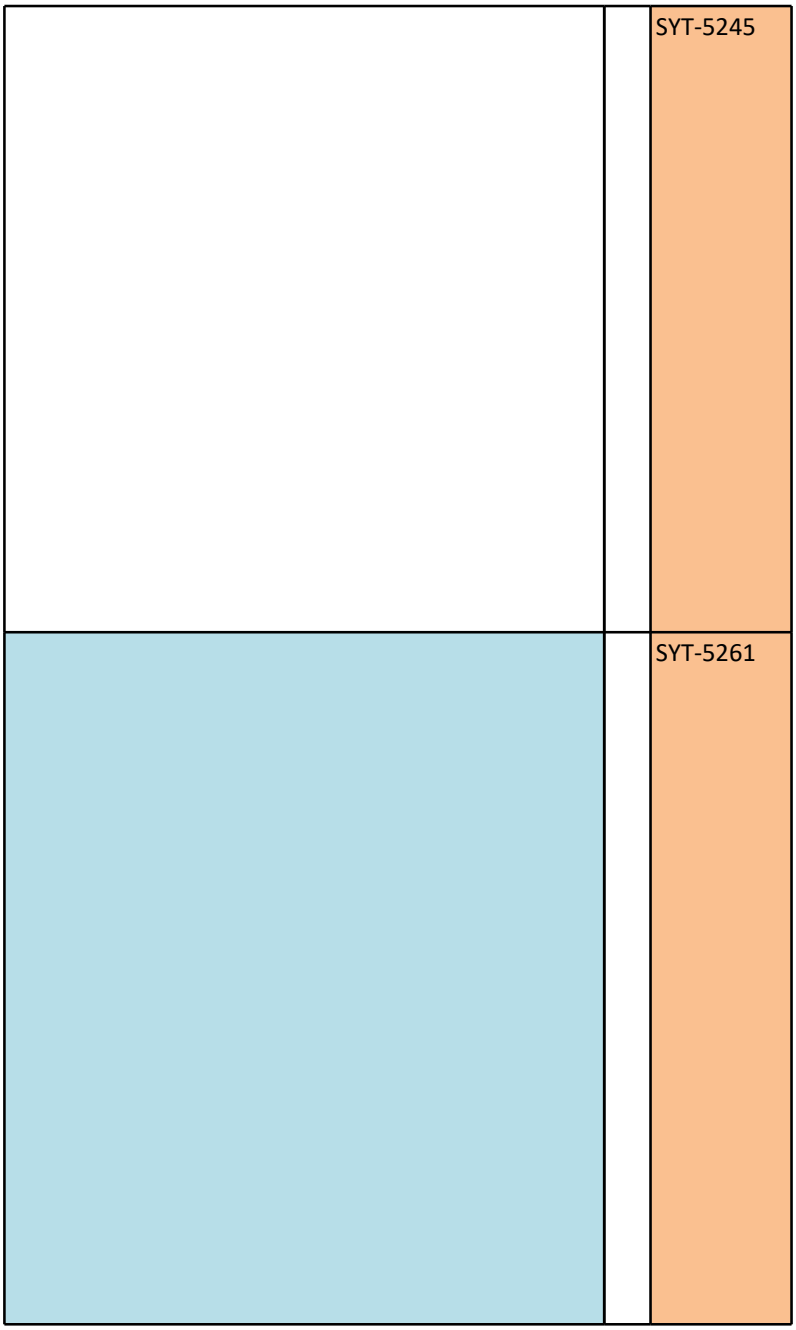

SYT-5234
SYT-5247
SYT-5243

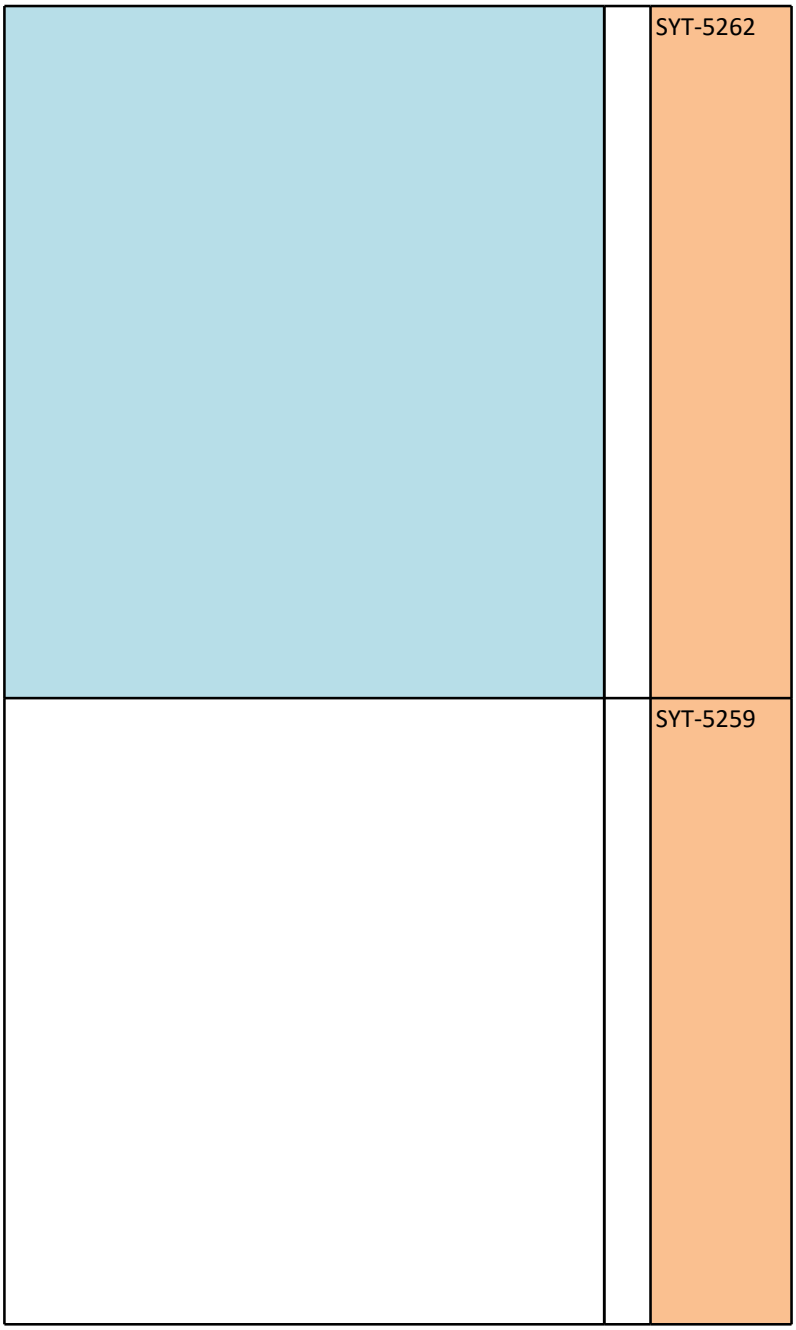

SYT-5241
SYT-5242
SYT-5239

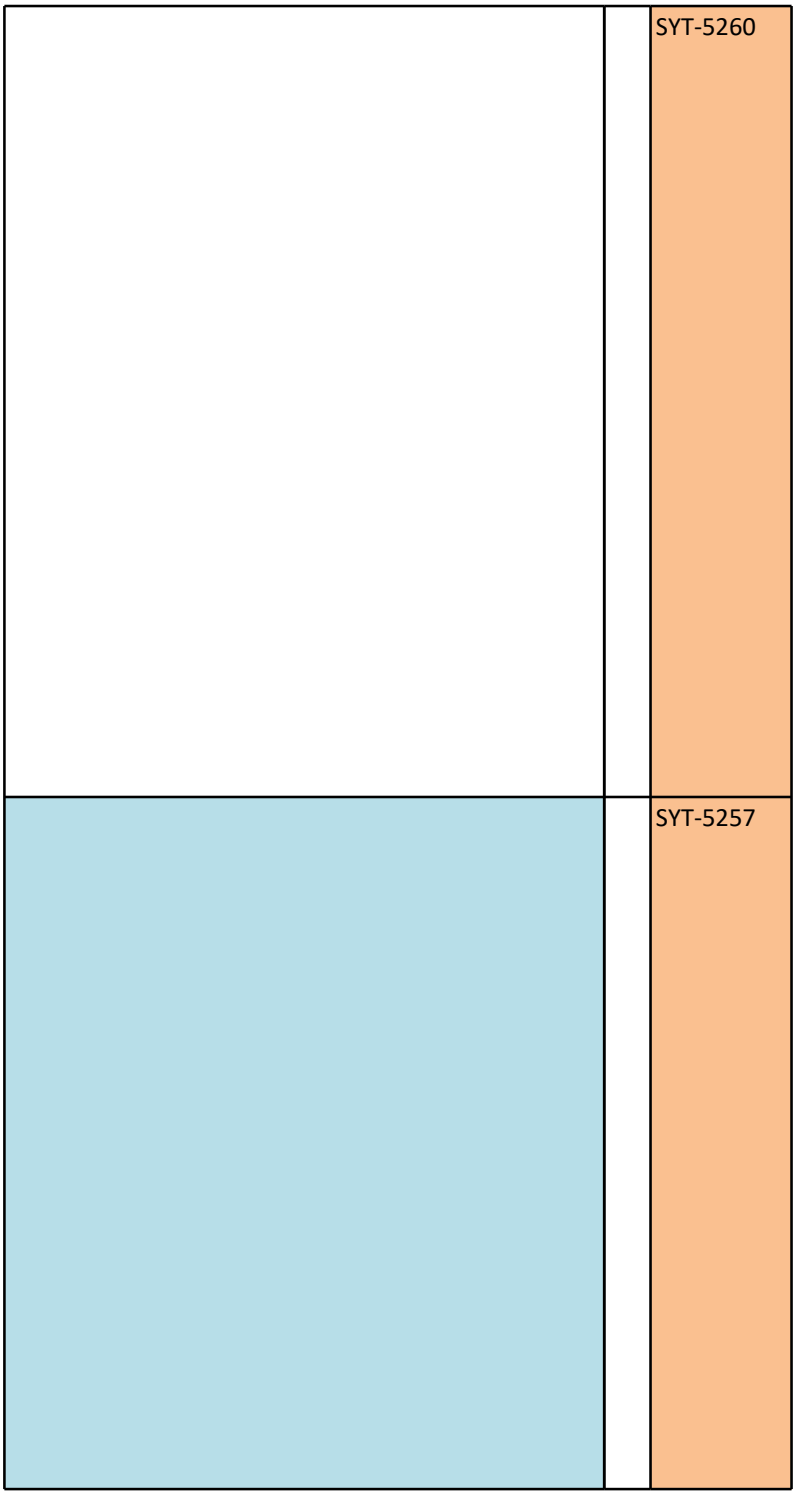
		SYT-5240
		SYT-5236
		SYT-5238

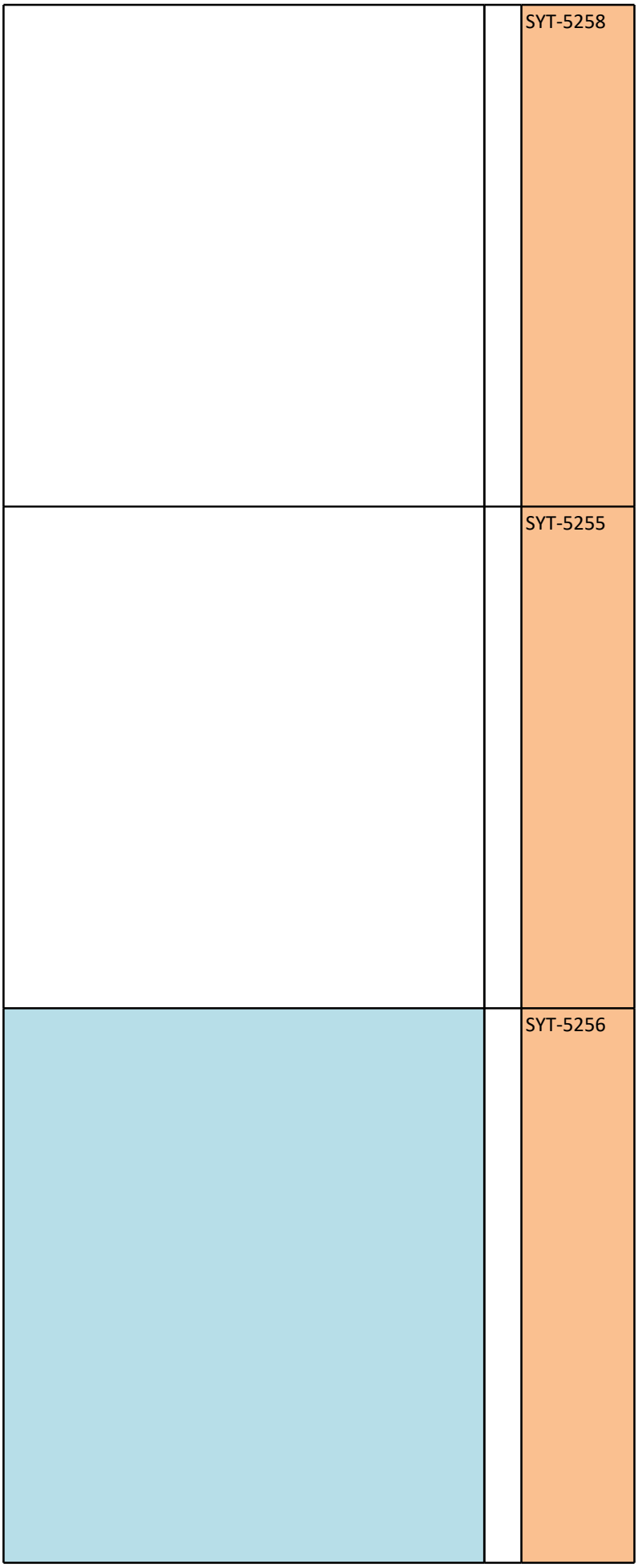

SYT-5250
SYT-5248

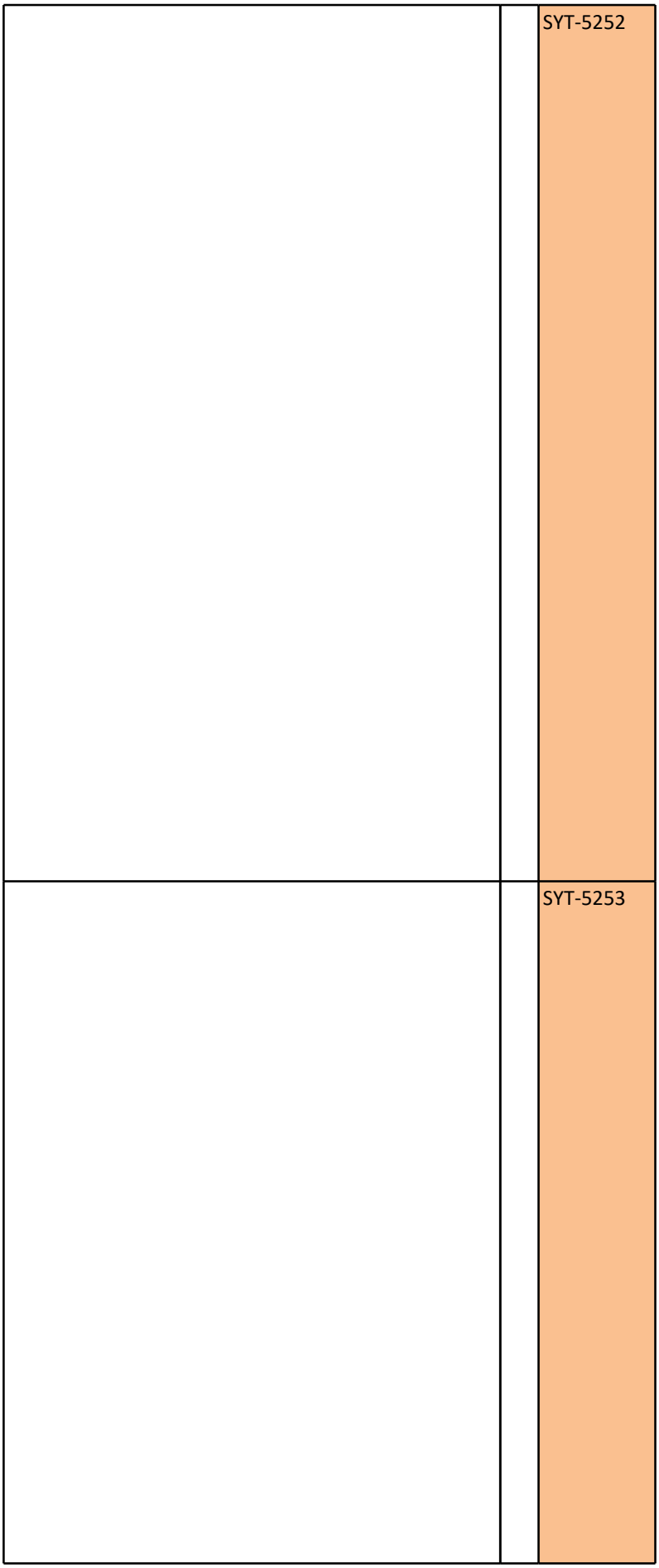

SYT-5249
SYT-5244

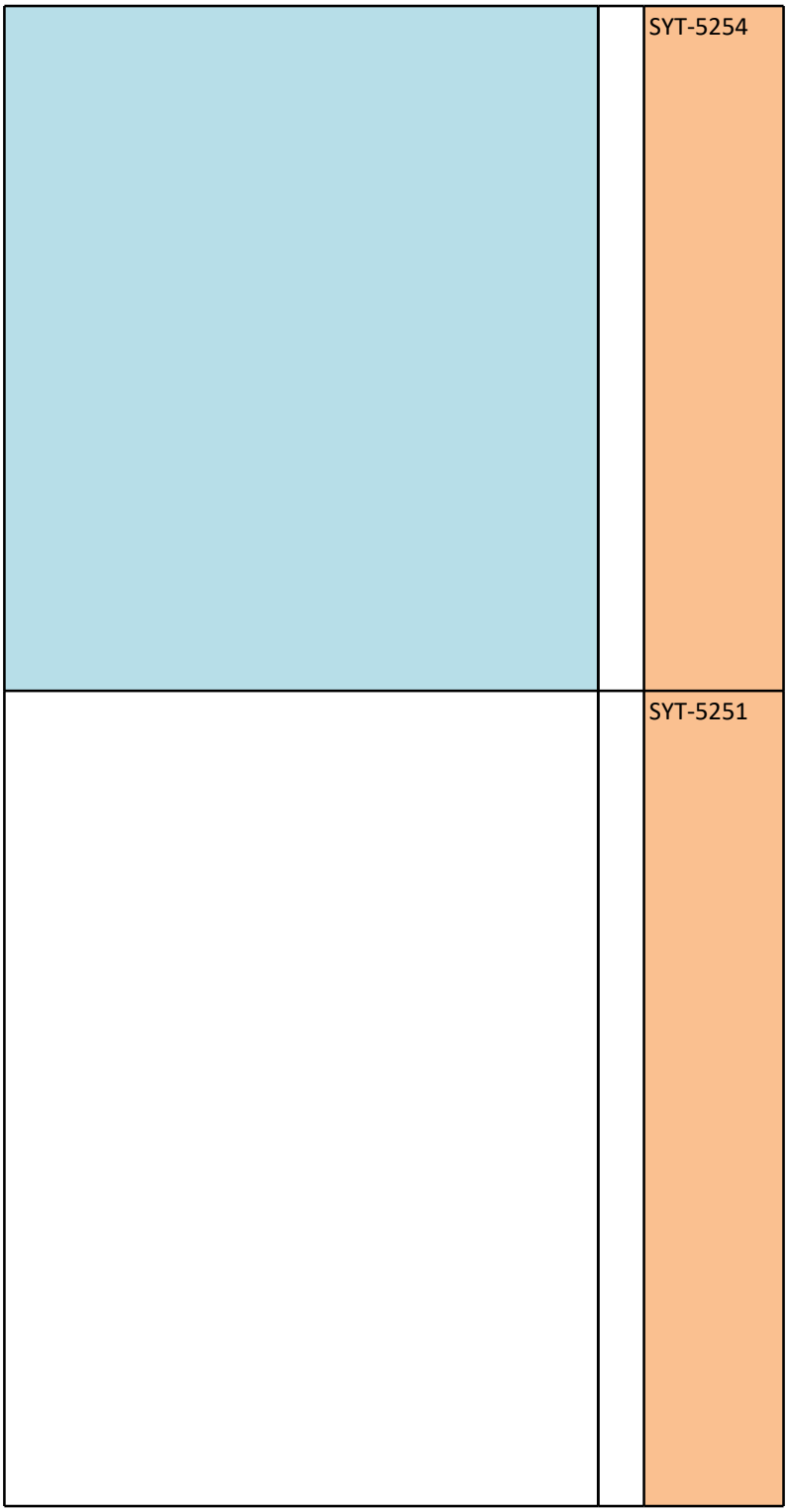

SYT-5245
SYT-5261

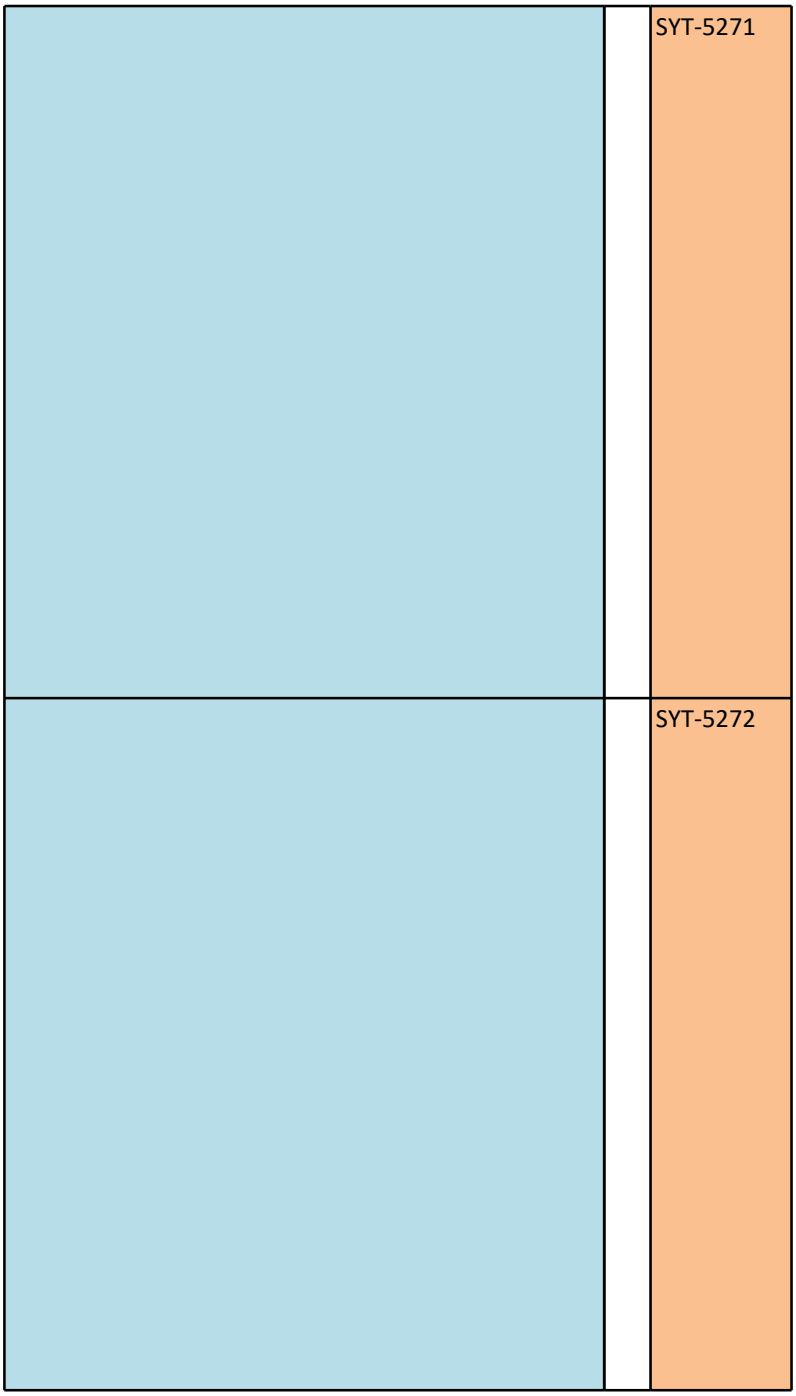

SYT-5262
SYT-5259


SYT-5260
SYT-5257

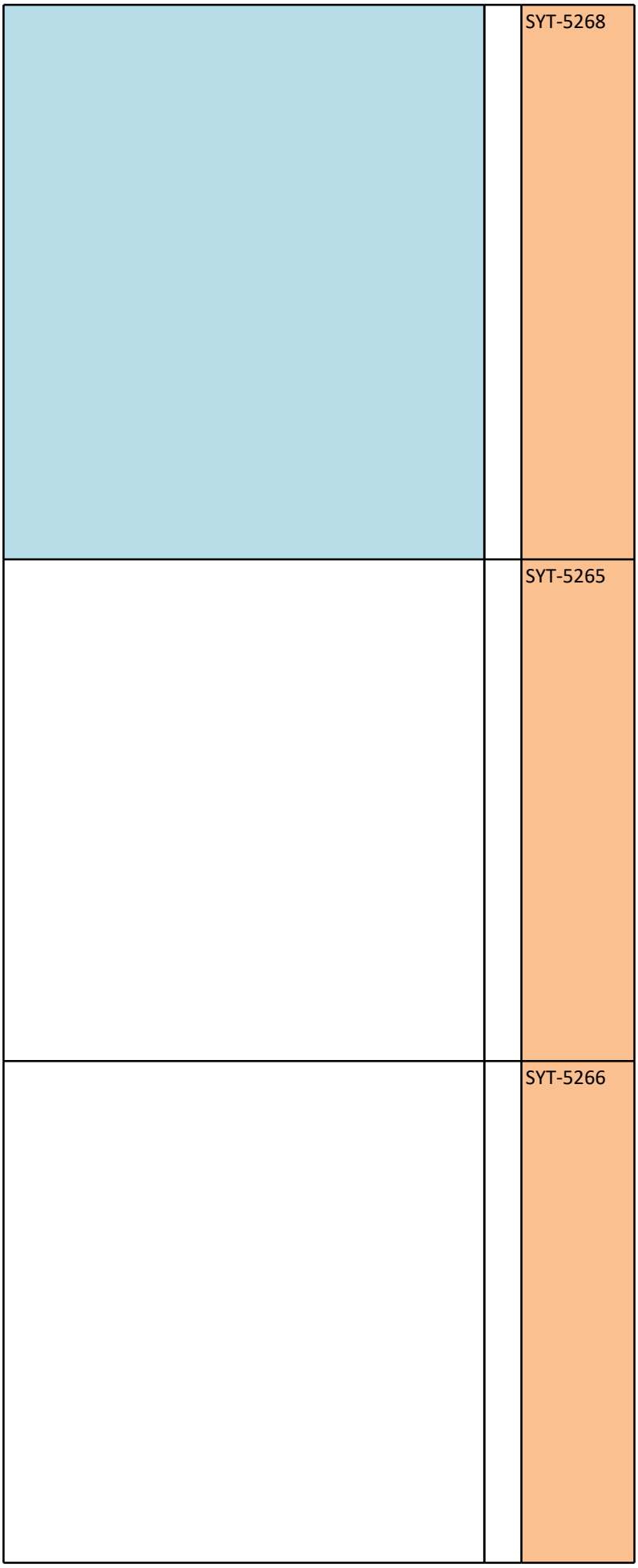

SYT-5258
SYT-5255
SYT-5256

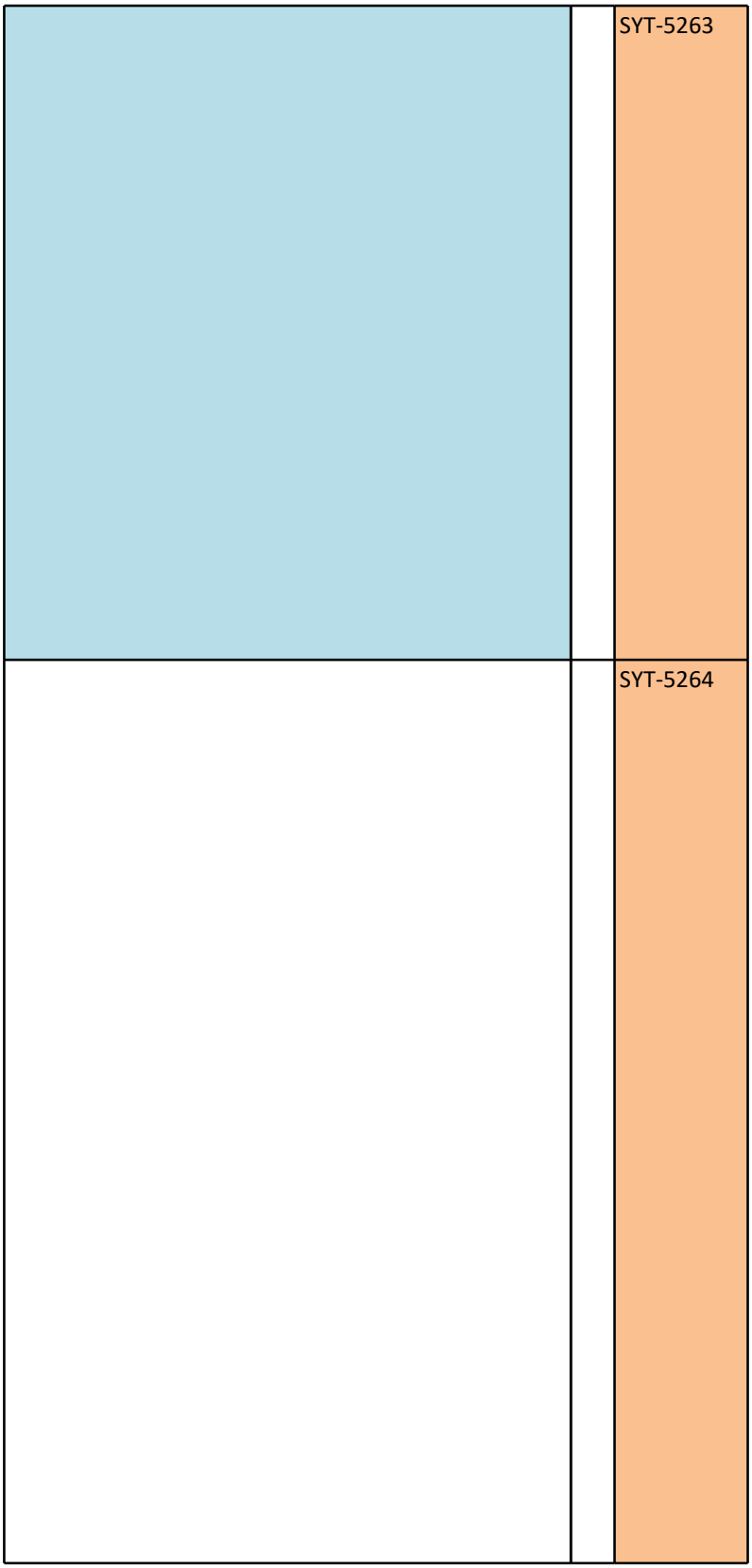

SYT-5252
SYT-5253

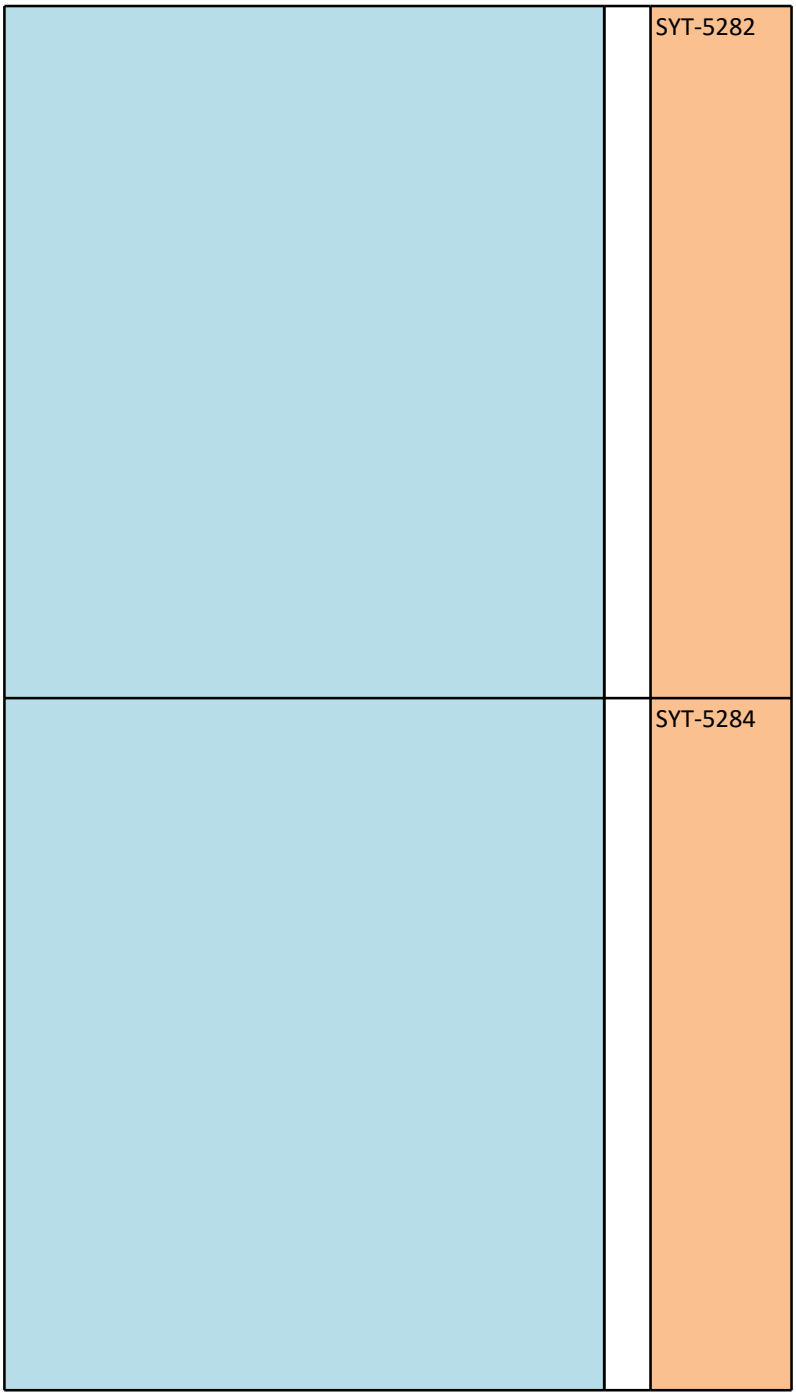

SYT-5254
SYT-5251

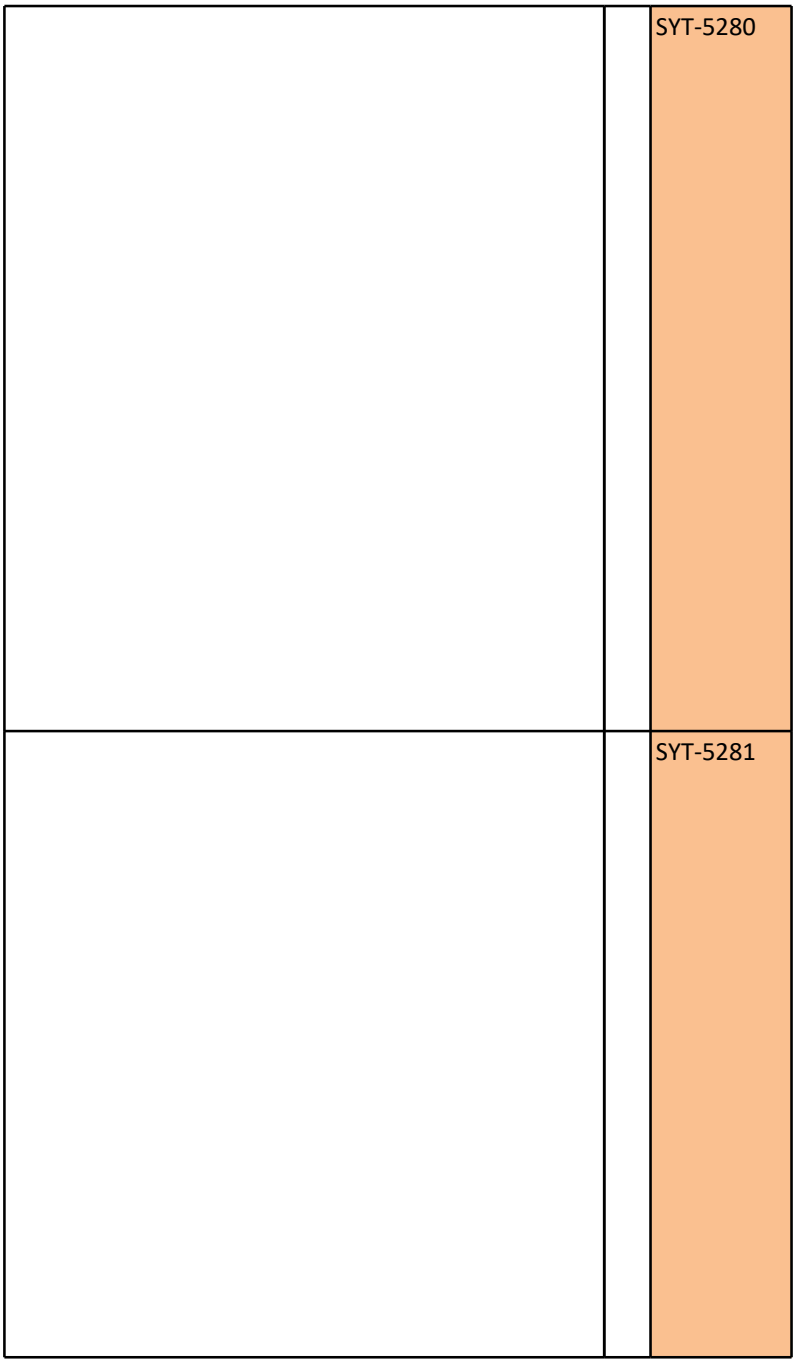

SYT-5271
SYT-5272

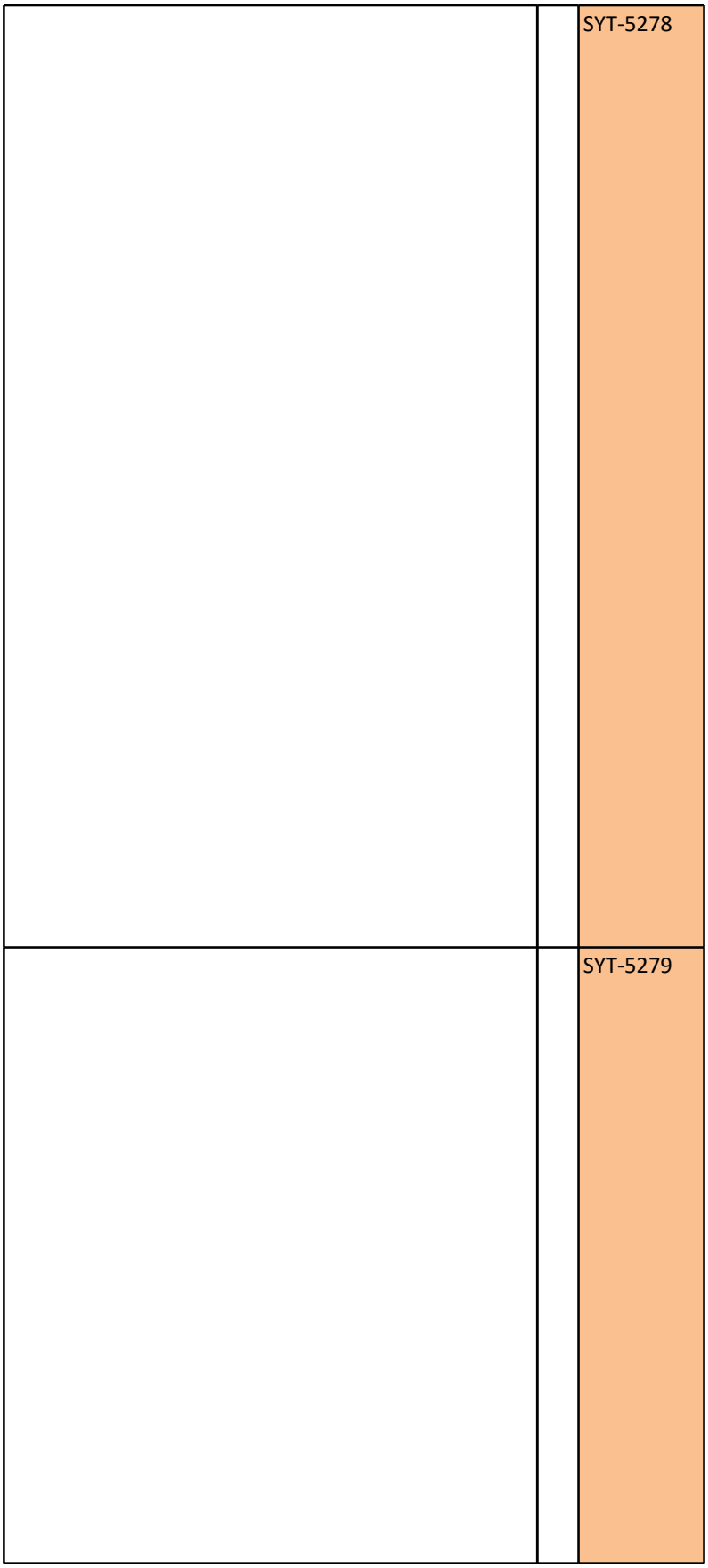
		SYT-5269
		SYT-5270
		SYT-5267

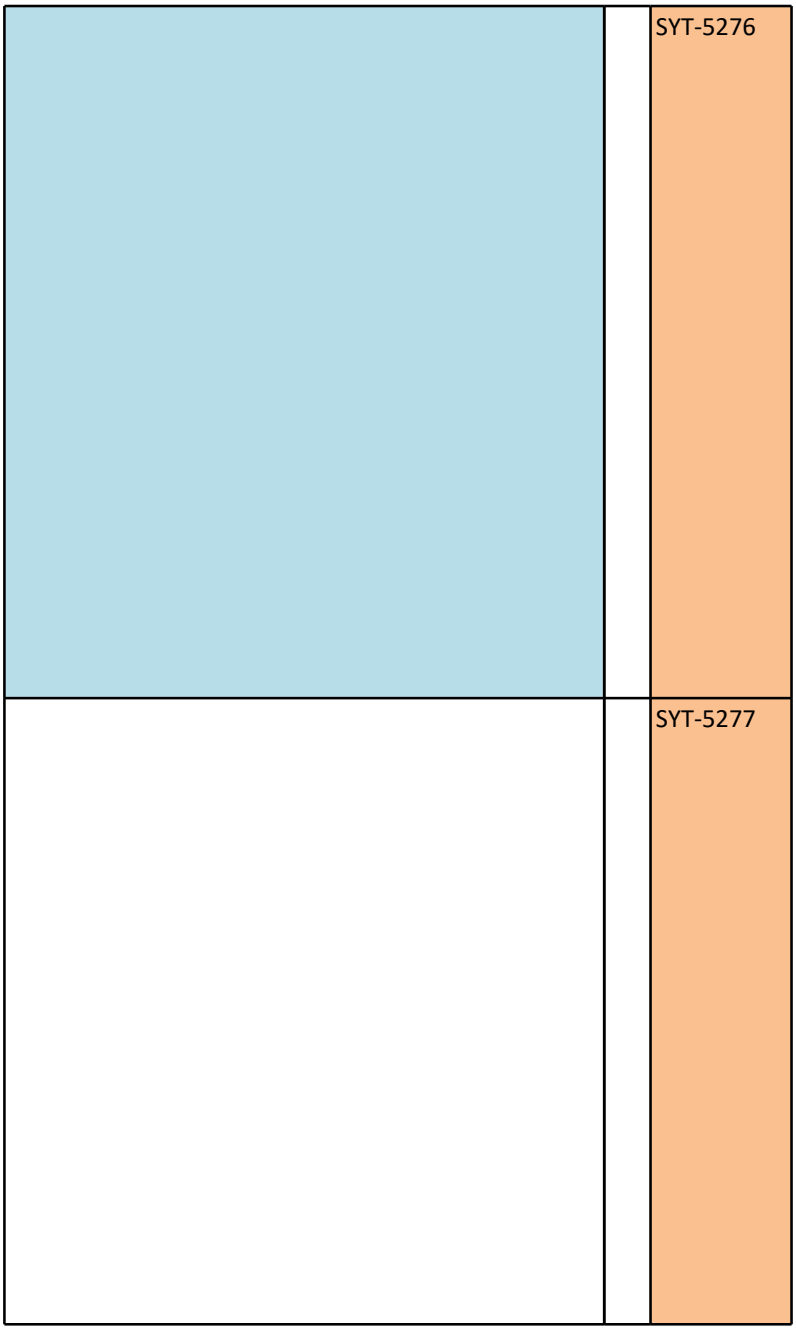

SYT-5268
SYT-5265
SYT-5266

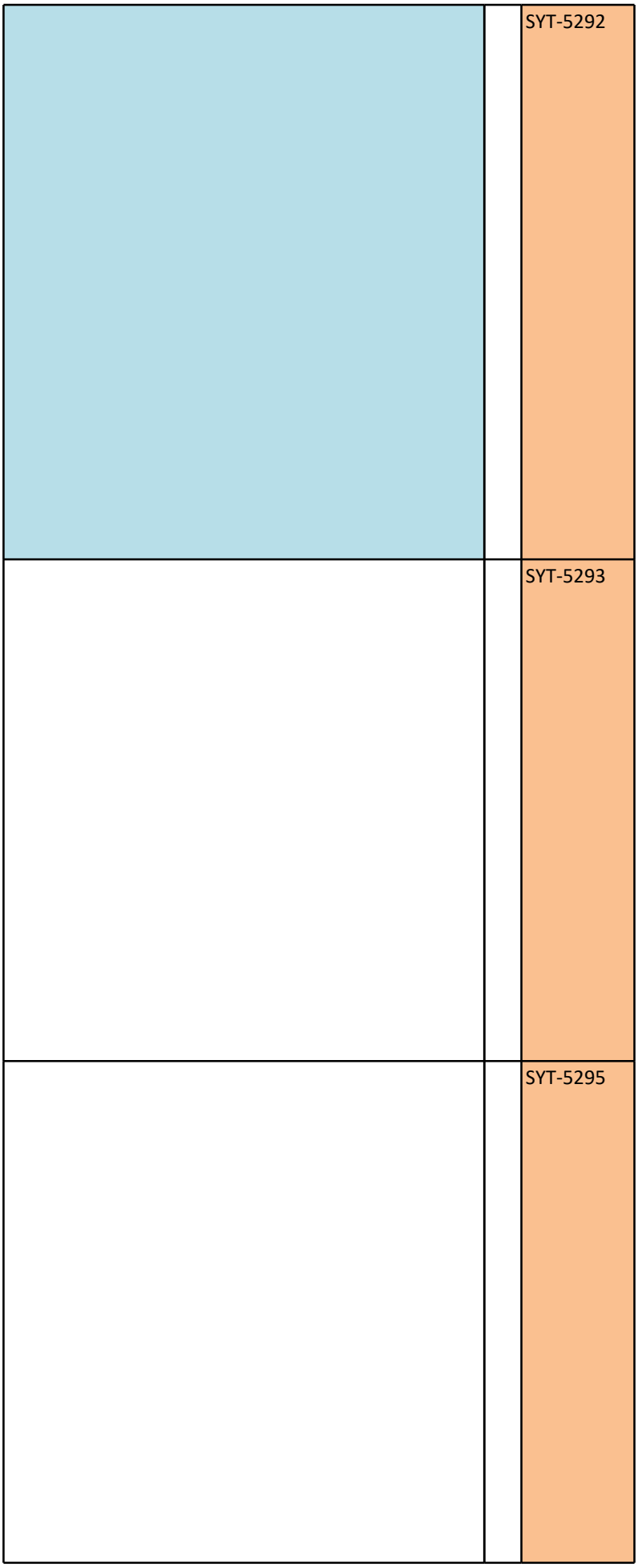

SYT-5263
SYT-5264

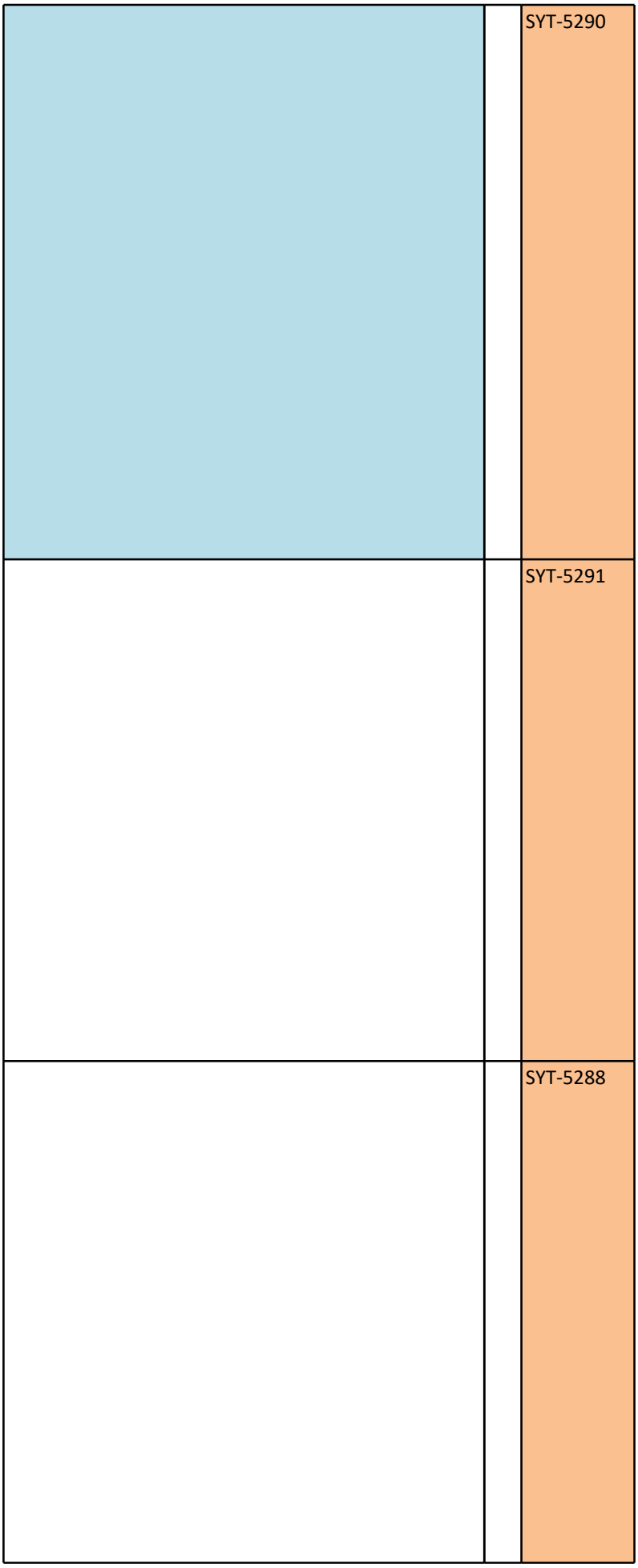

SYT-5282
SYT-5284

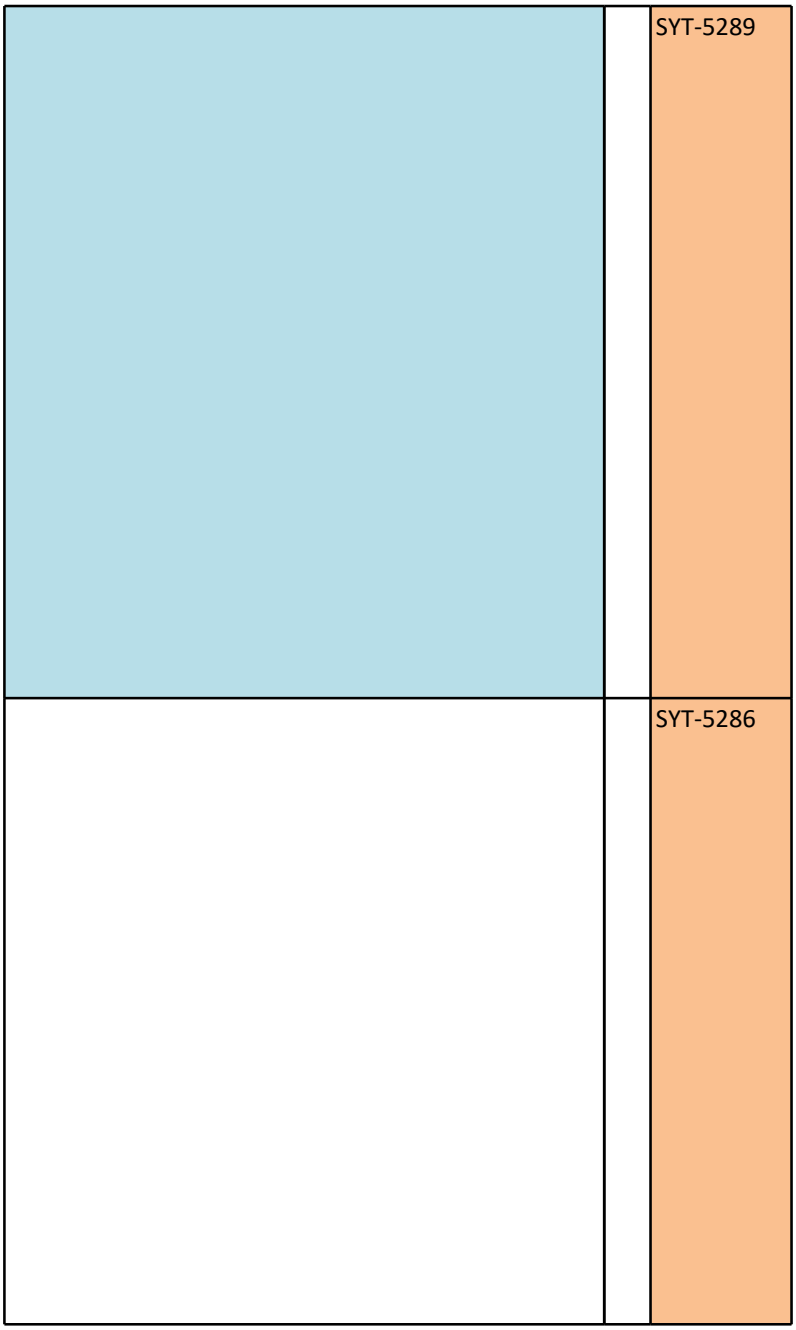

SYT-5280
SYT-5281


SYT-5278
SYT-5279

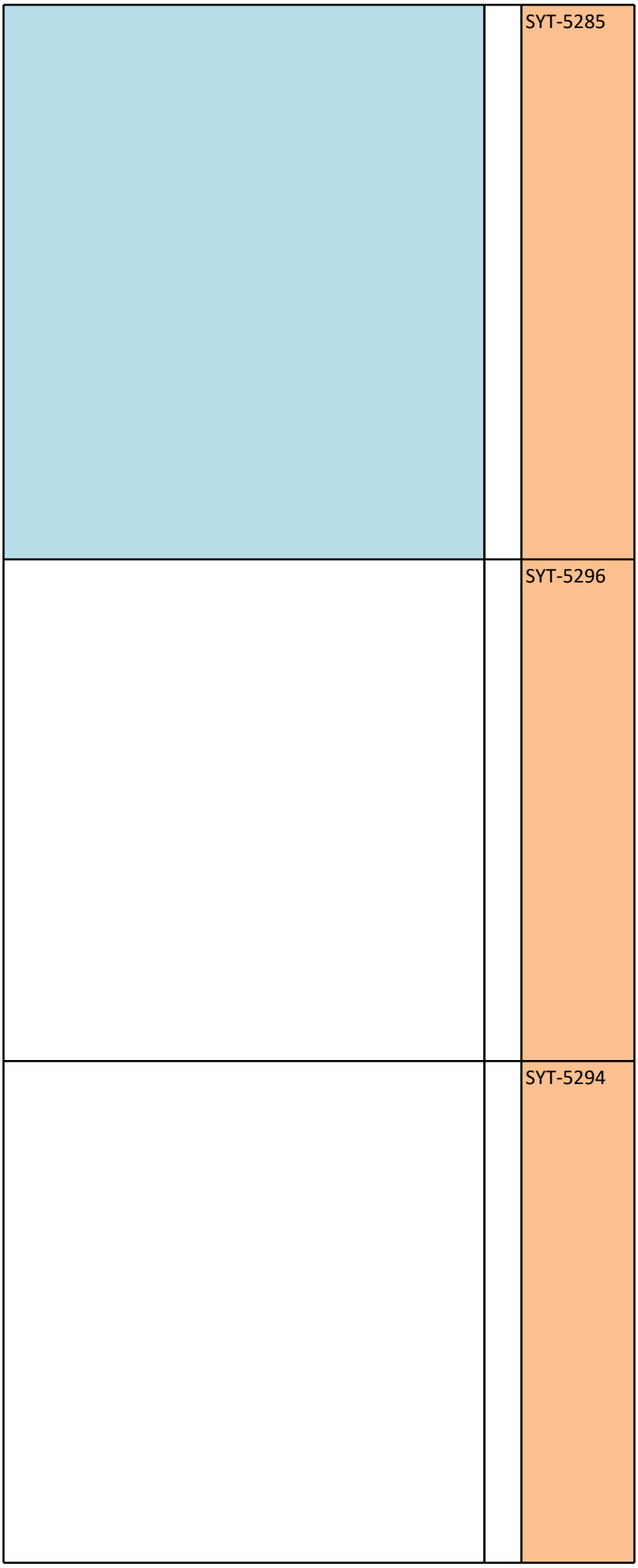

SYT-5276
SYT-5277

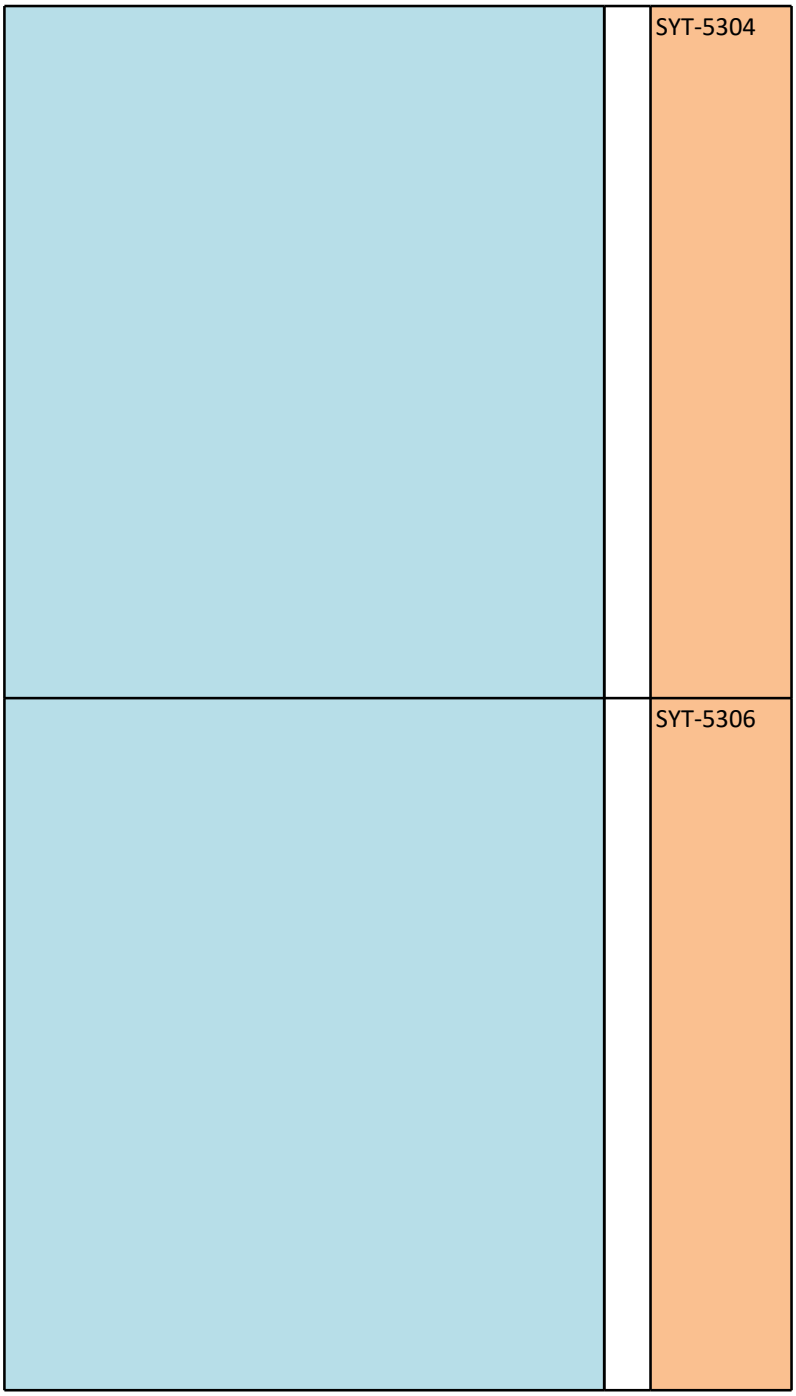

SYT-5292
SYT-5293
SYT-5295

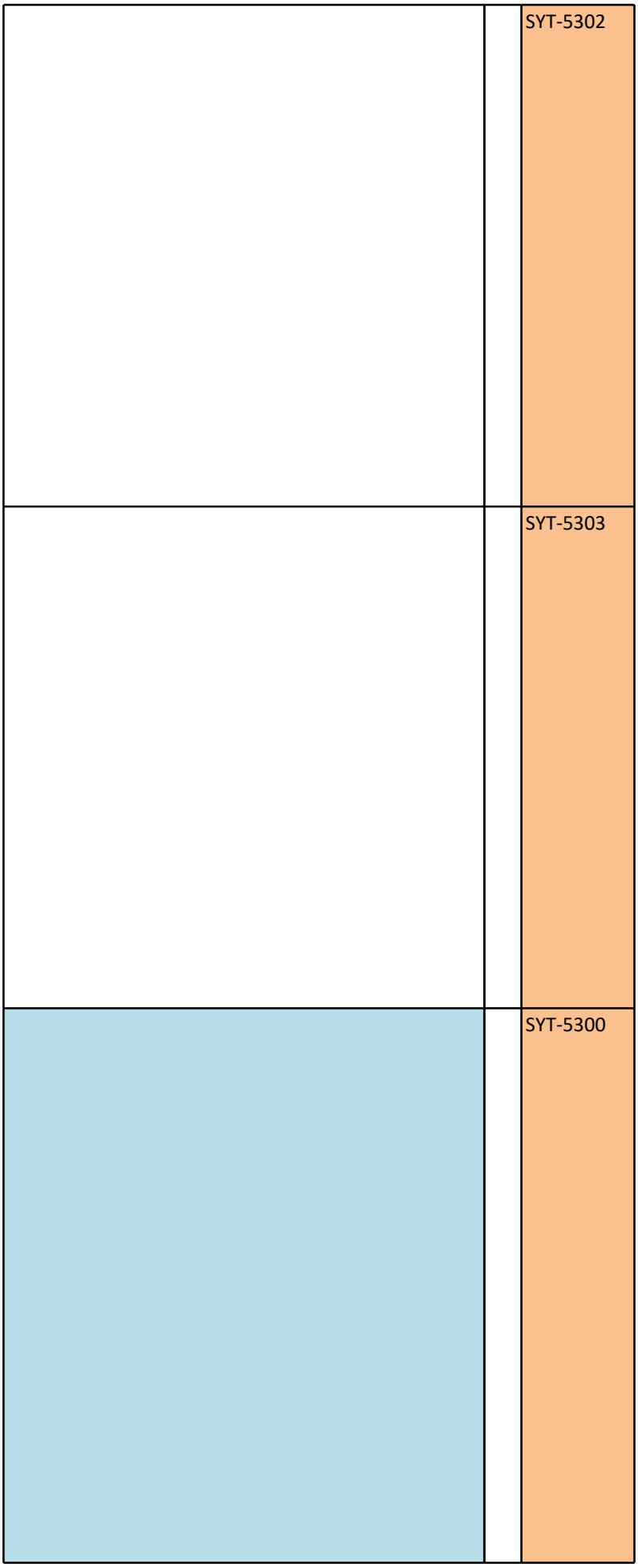

SYT-5290
SYT-5291
SYT-5288


SYT-5289
SYT-5286

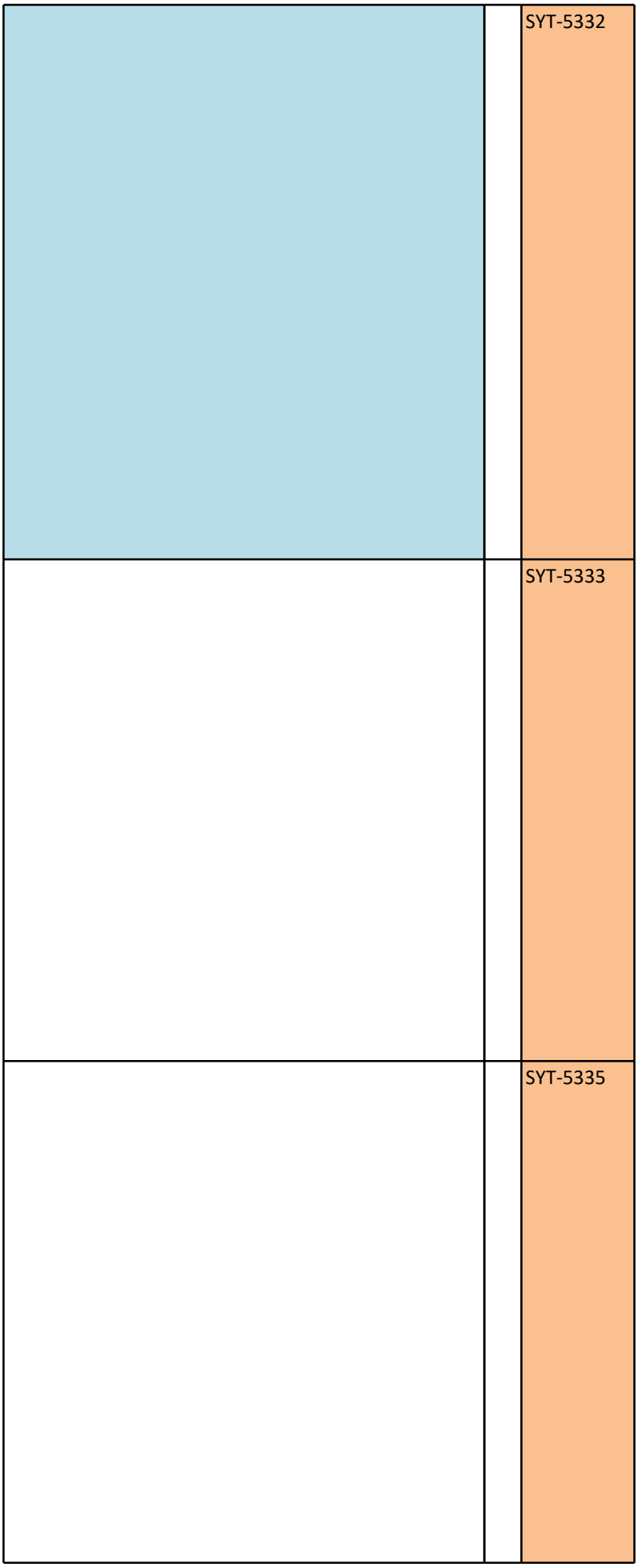

SYT-5287
SYT-5283

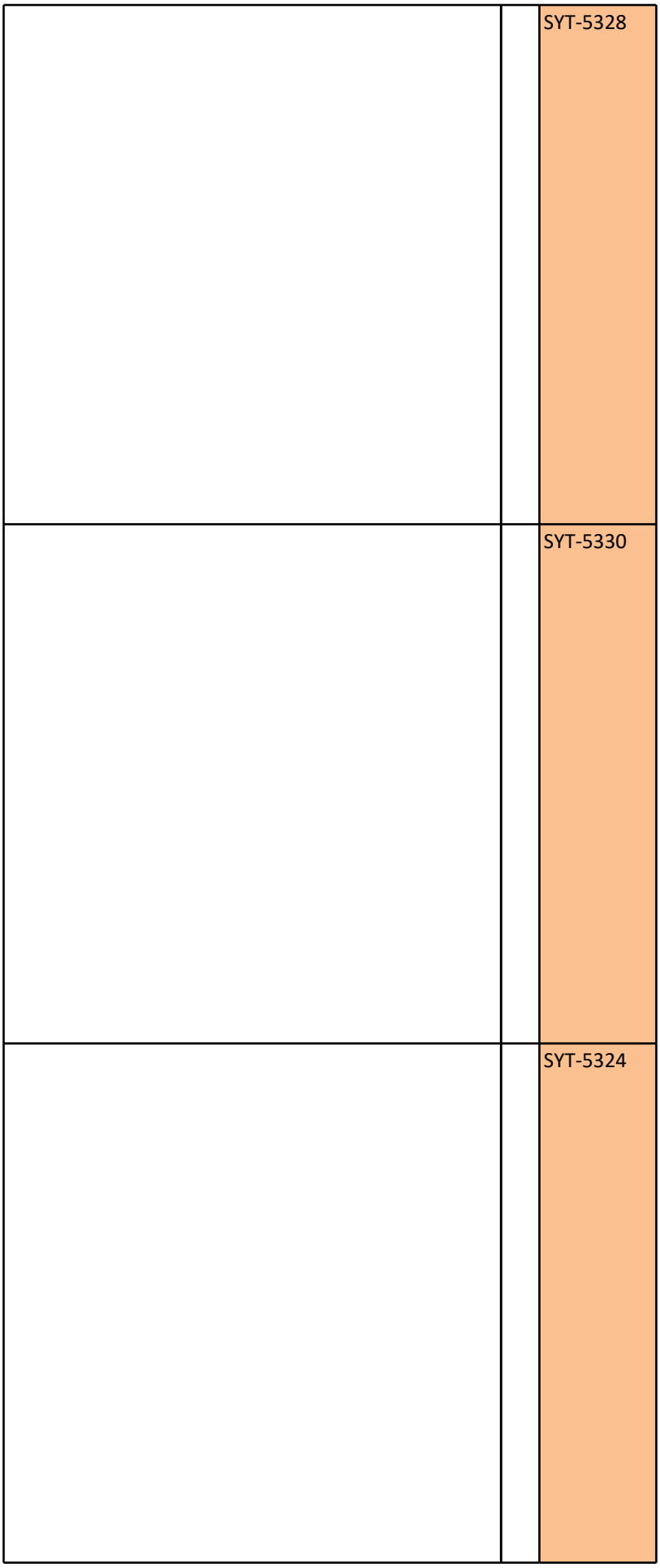

SYT-5285
SYT-5296
SYT-5294

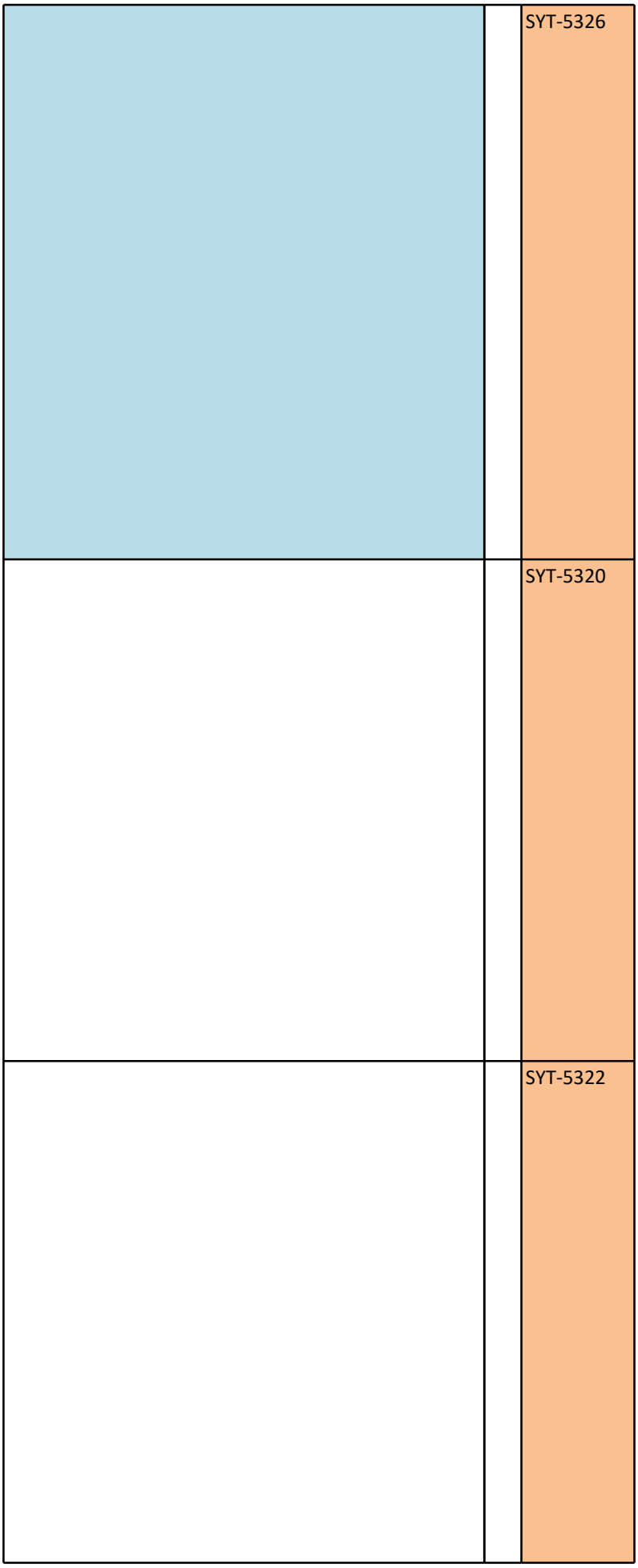

SYT-5304
SYT-5306


SYT-5302
SYT-5303
SYT-5300

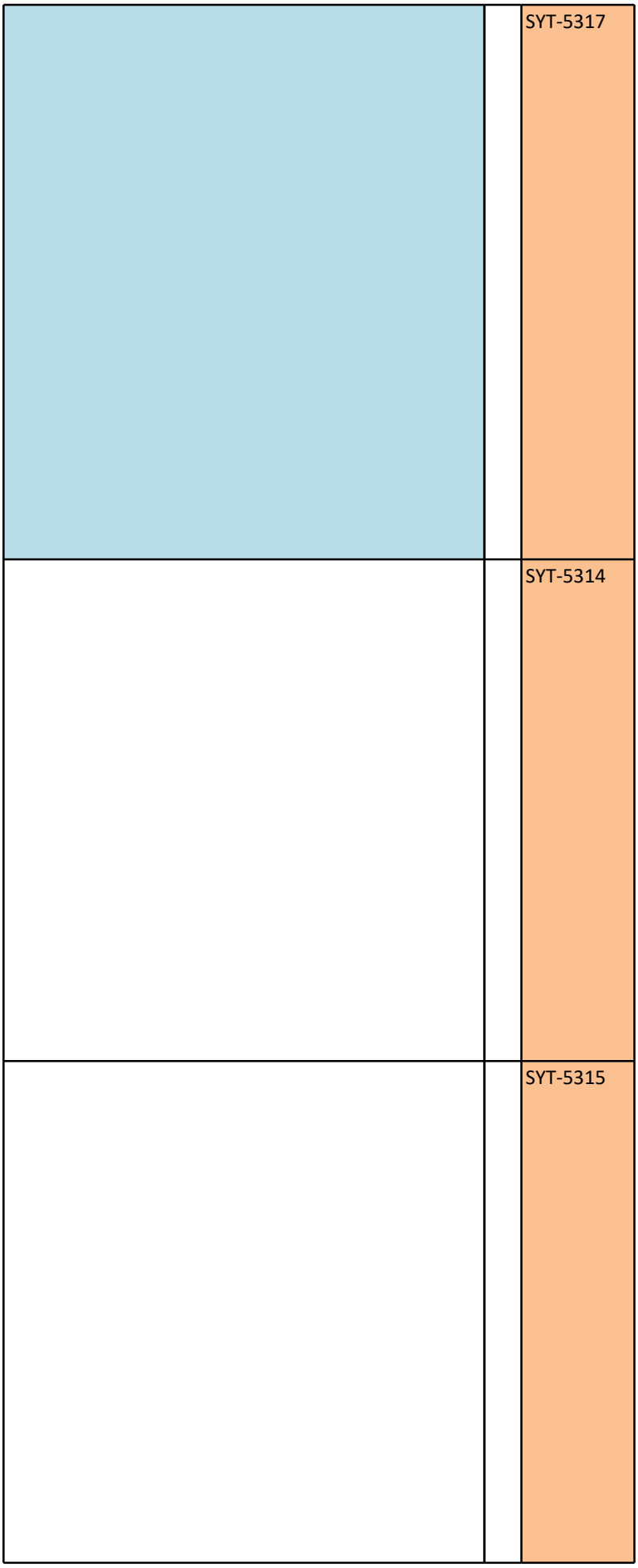
		SYT-5301
		SYT-5298
		SYT-5299

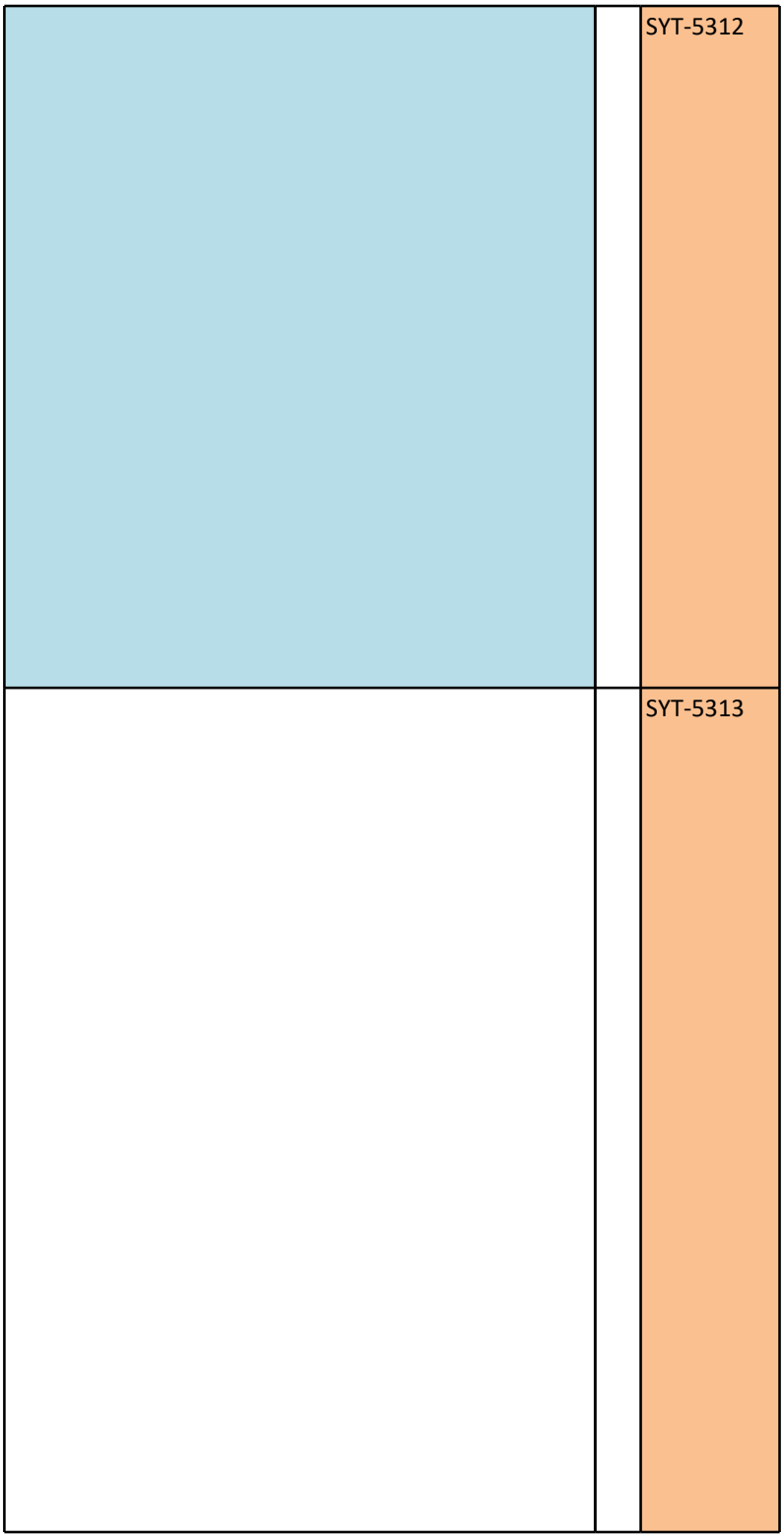

SYT-5332
SYT-5333
SYT-5335

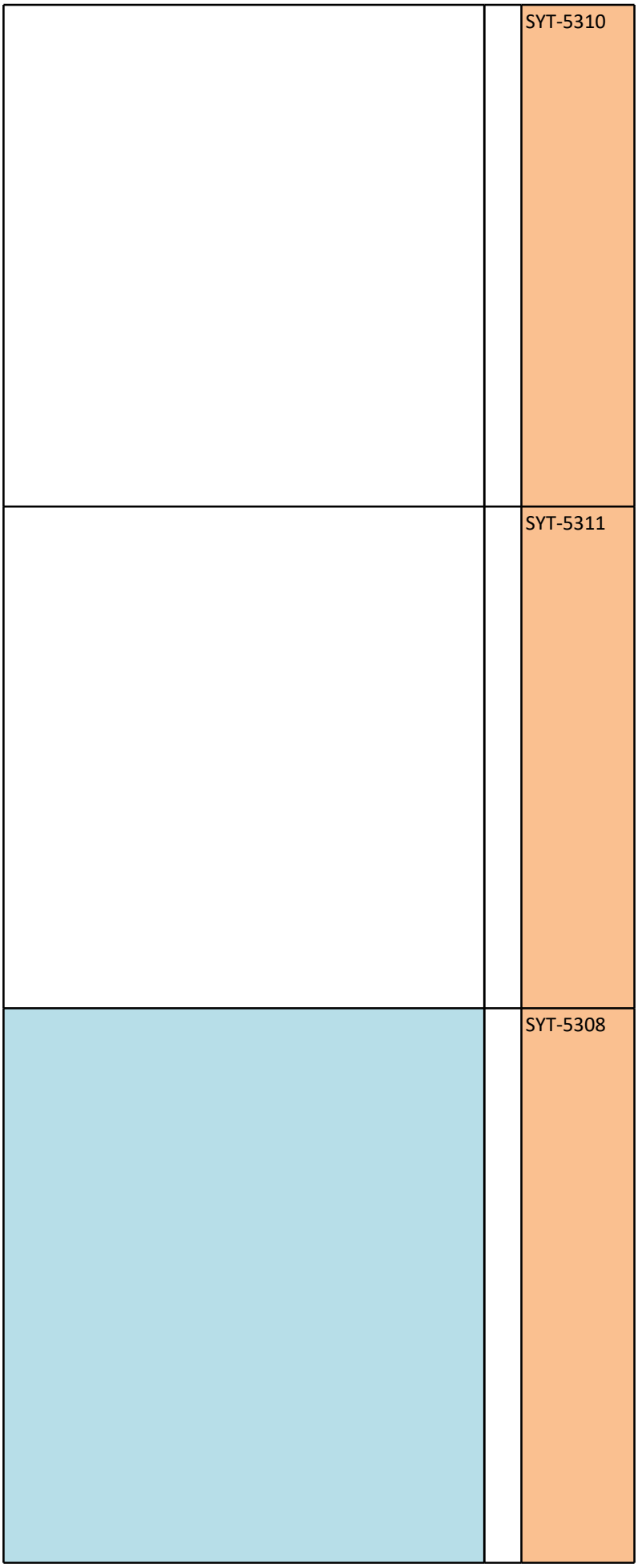

SYT-5328
SYT-5330
SYT-5324


SYT-5326
SYT-5320
SYT-5322

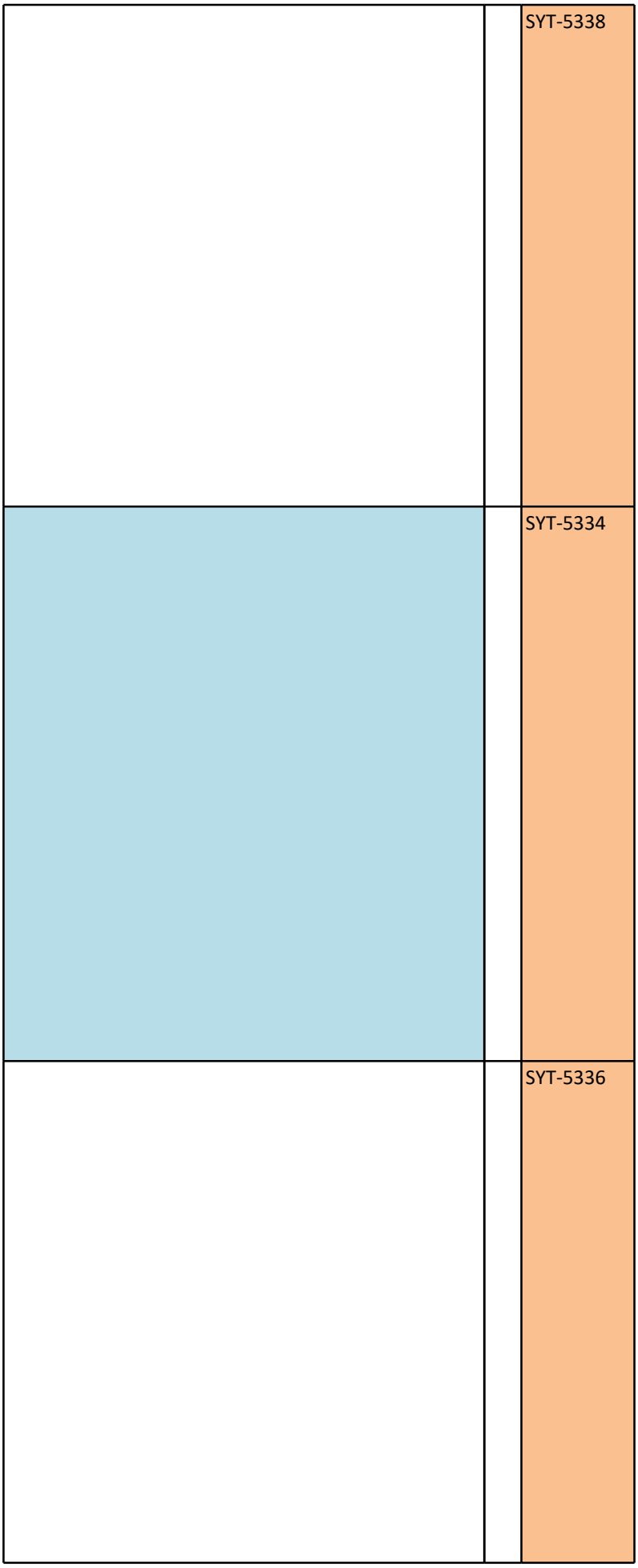

SYT-5305
SYT-5307


SYT-5317
SYT-5314
SYT-5315

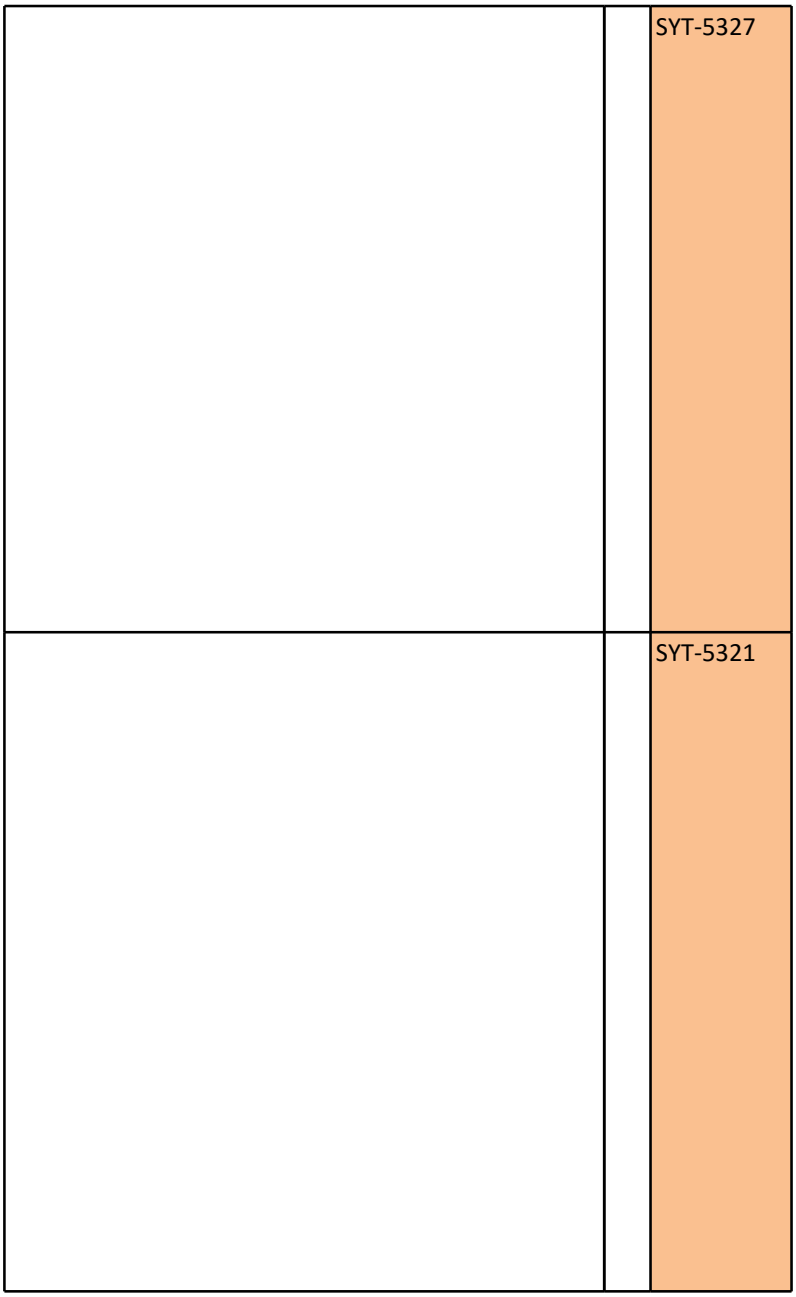

SYT-5312
SYT-5313

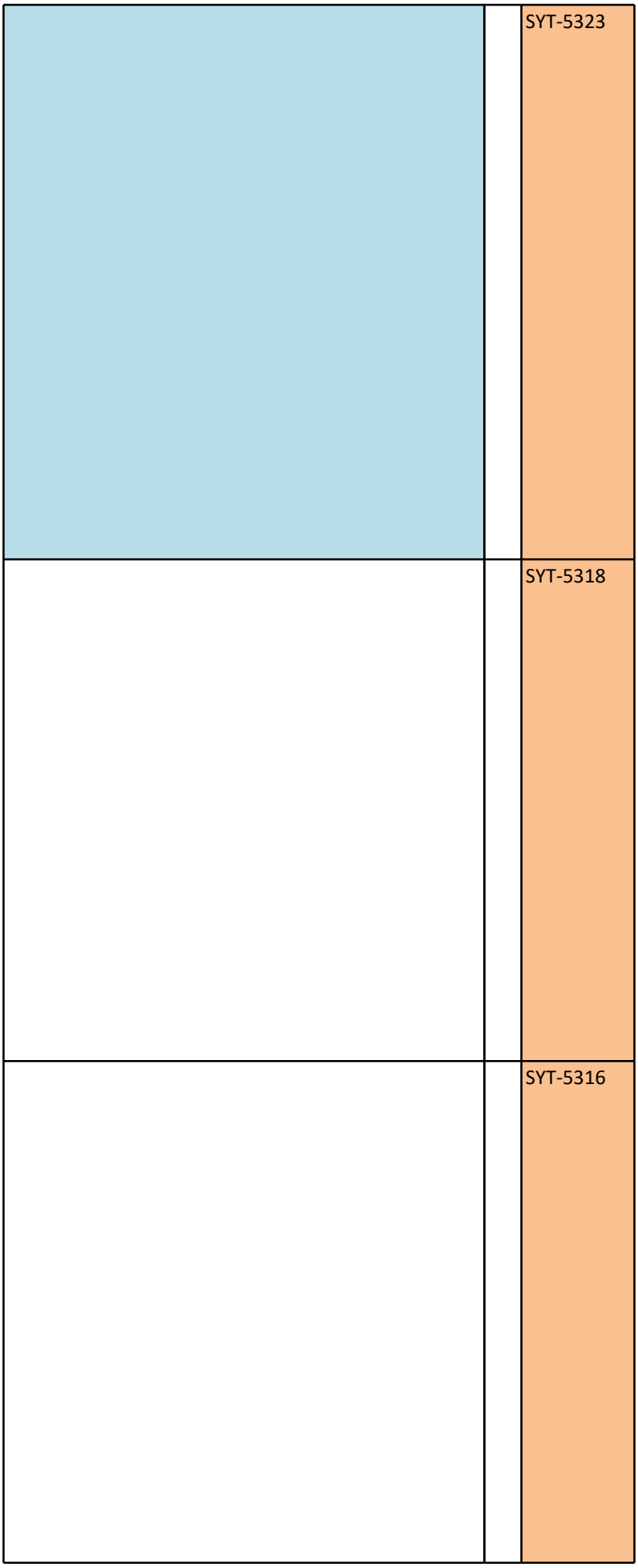

SYT-5310
SYT-5311
SYT-5308

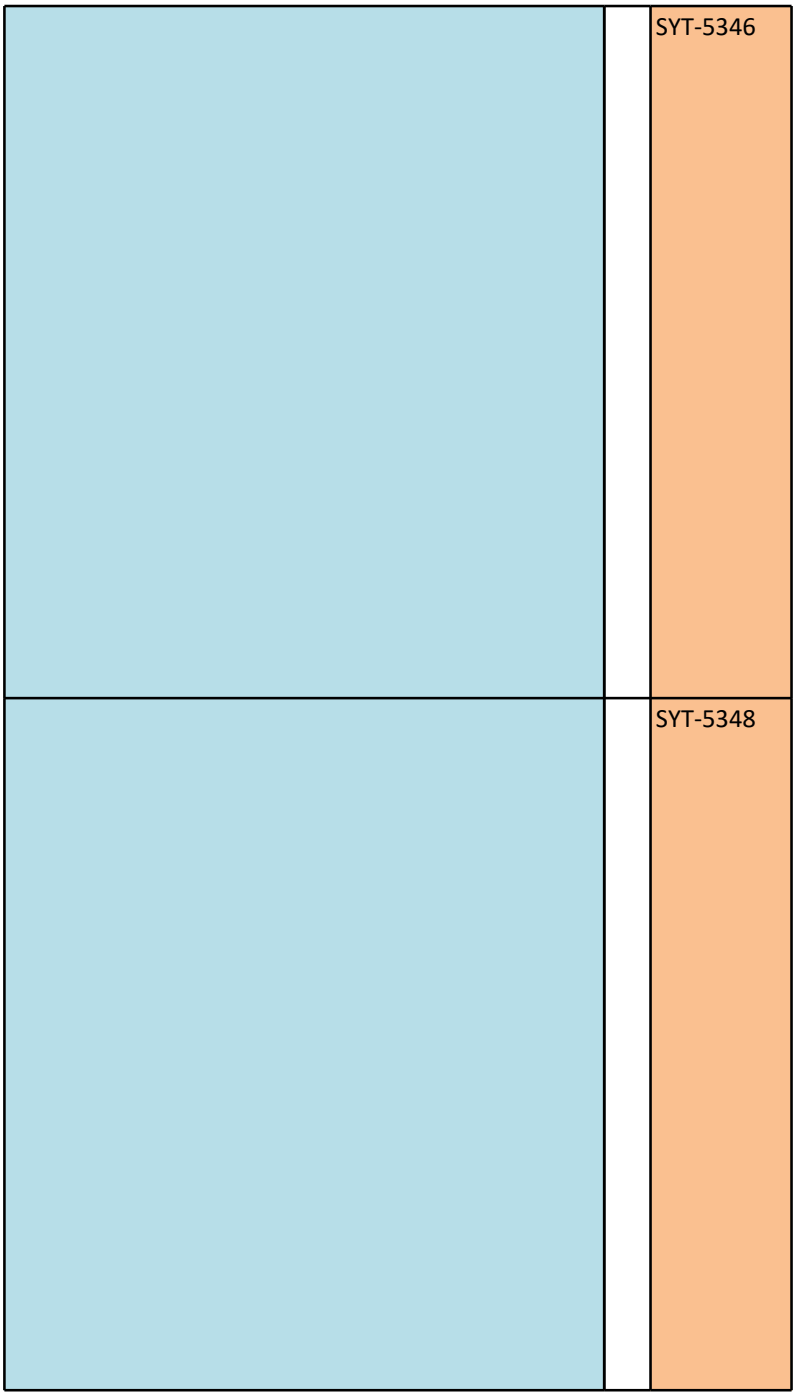
		SYT-5309
		SYT-5319
		SYT-5337

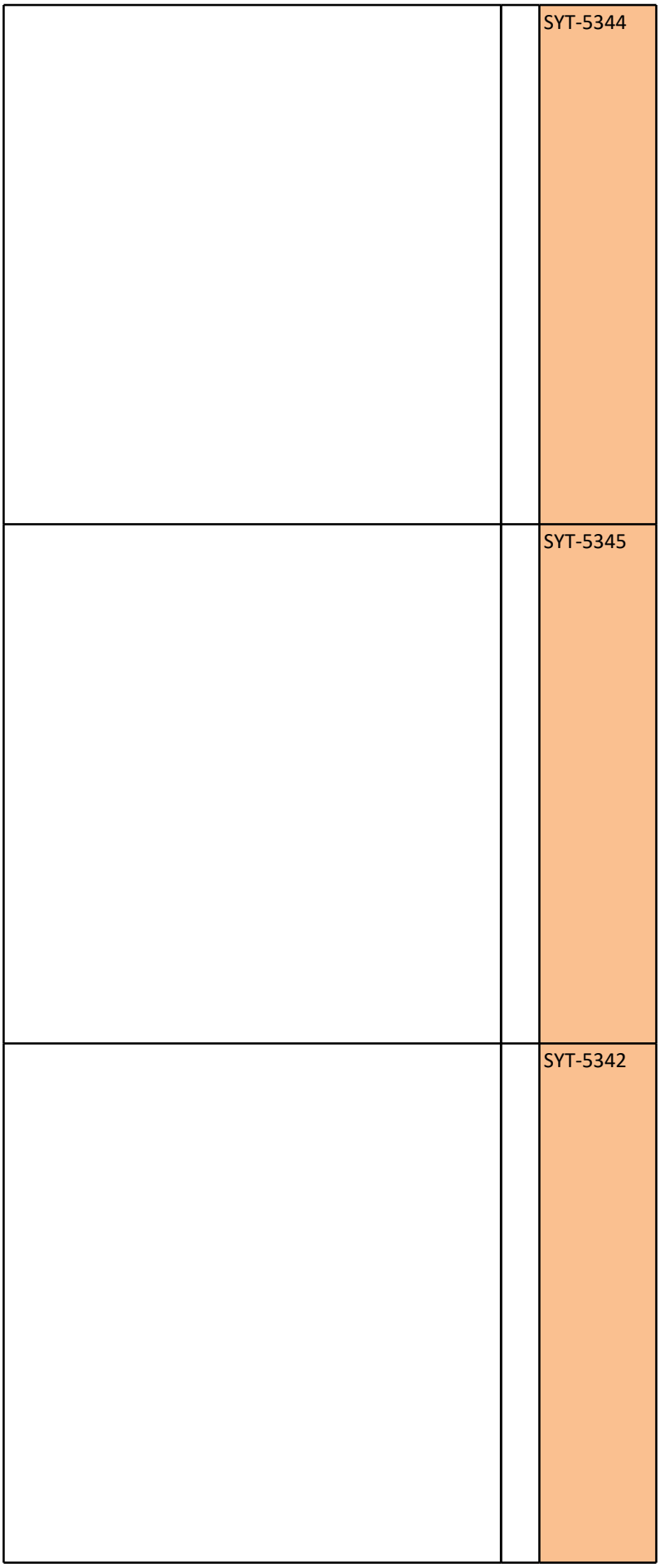

SYT-5338
SYT-5334
SYT-5336

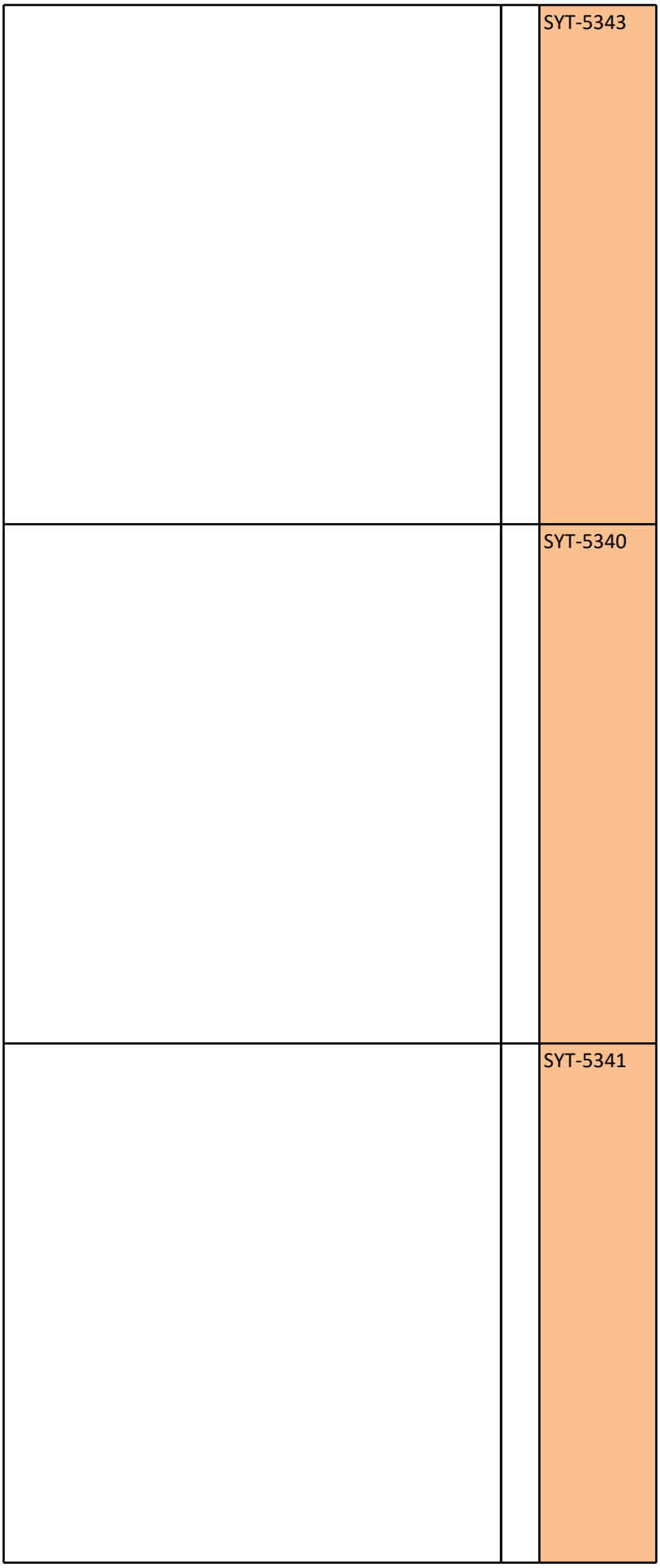
		SYT-5329
		SYT-5331
		SYT-5325

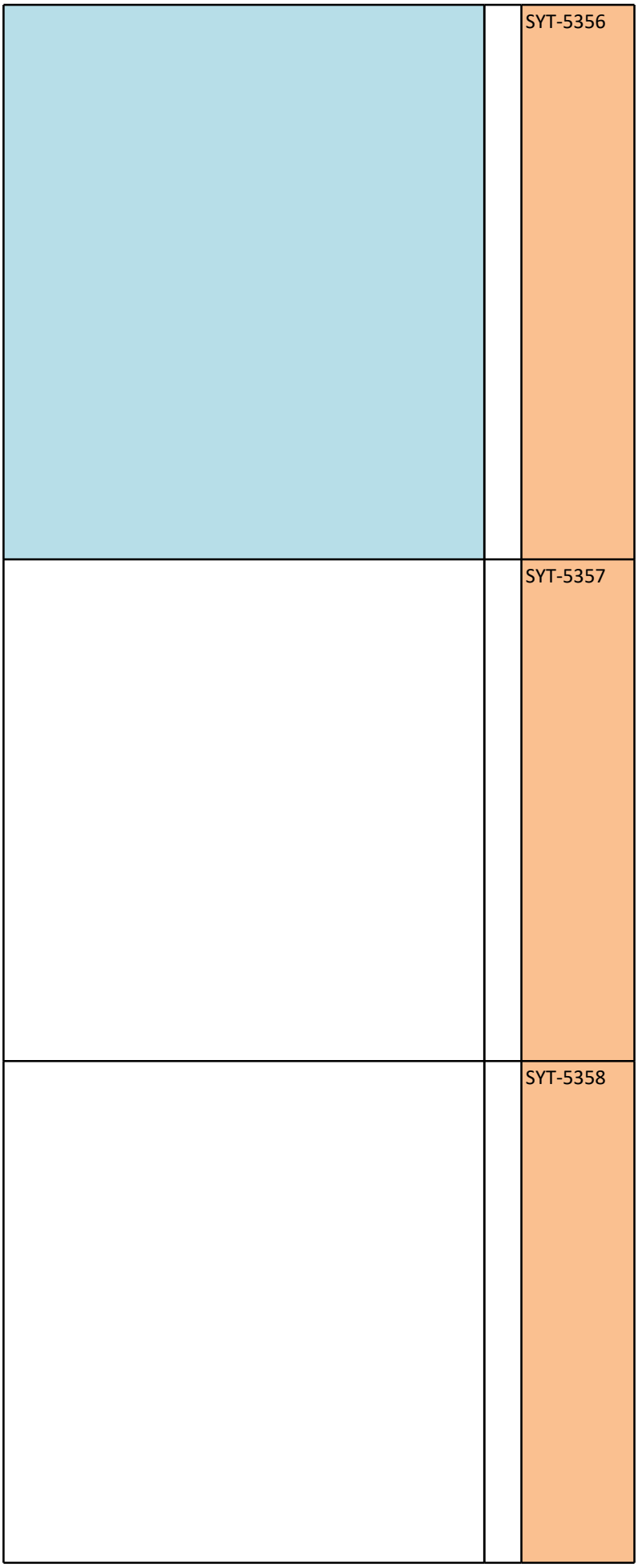

SYT-5327
SYT-5321

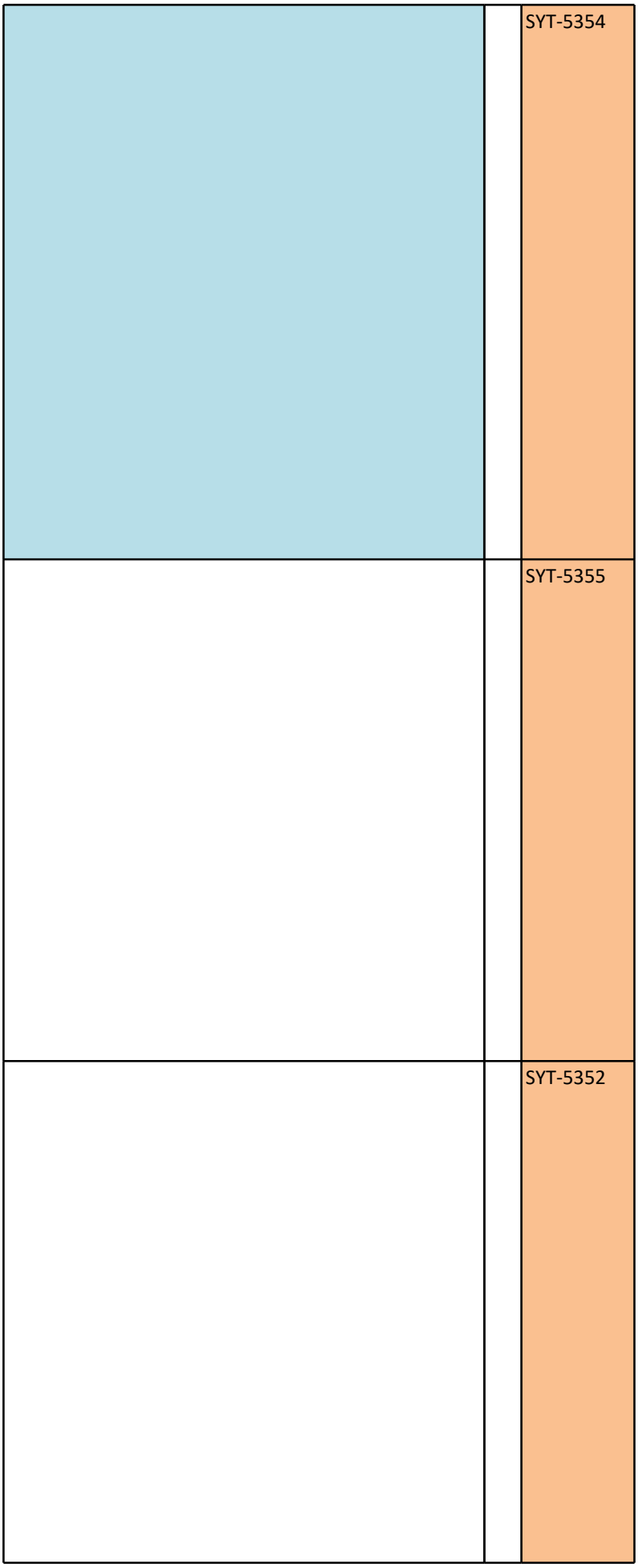

SYT-5323
SYT-5318
SYT-5316

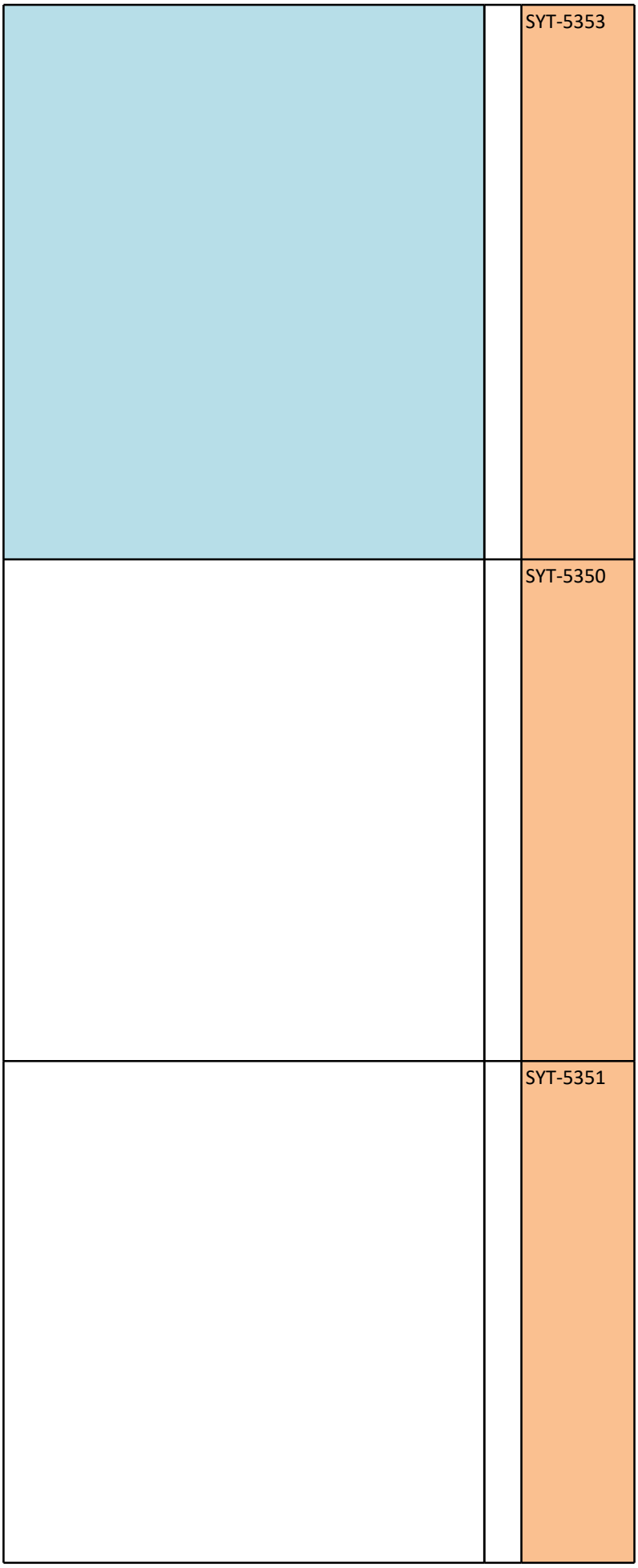

SYT-5346
SYT-5348

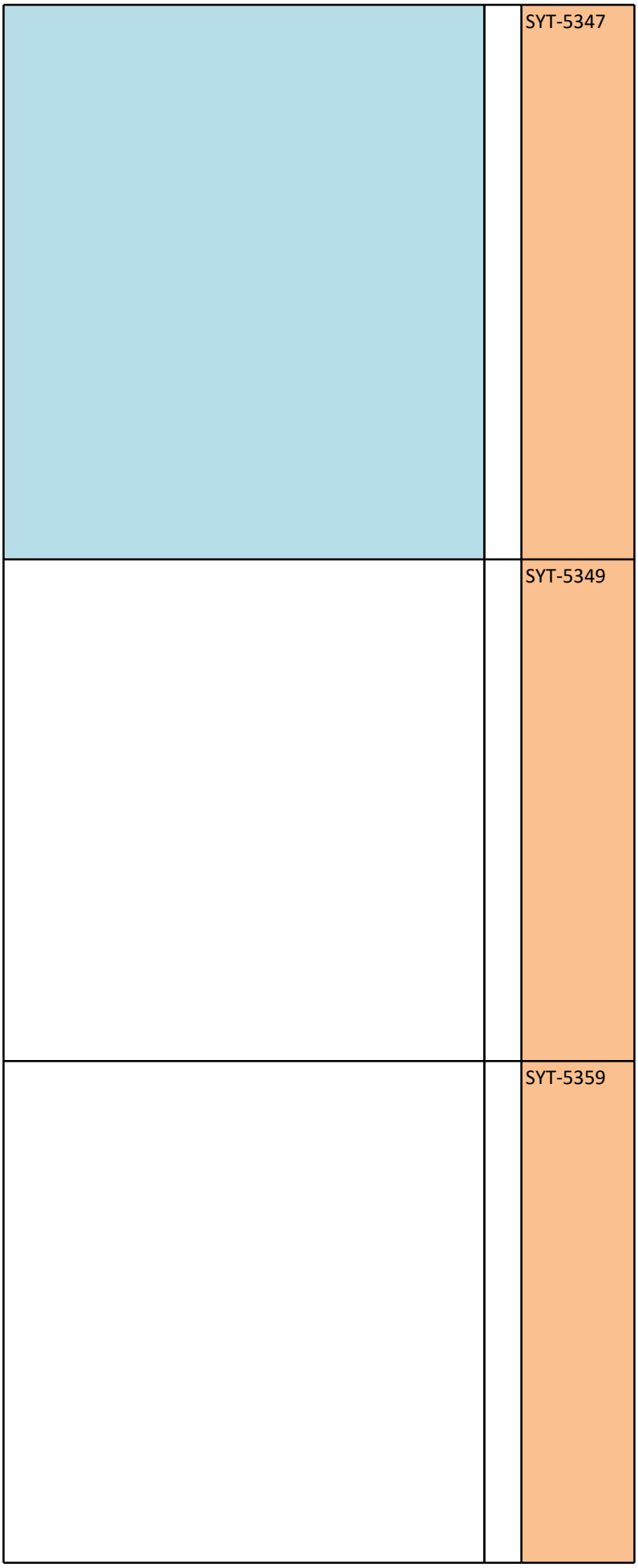

SYT-5344
SYT-5345
SYT-5342

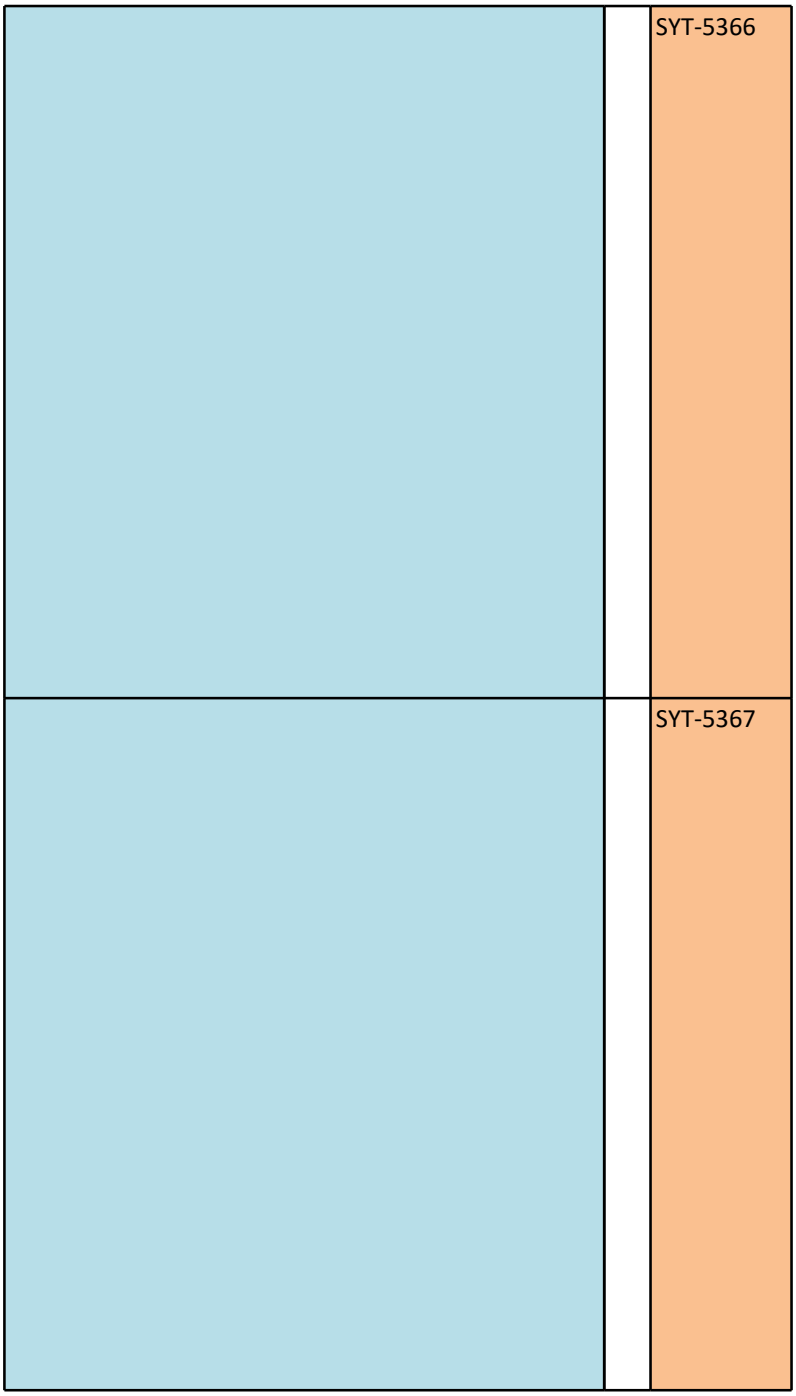

SYT-5343
SYT-5340
SYT-5341

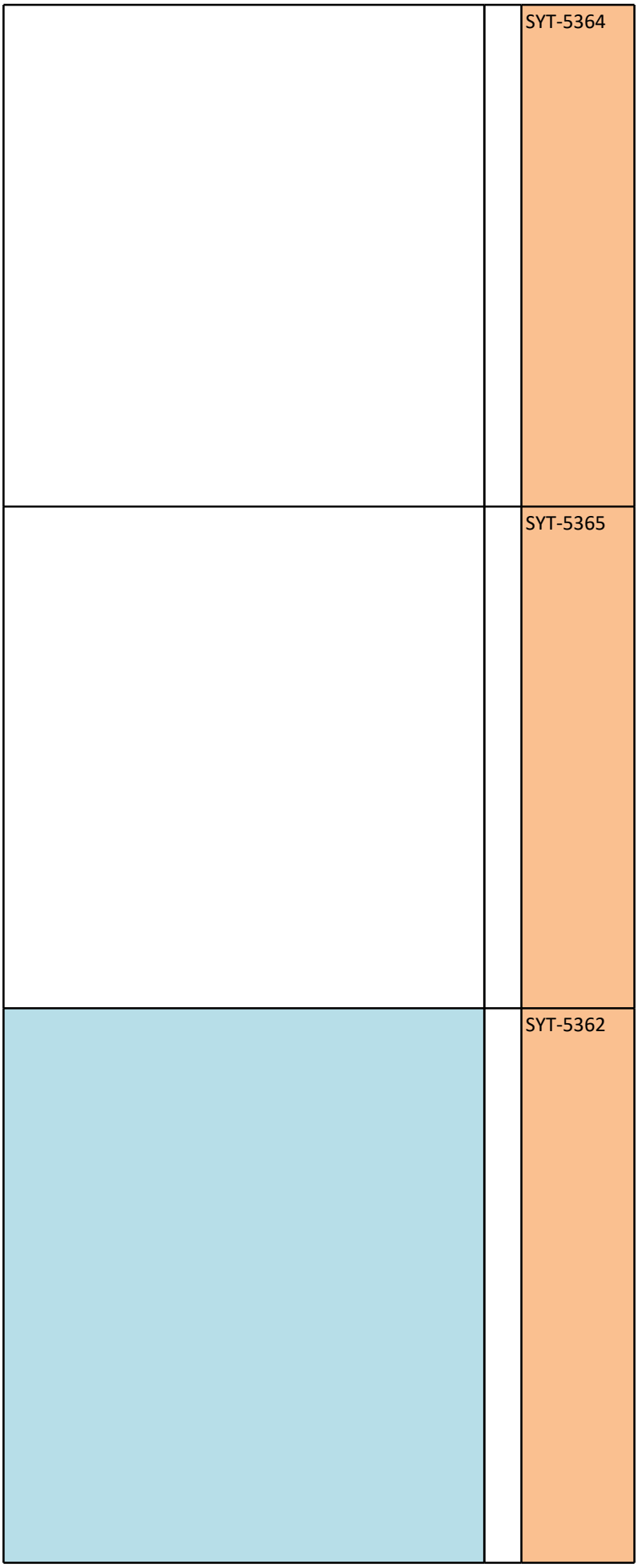

SYT-5356
SYT-5357
SYT-5358


SYT-5354
SYT-5355
SYT-5352

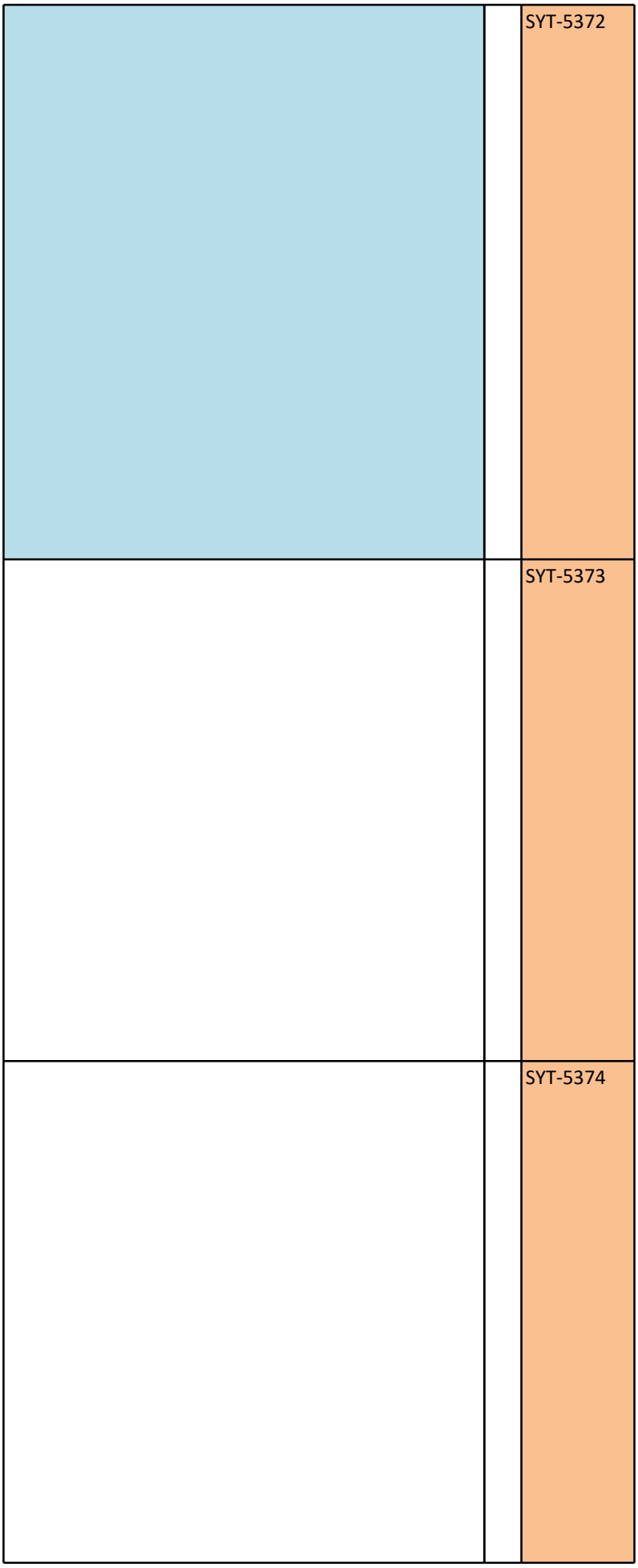

SYT-5353
SYT-5350
SYT-5351

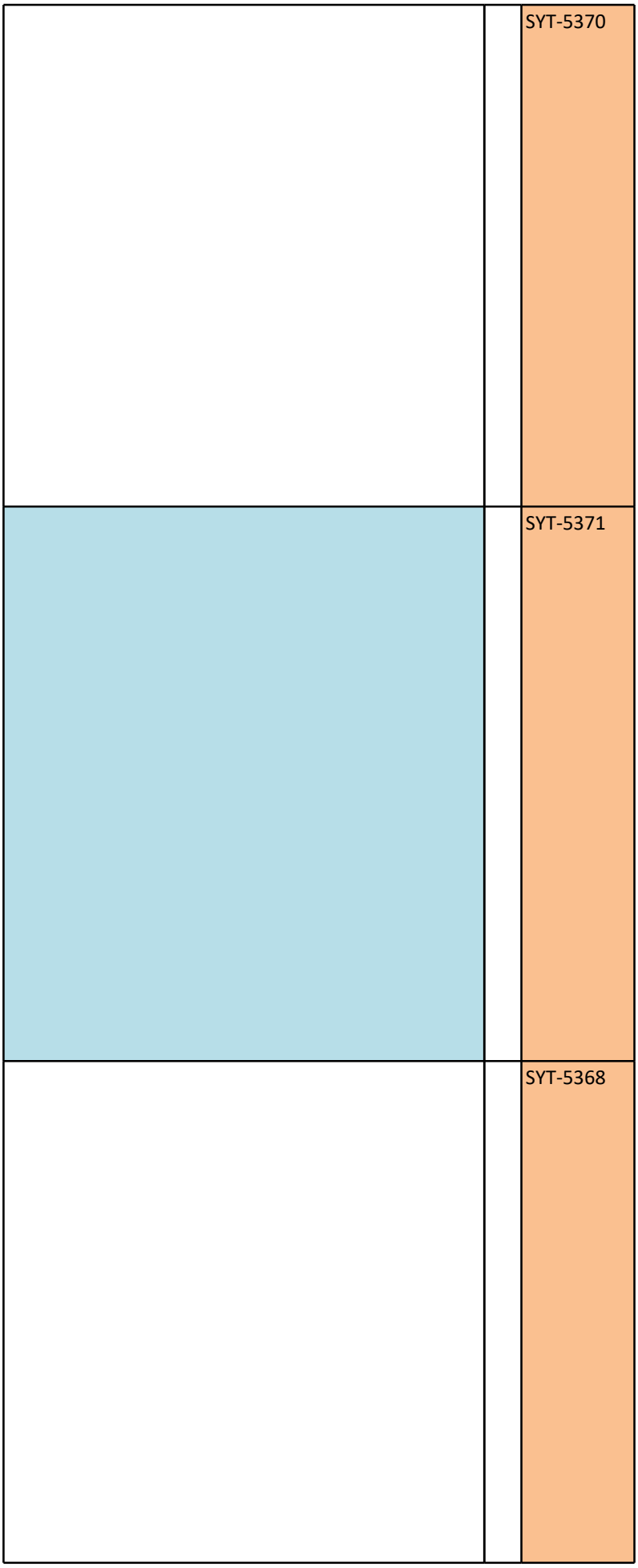

SYT-5347
SYT-5349
SYT-5359

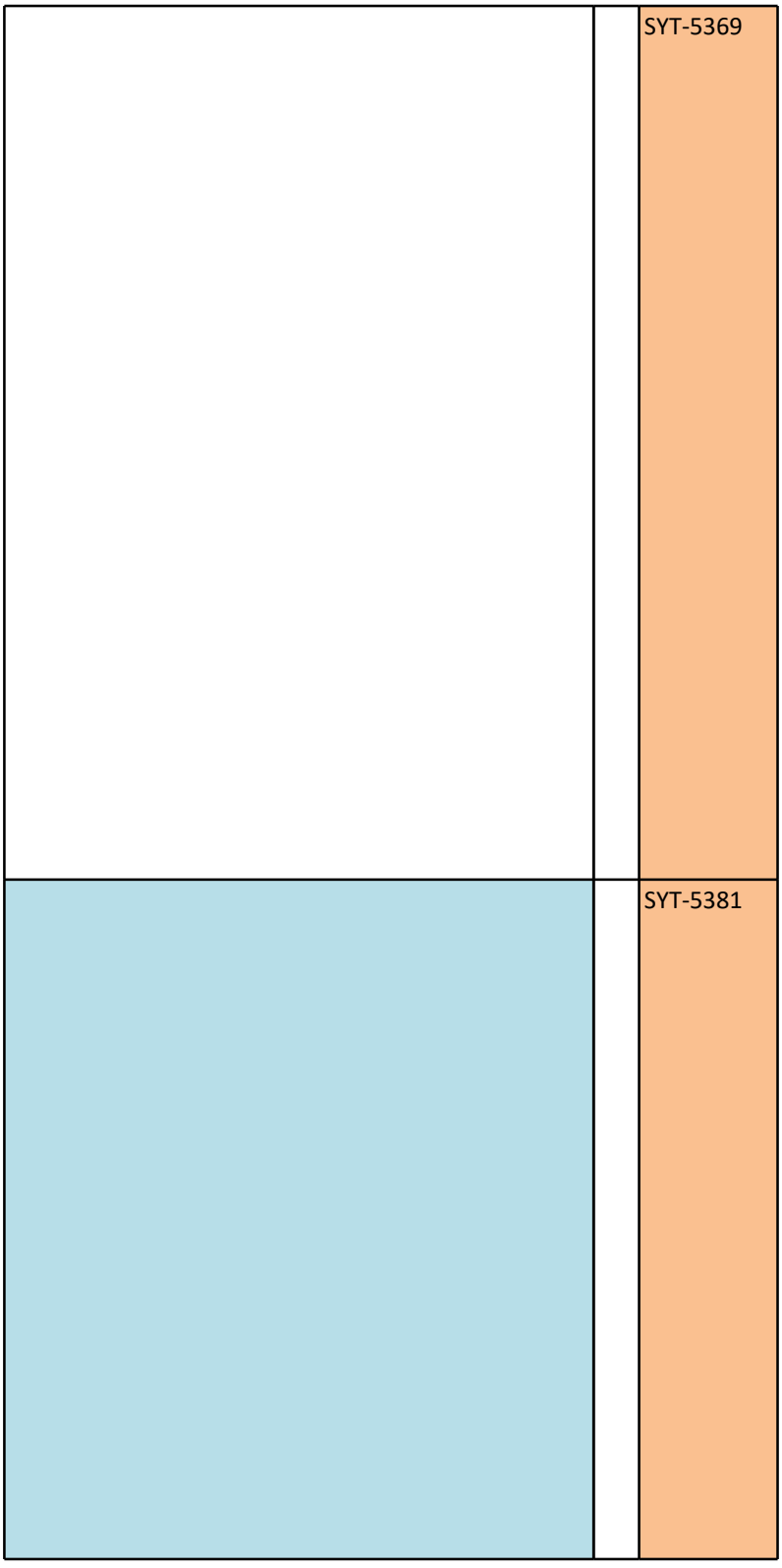

SYT-5366
SYT-5367

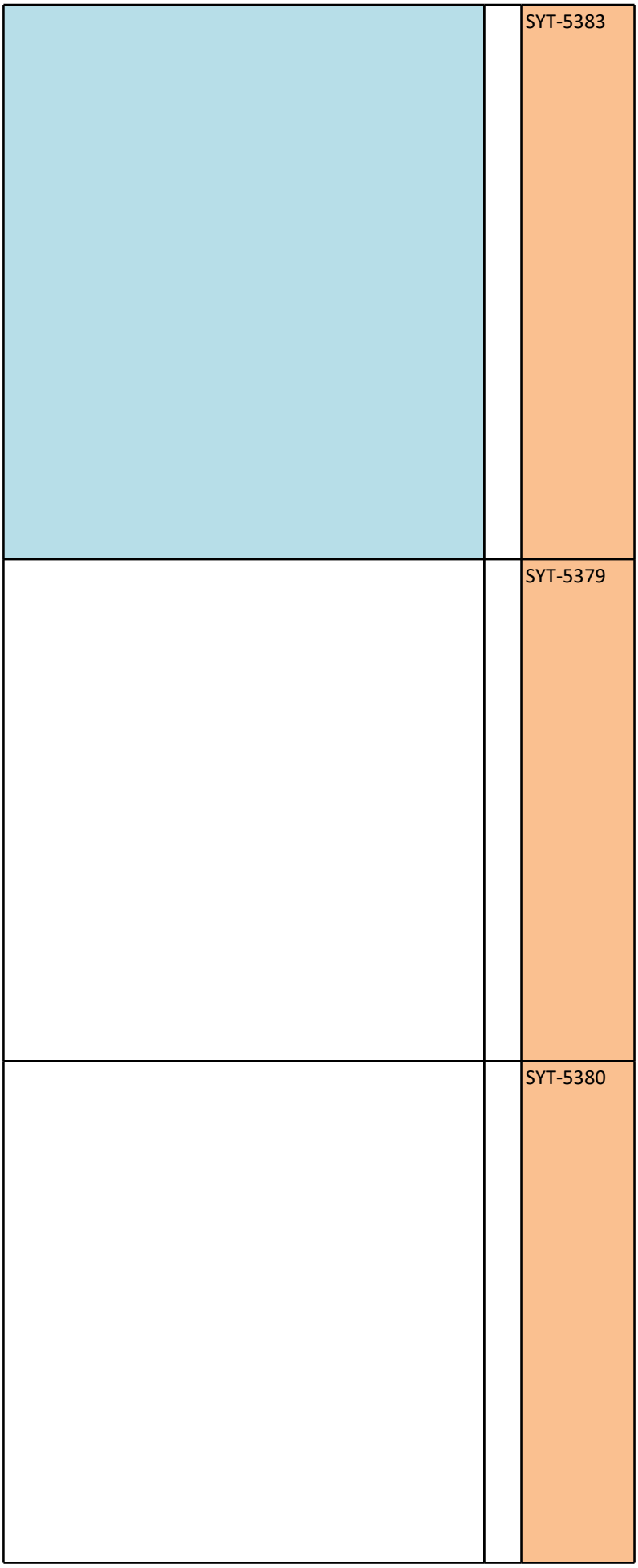

SYT-5364
SYT-5365
SYT-5362

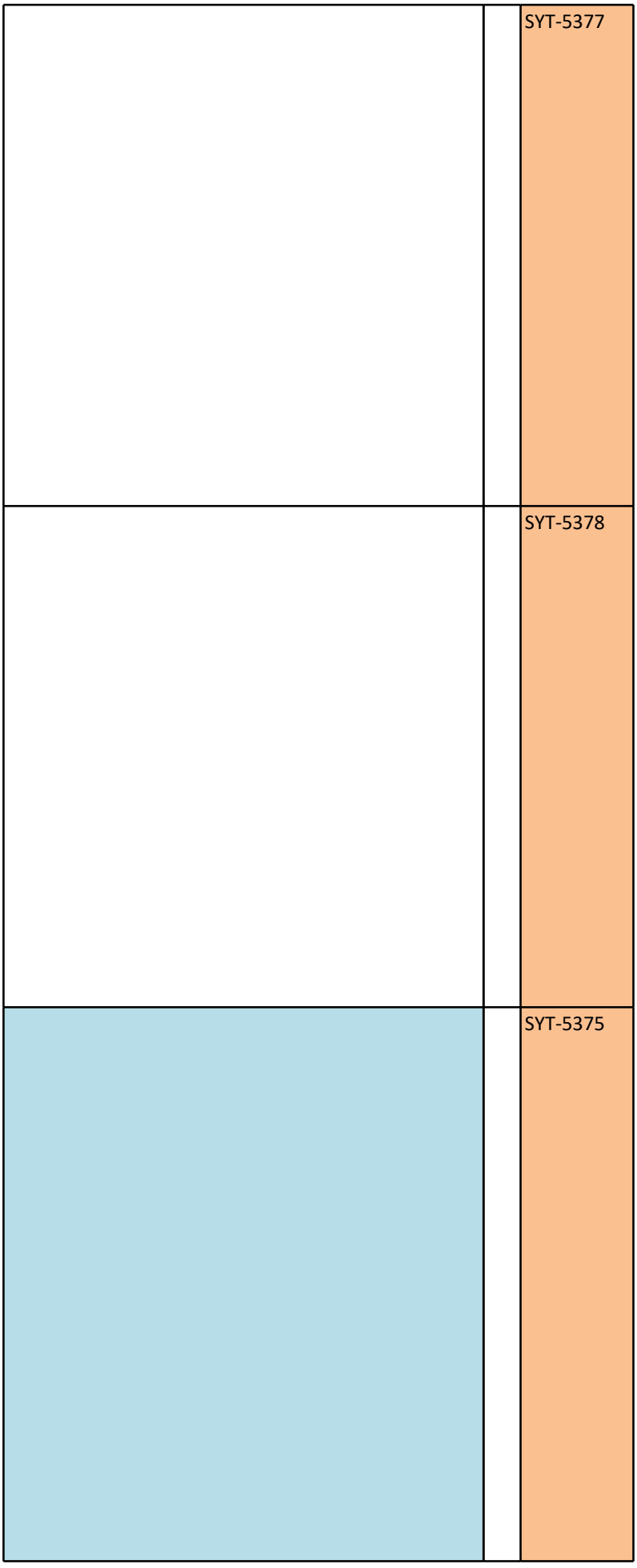
		SYT-5363
		SYT-5360
		SYT-5361

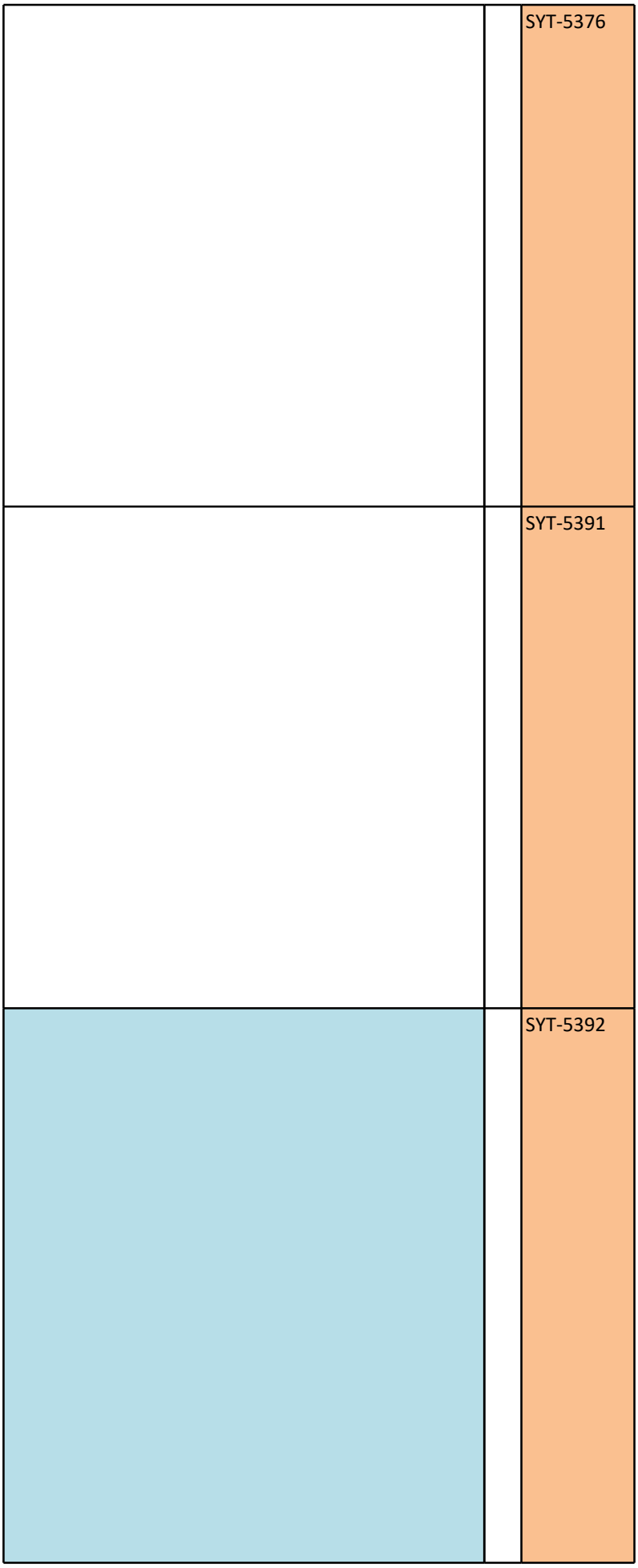

SYT-5372
SYT-5373
SYT-5374

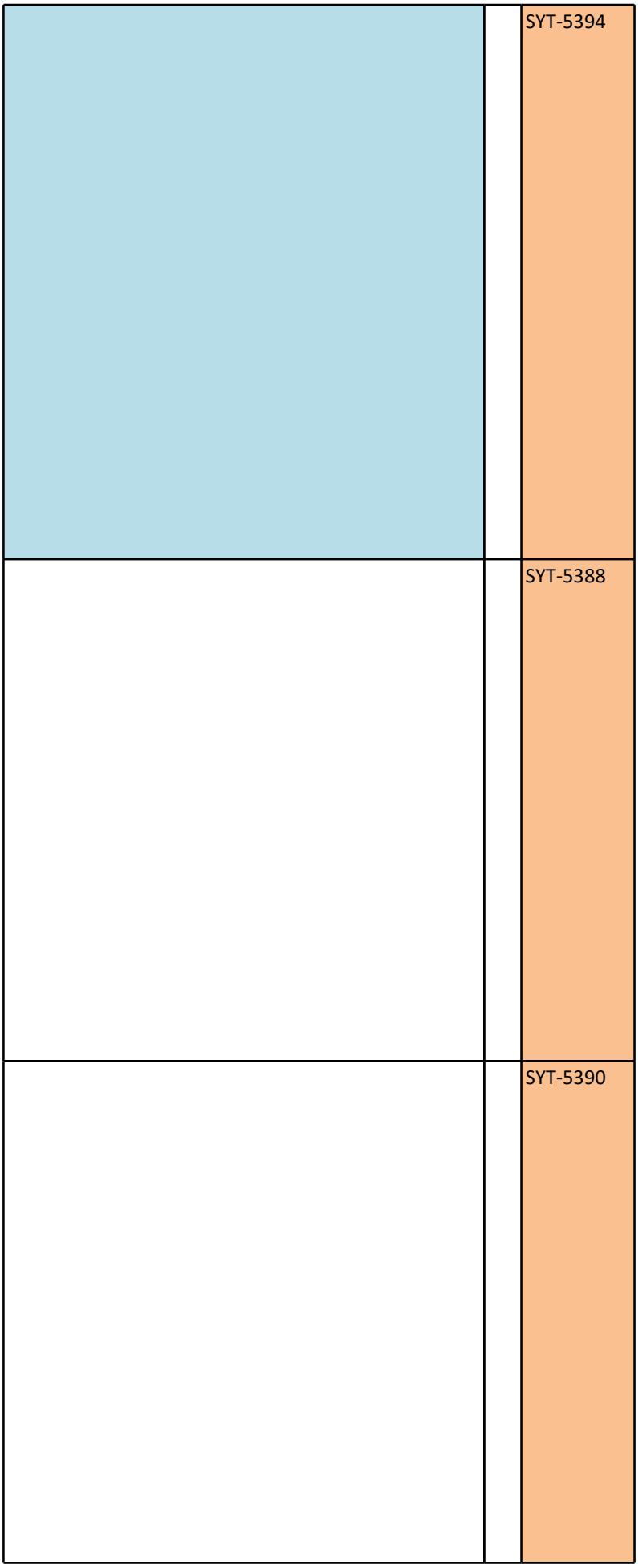

SYT-5370
SYT-5371
SYT-5368

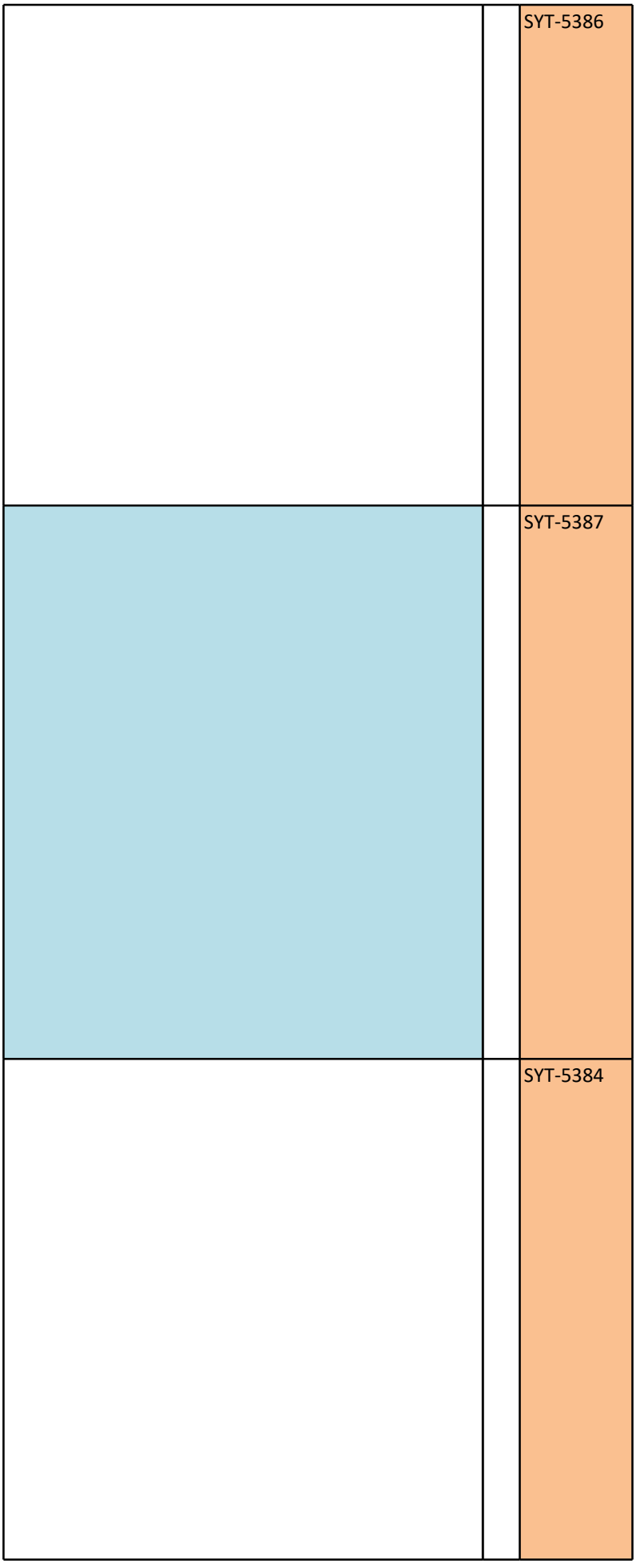

SYT-5369
SYT-5381

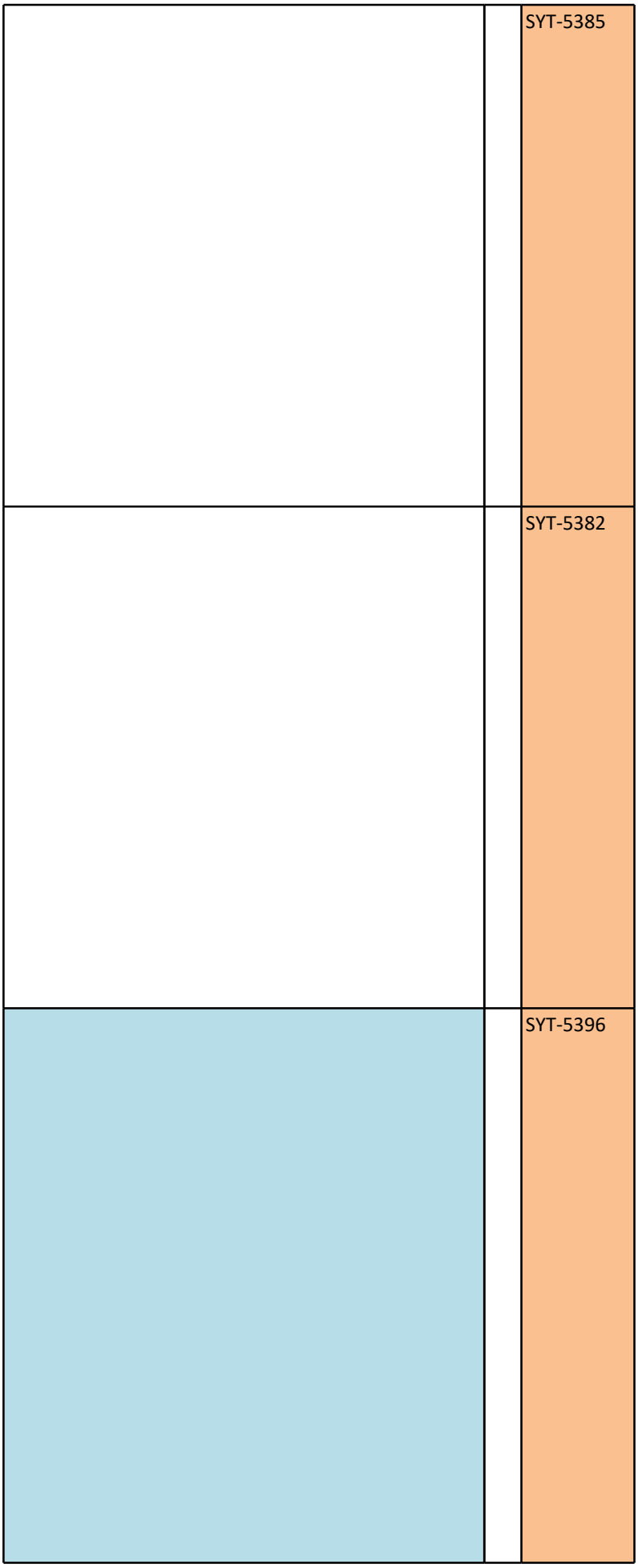

SYT-5383
SYT-5379
SYT-5380


SYT-5377
SYT-5378
SYT-5375

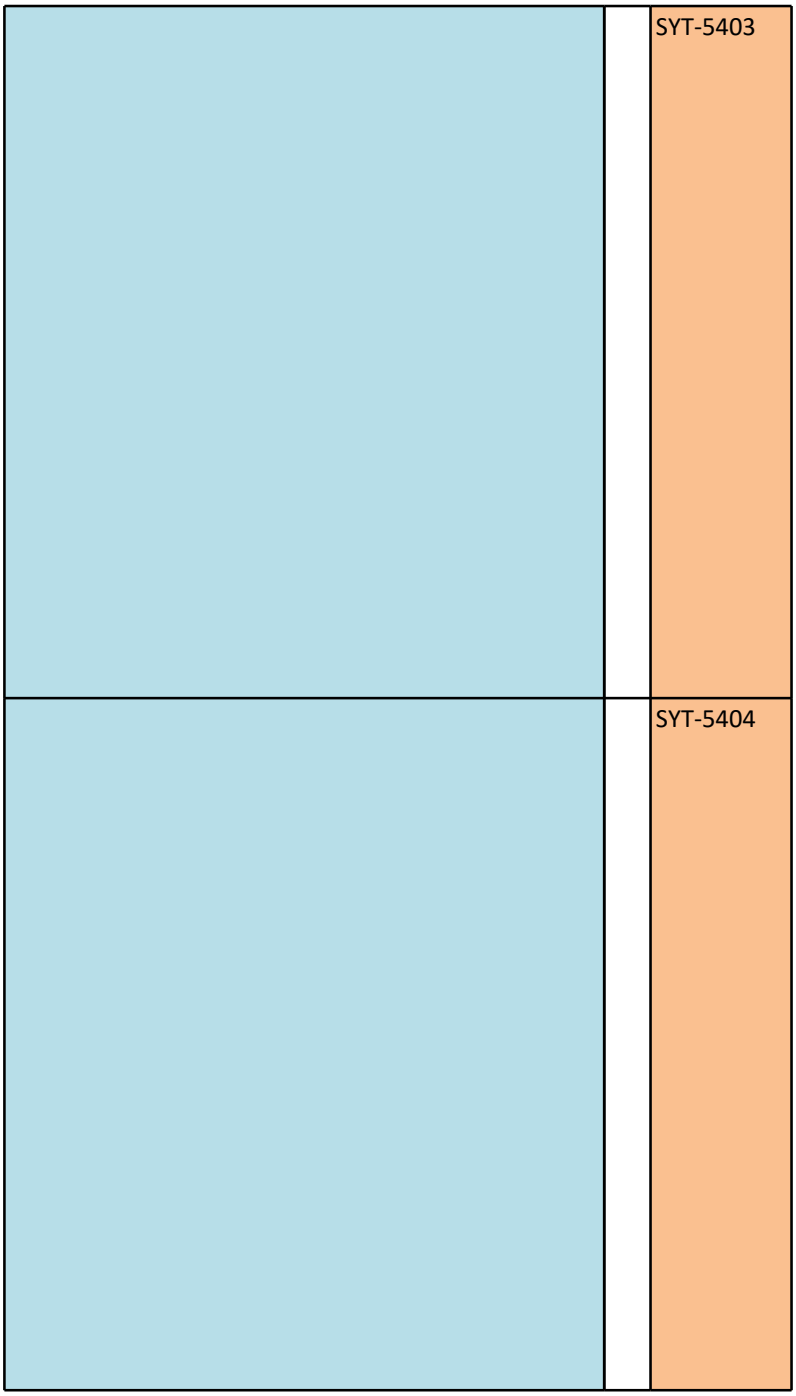

SYT-5376
SYT-5391
SYT-5392

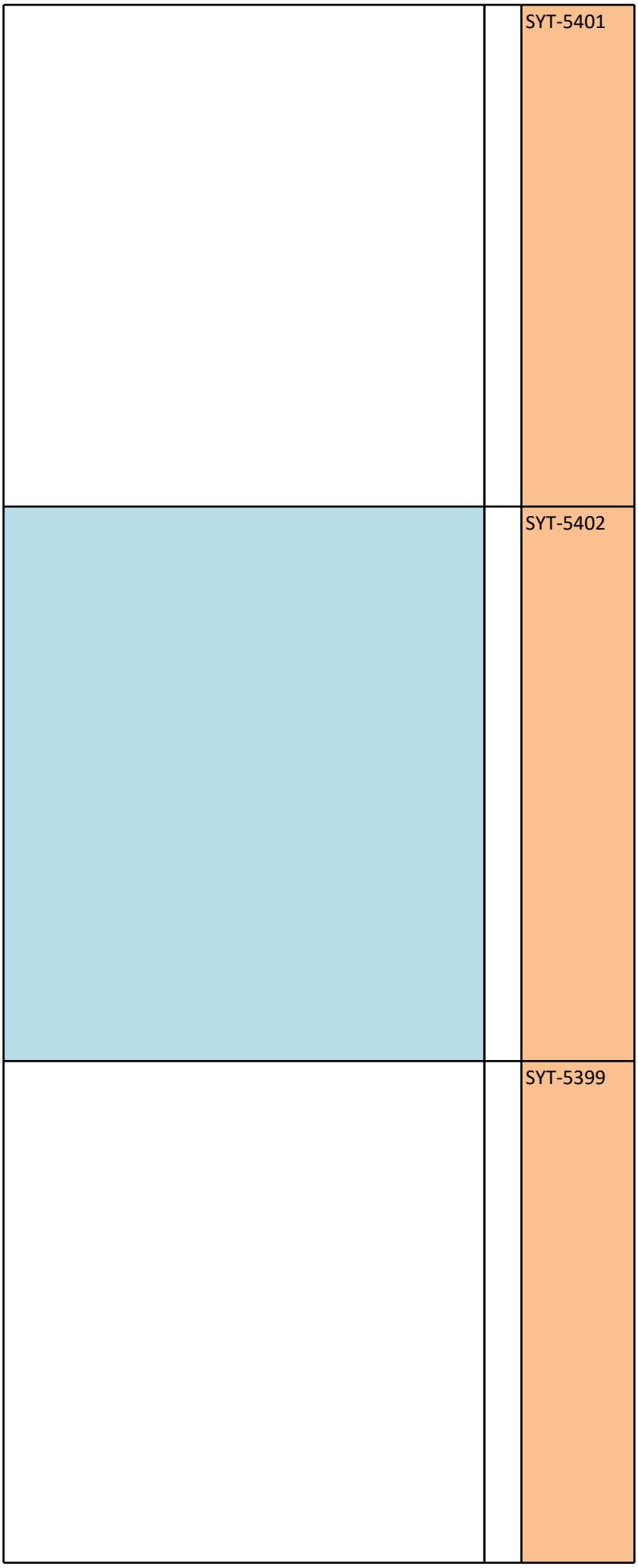

SYT-5394
SYT-5388
SYT-5390


SYT-5386
SYT-5387
SYT-5384

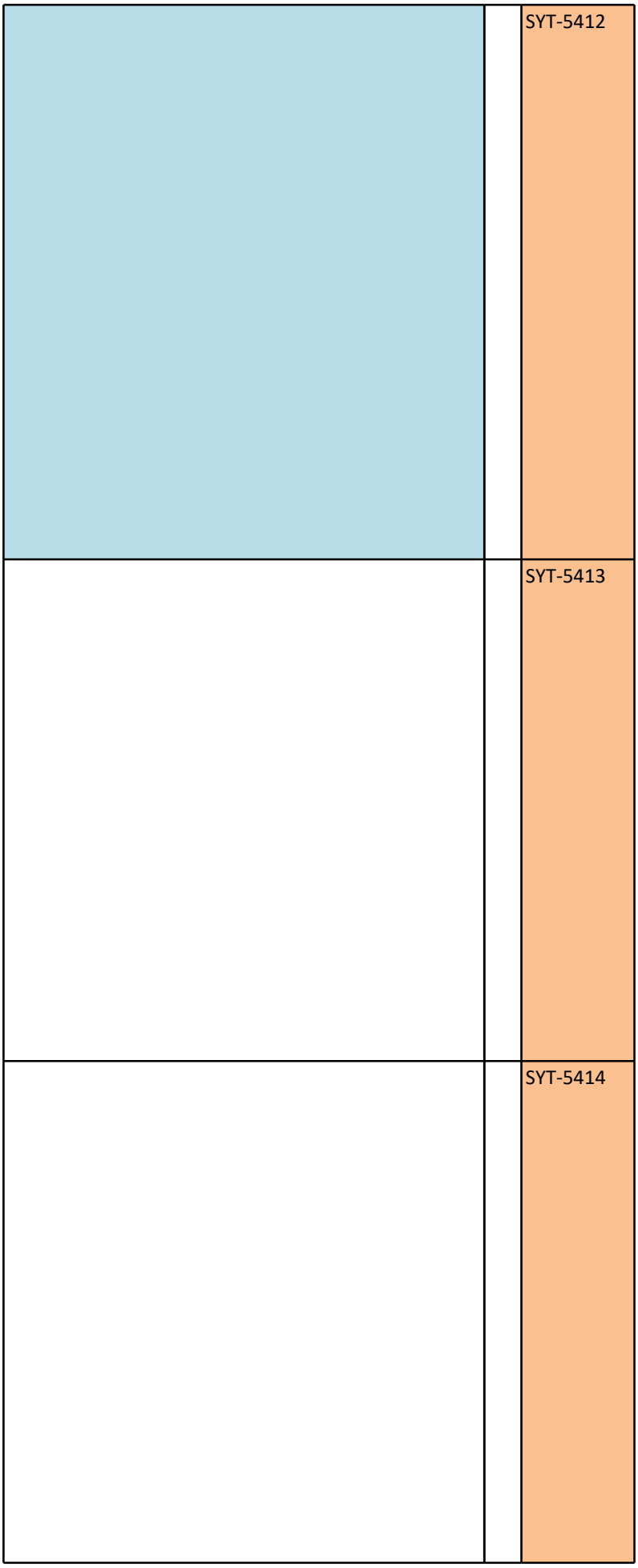

SYT-5385
SYT-5382
SYT-5396

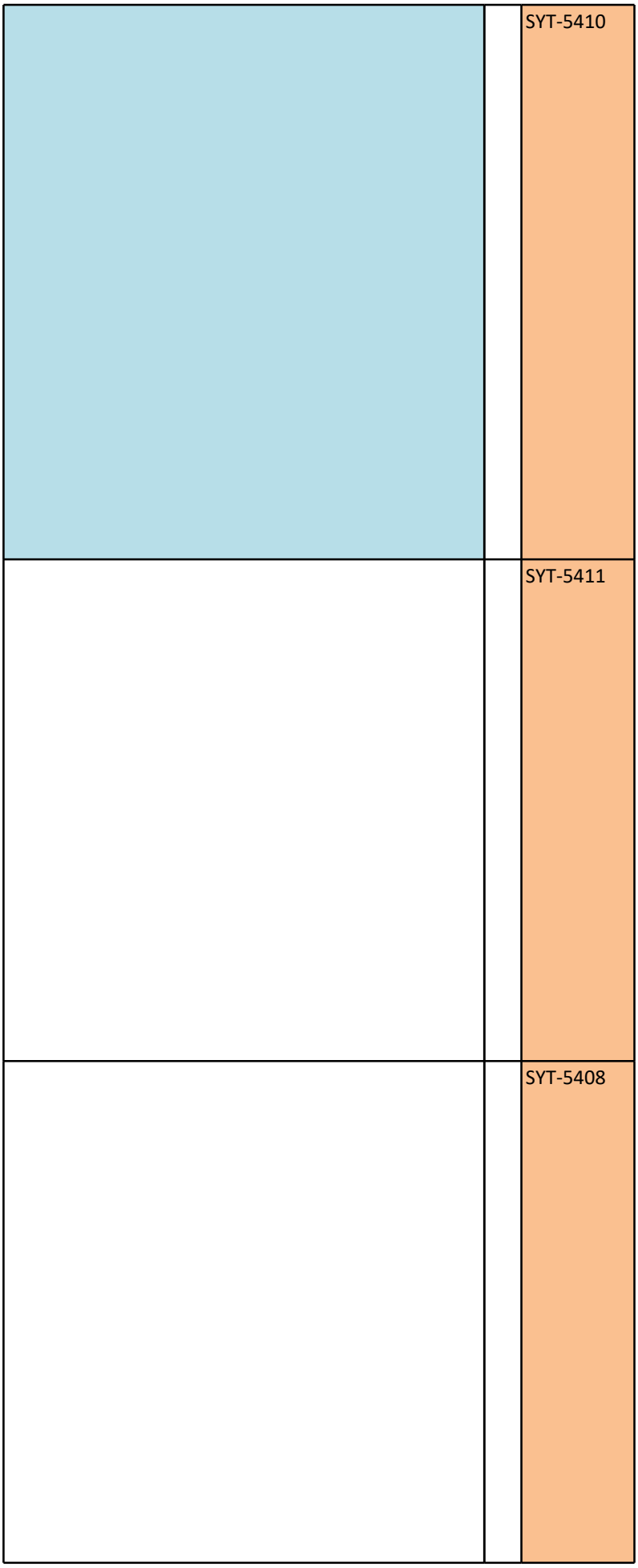
		SYT-5393
		SYT-5395
		SYT-5389

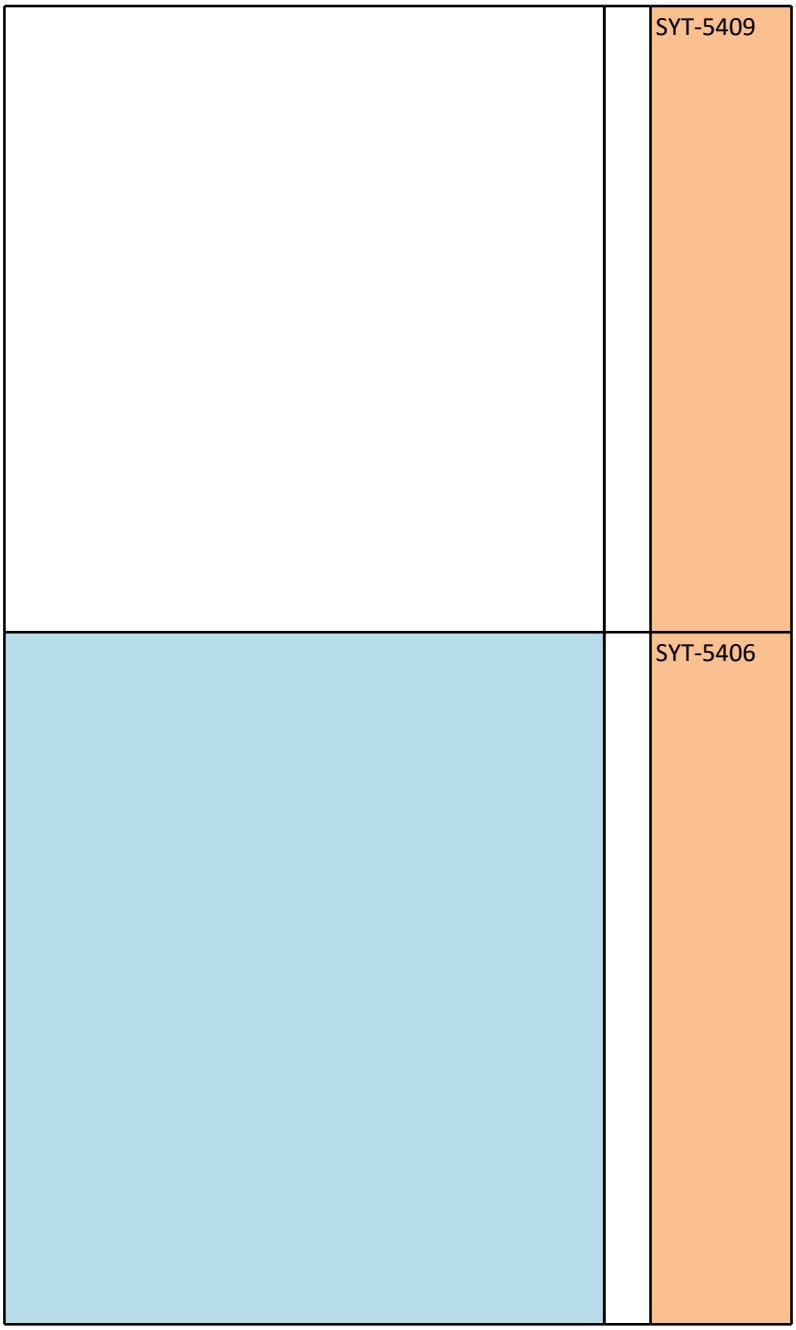

SYT-5403
SYT-5404

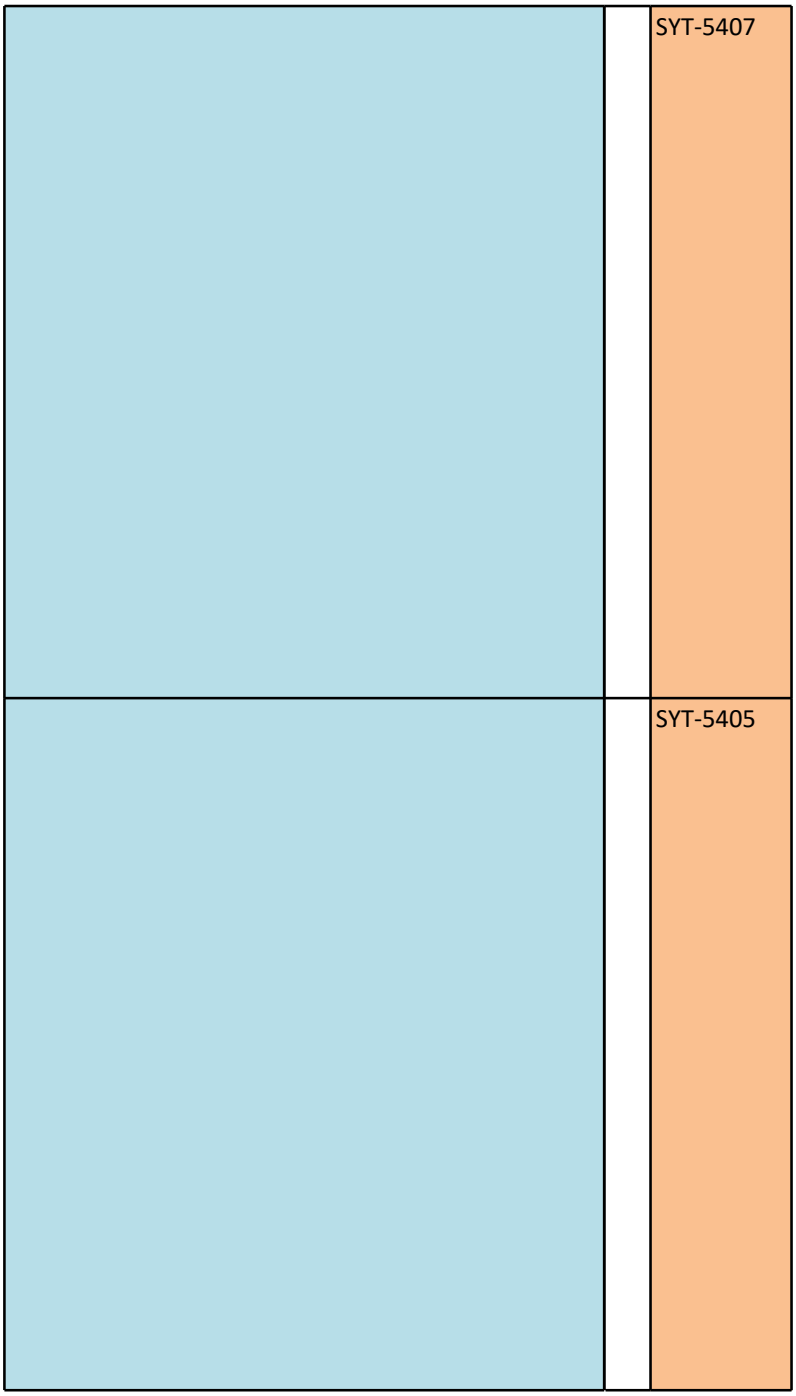

SYT-5401
SYT-5402
SYT-5399

		SYT-5400
		SYT-5397
		SYT-5398

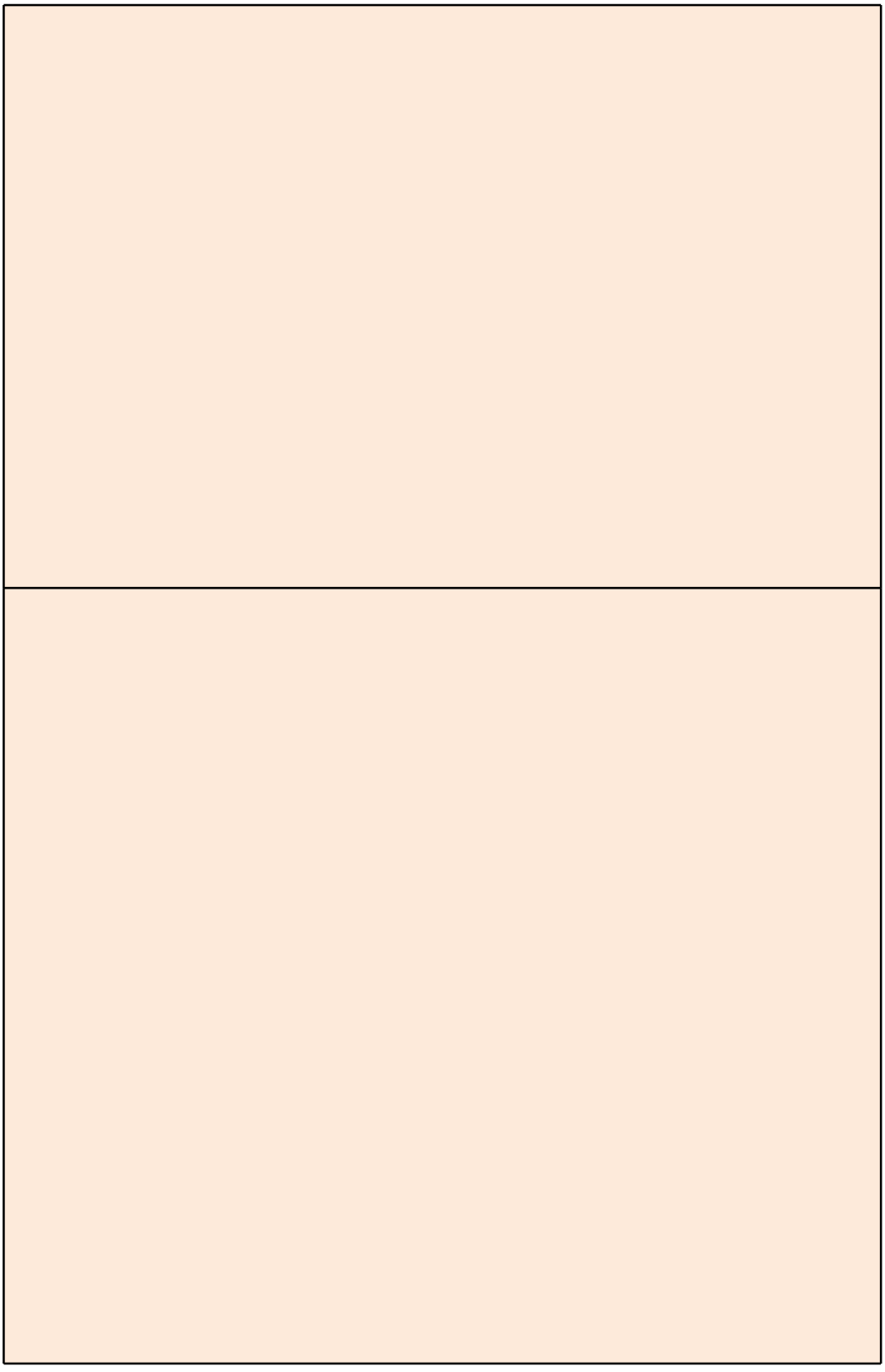

SYT-5412
SYT-5413
SYT-5414

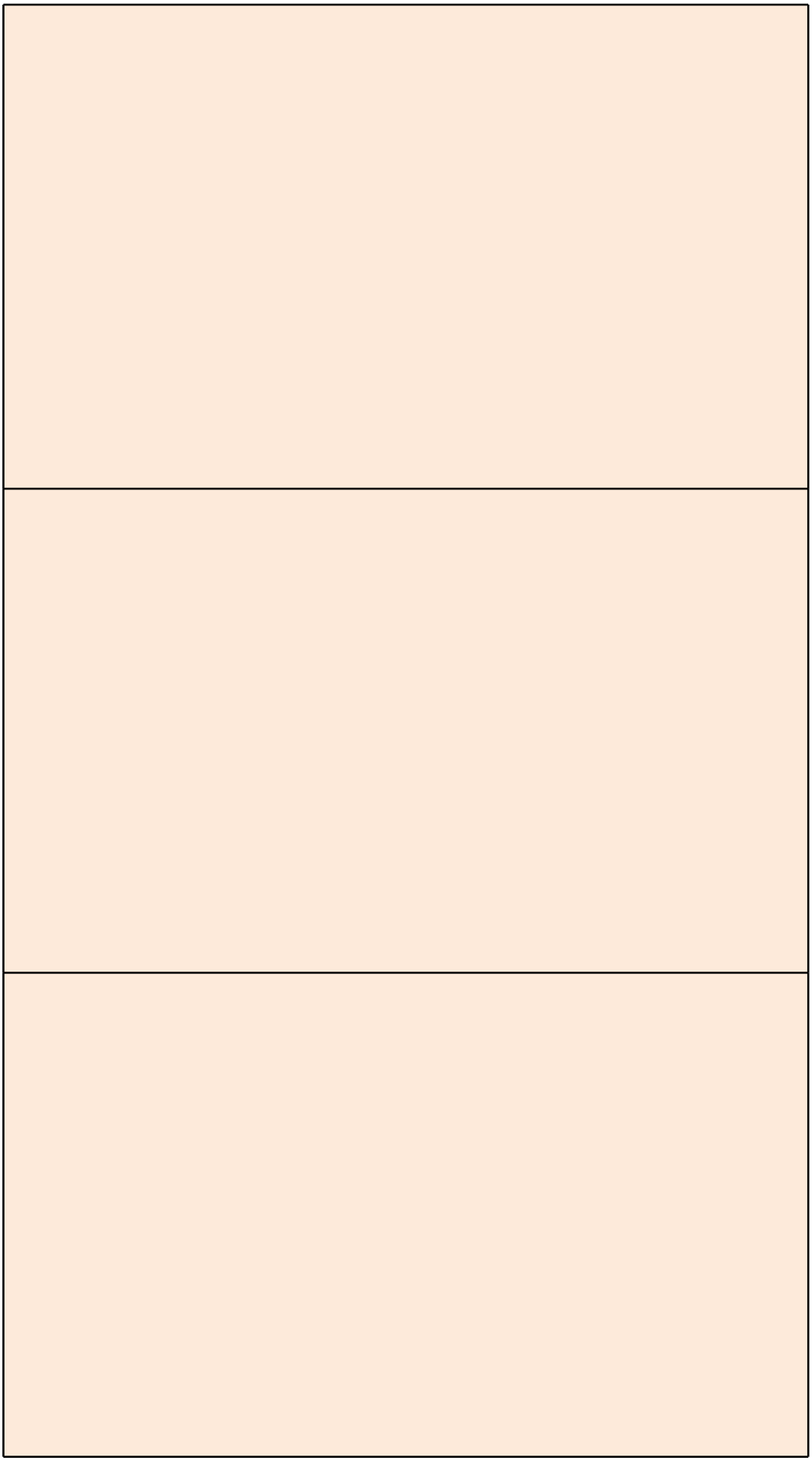

SYT-5410
SYT-5411
SYT-5408

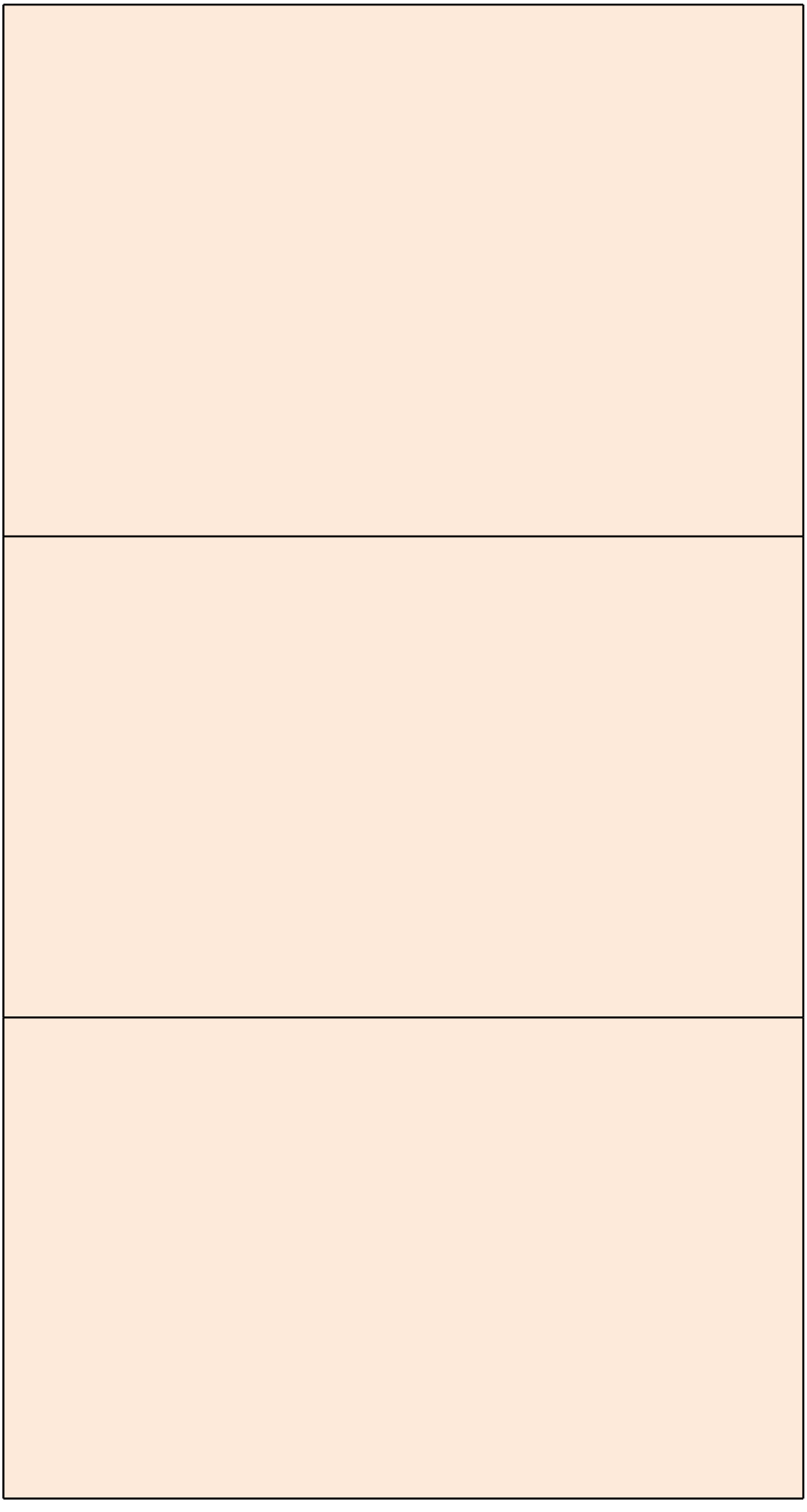

SYT-5409
SYT-5406

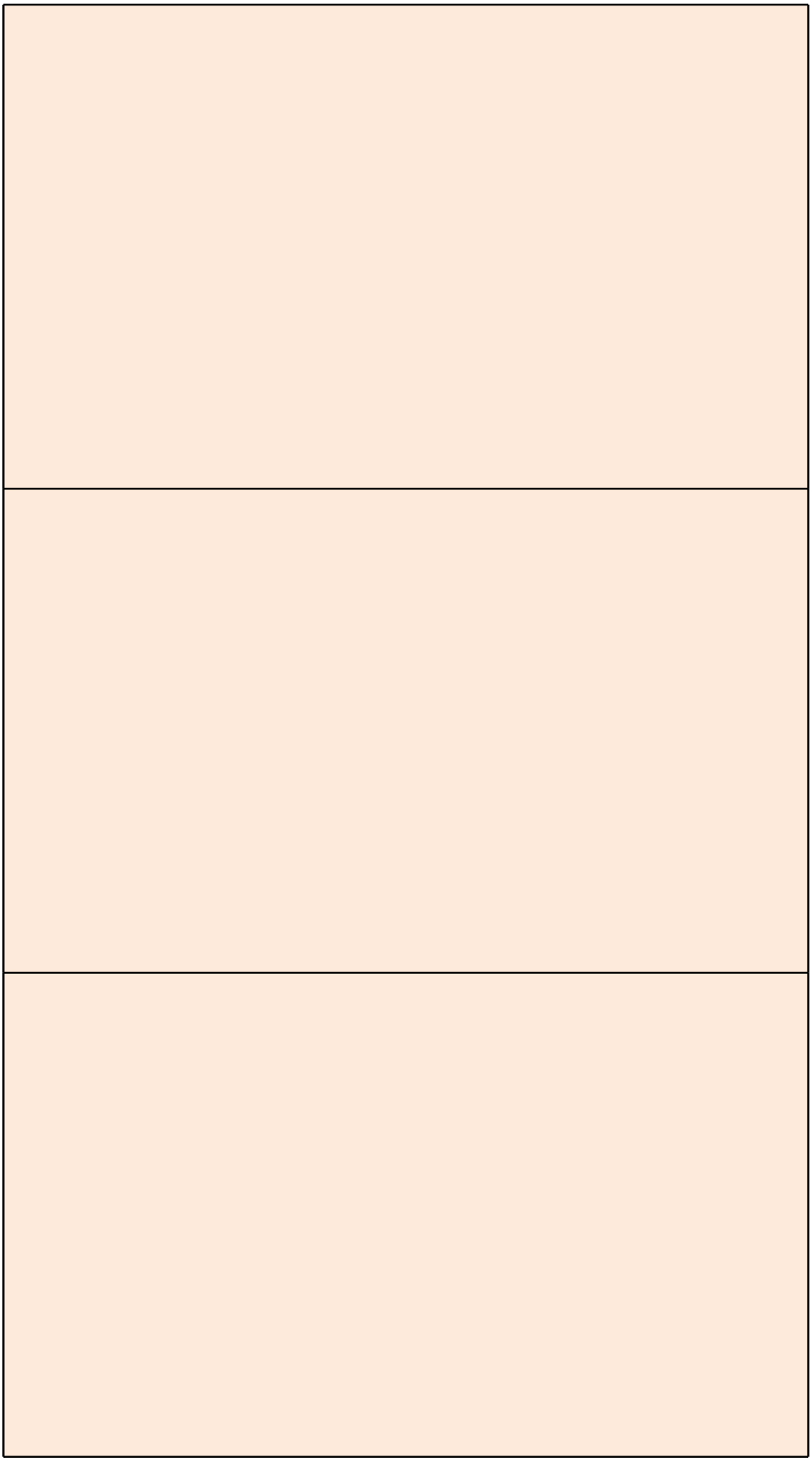

SYT-5407
SYT-5405

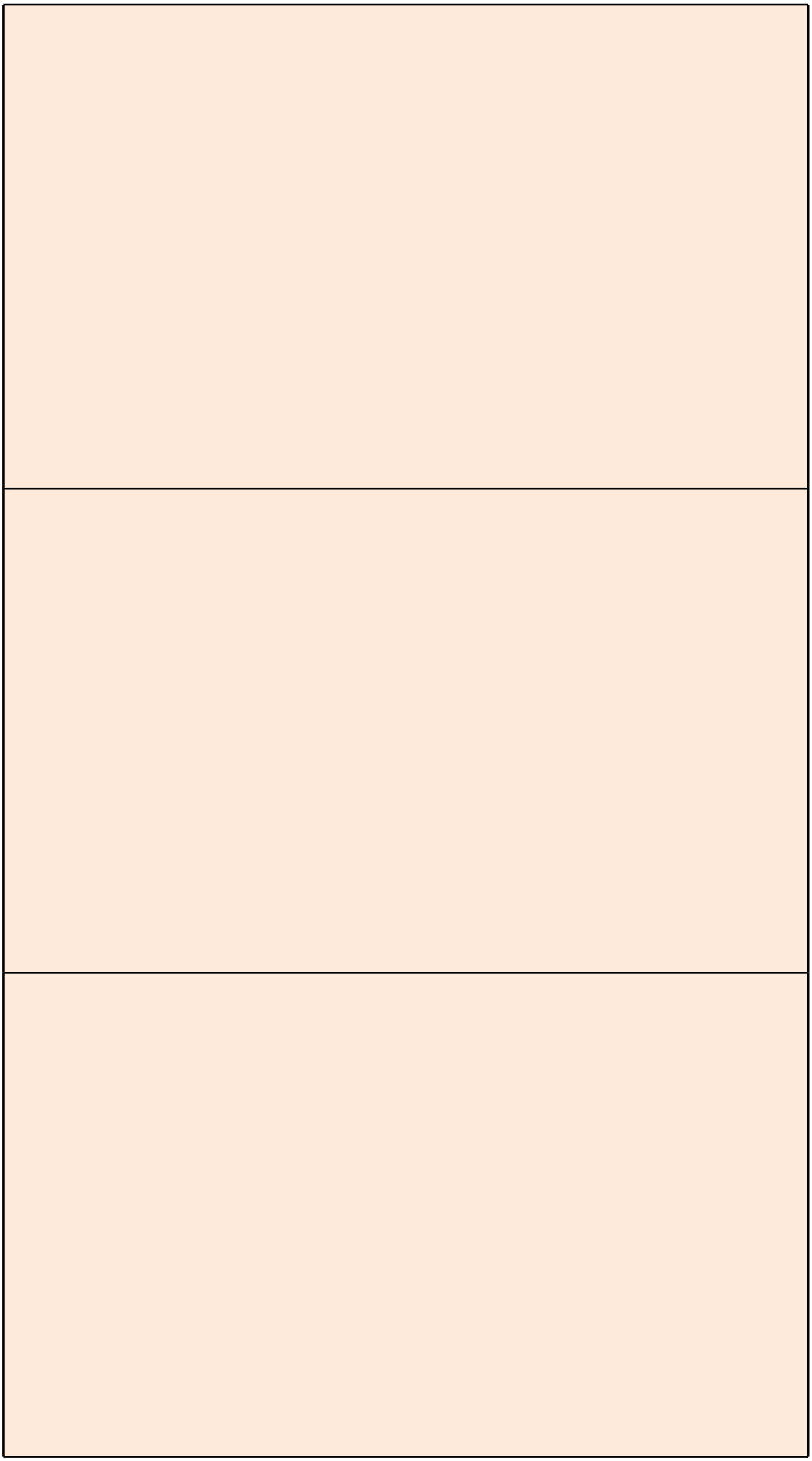
Ehdotus uudeksi tekstiksi

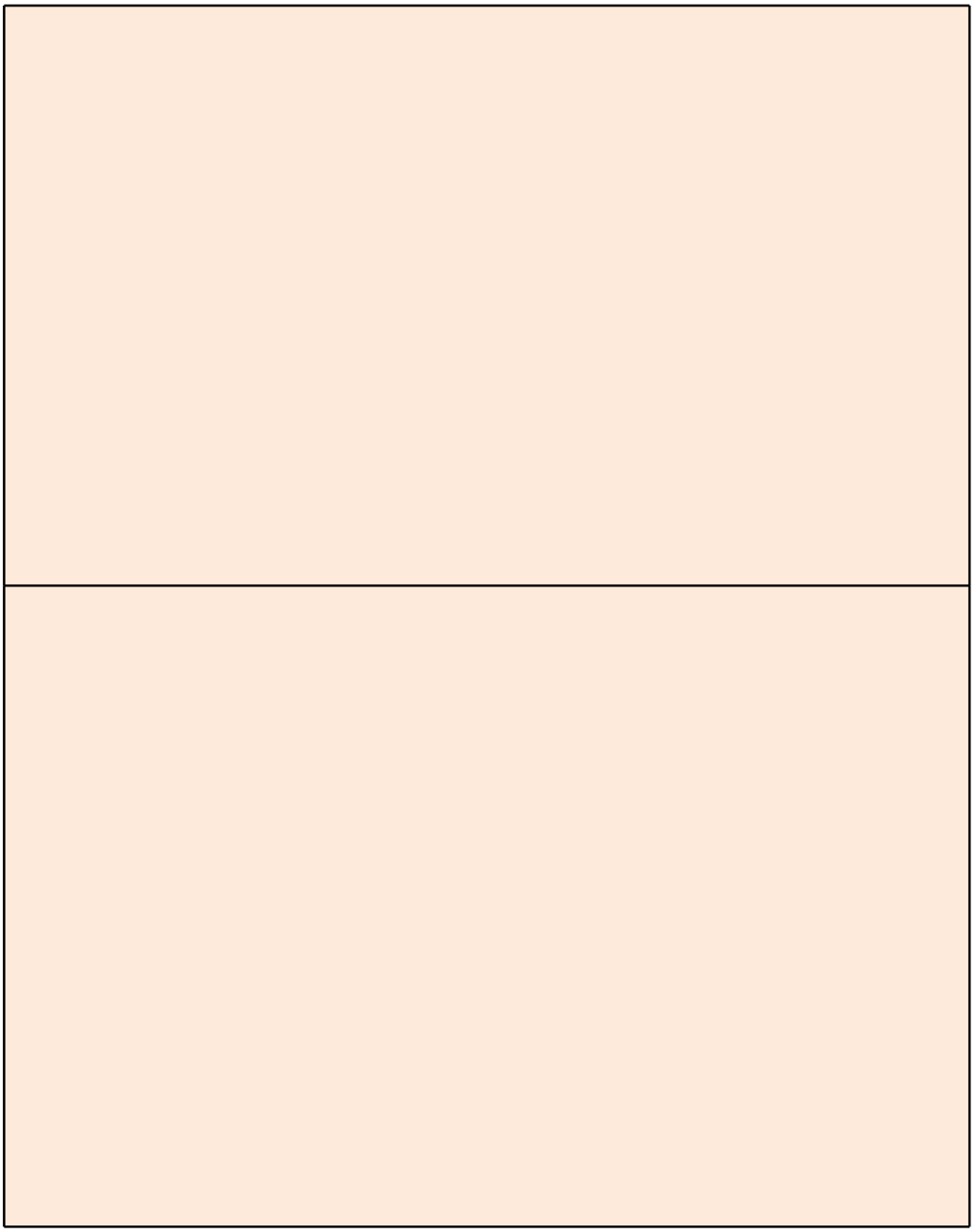


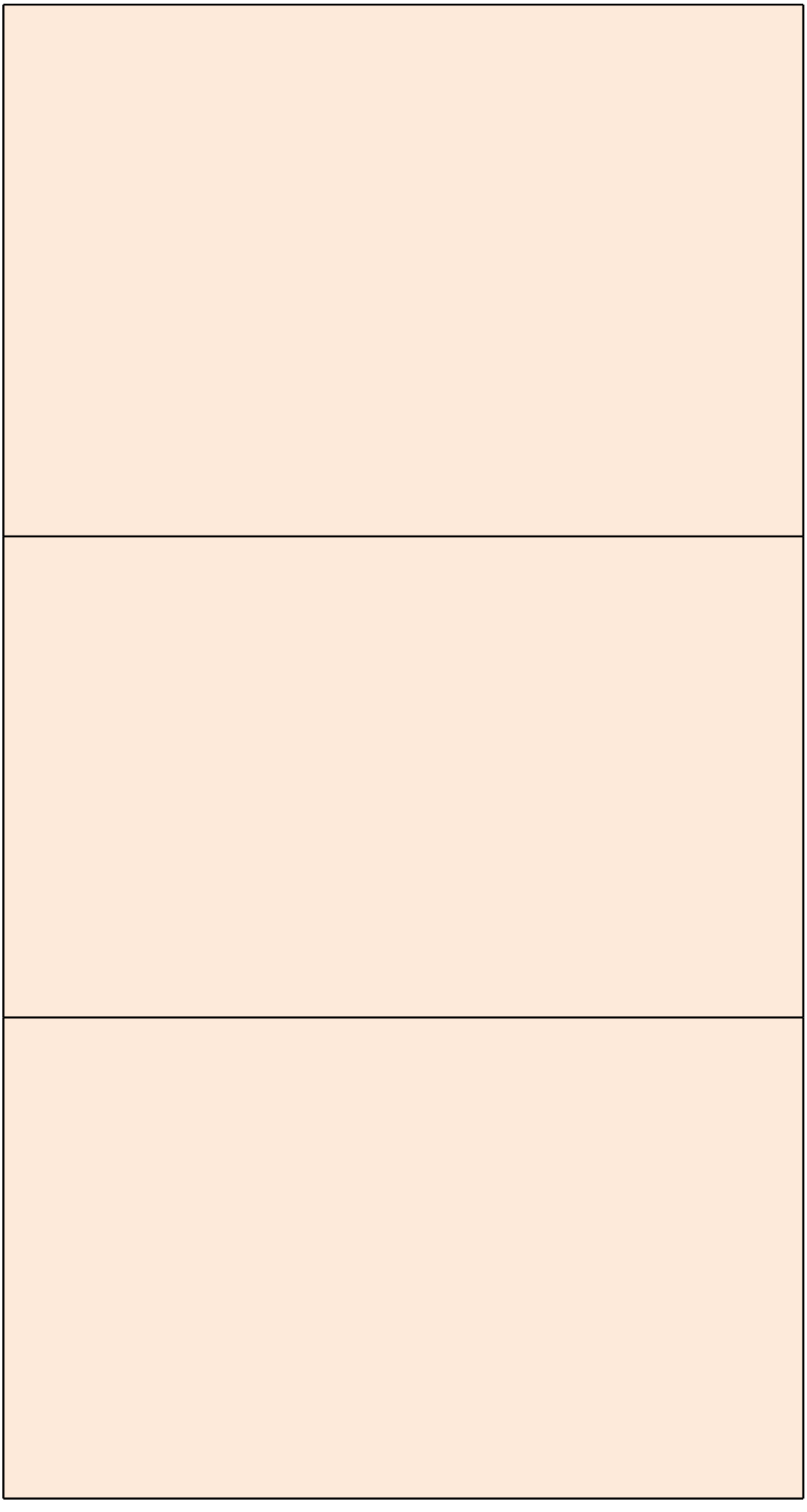


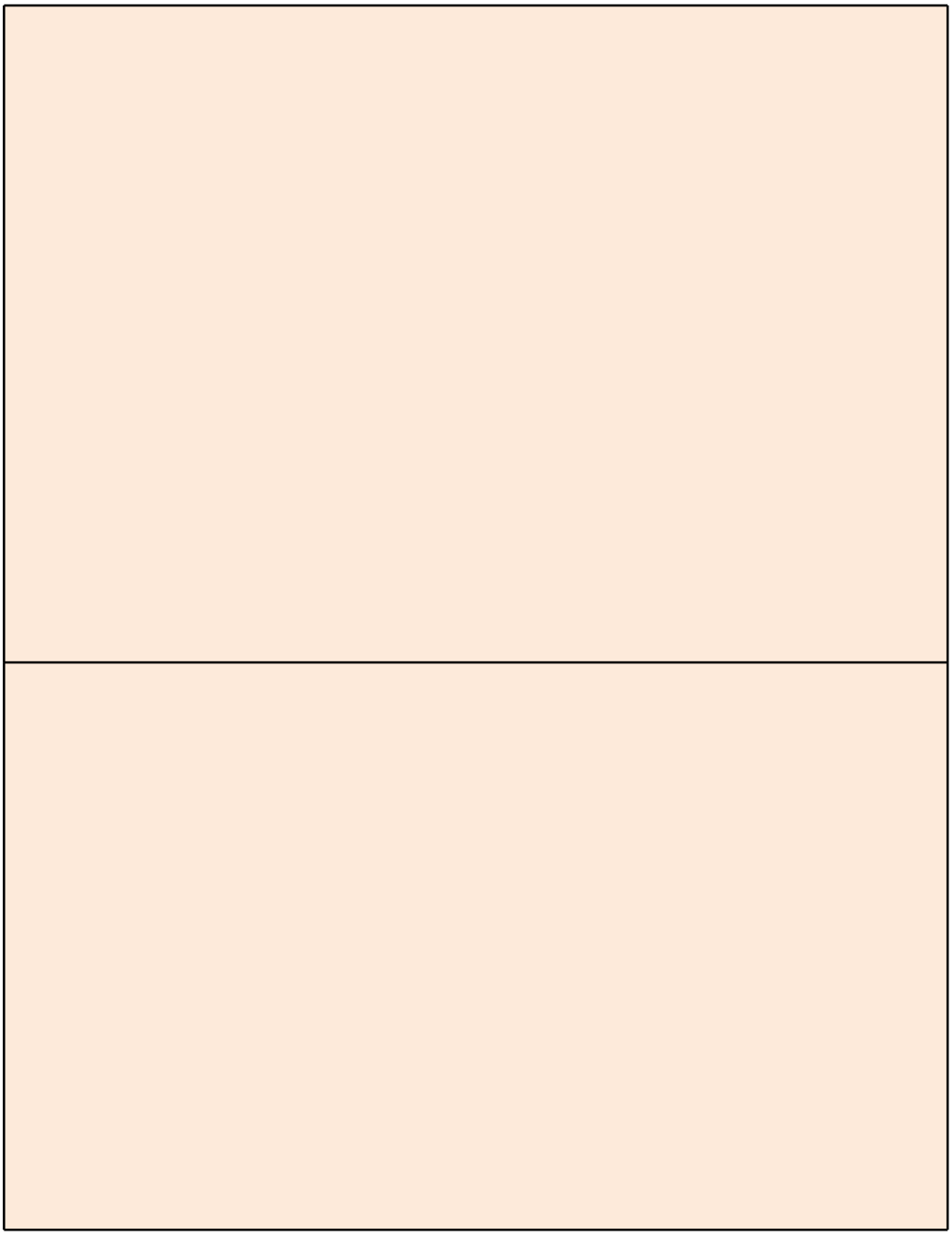


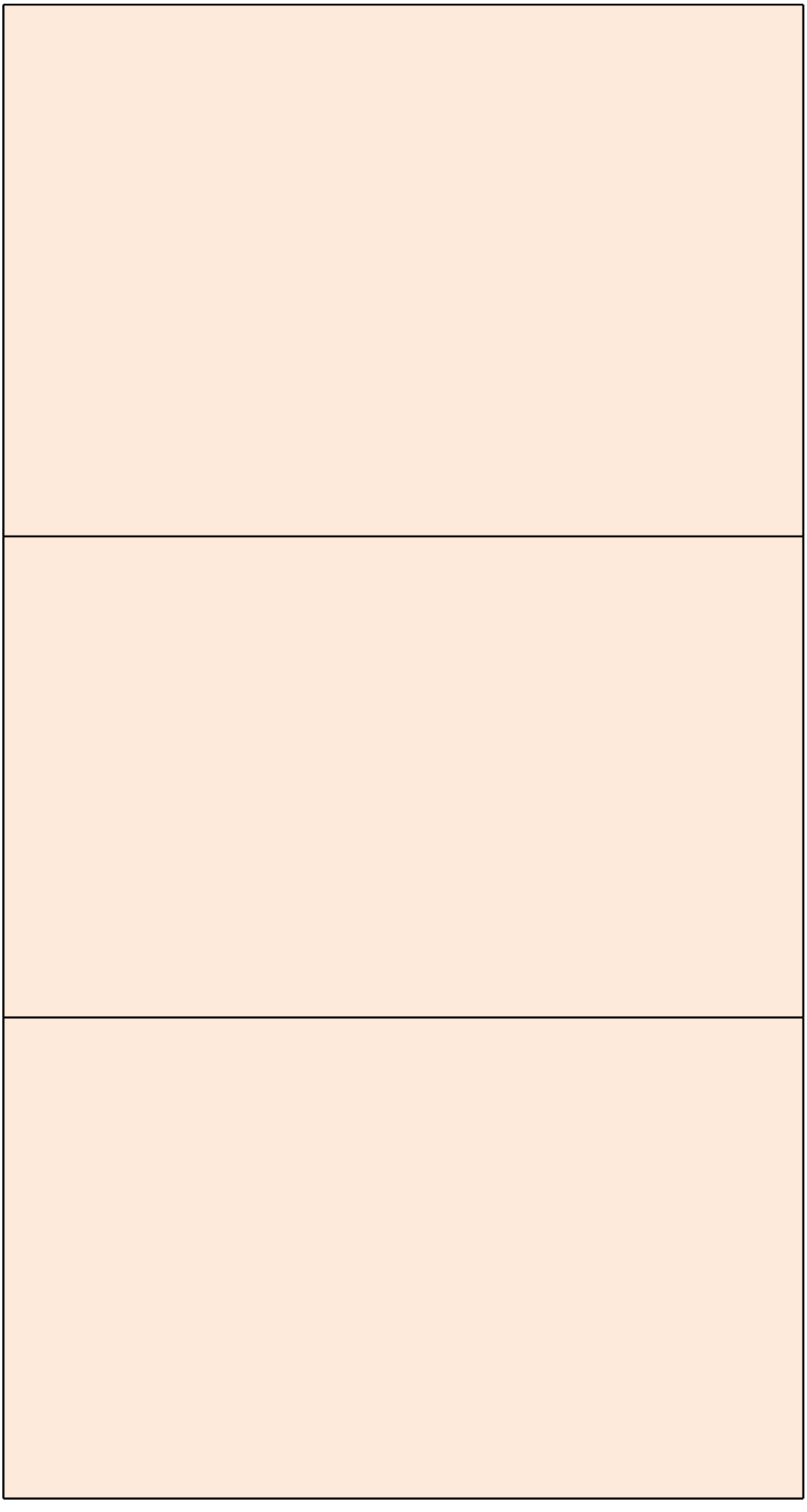


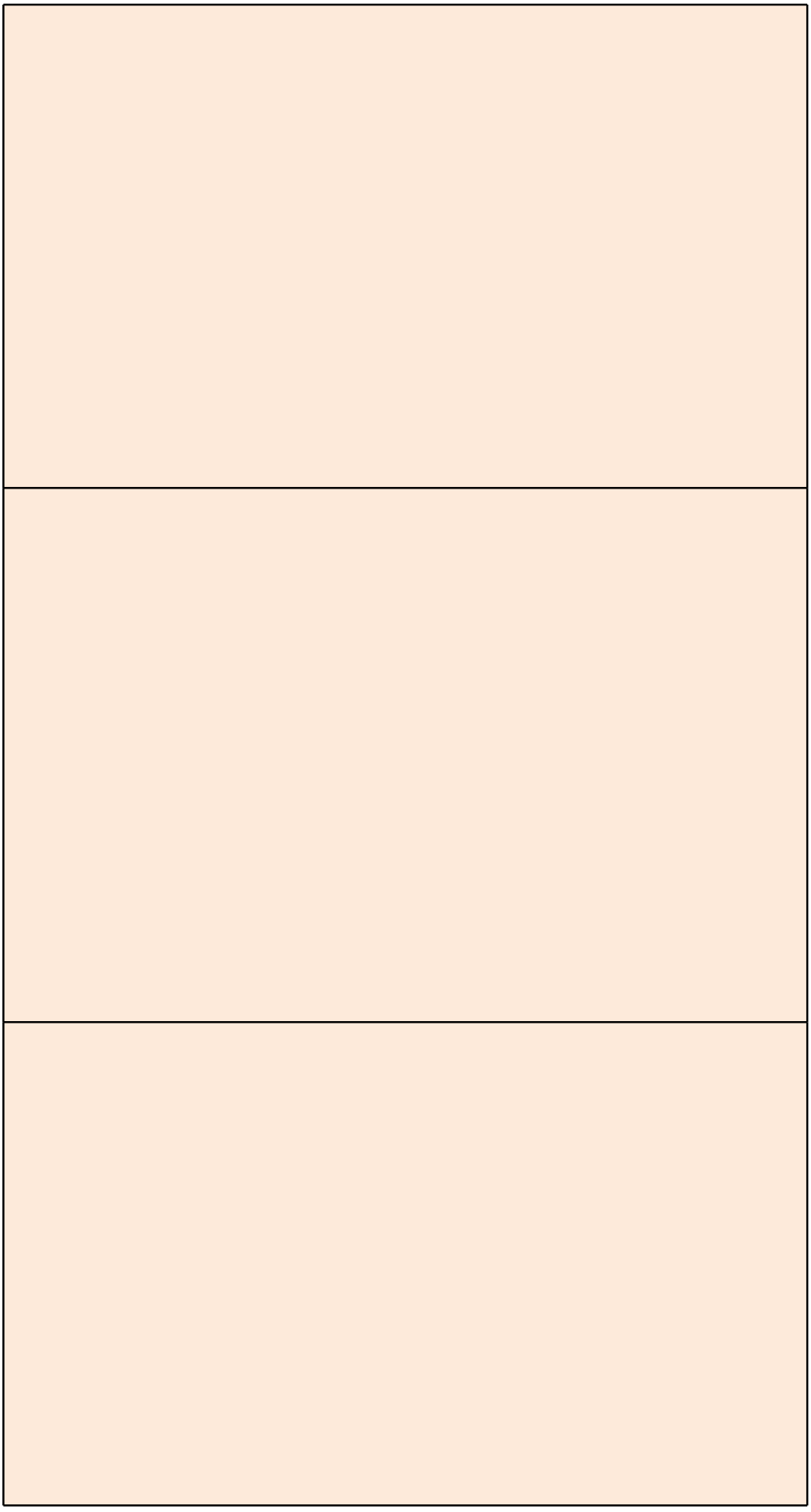


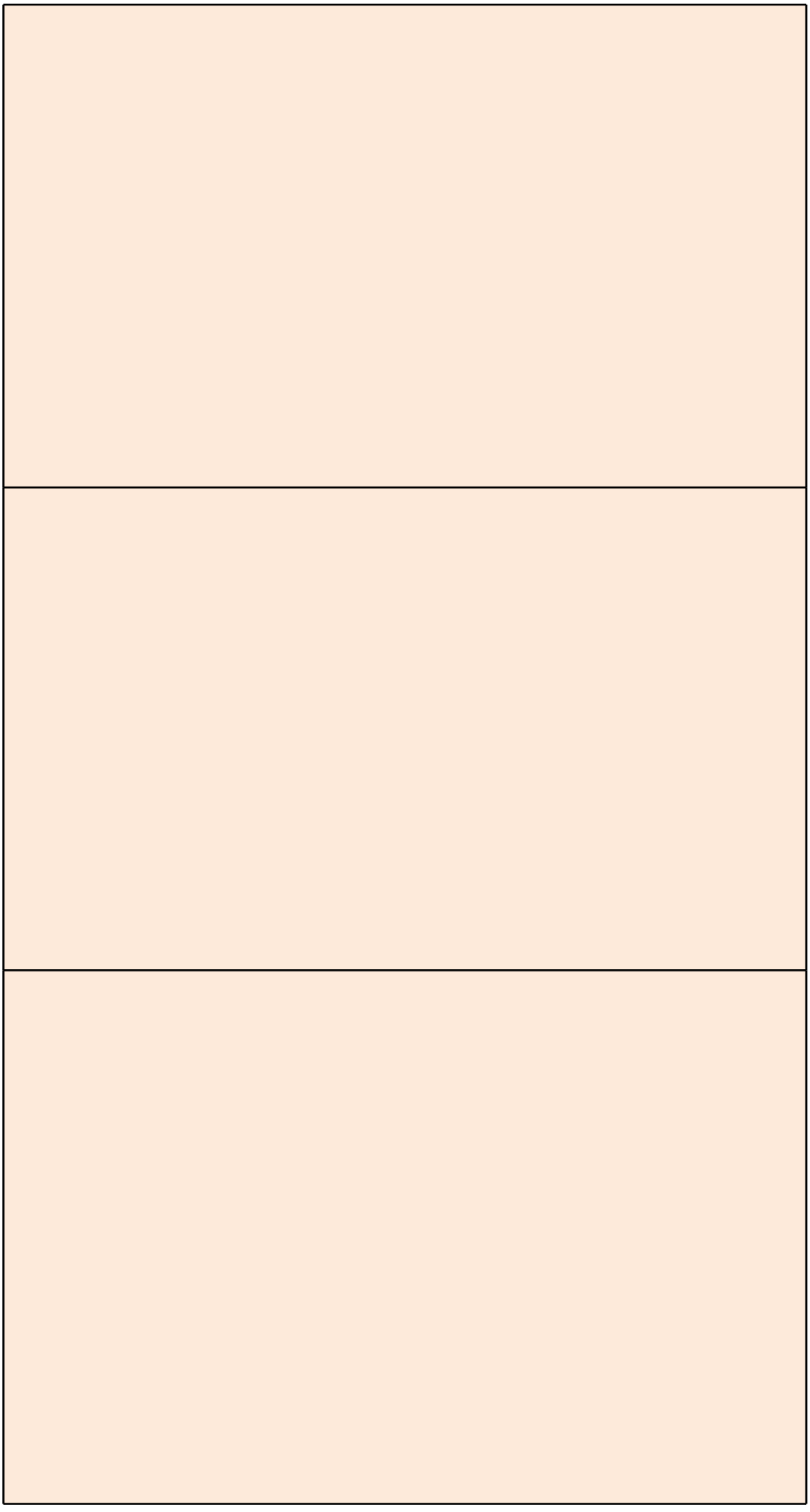


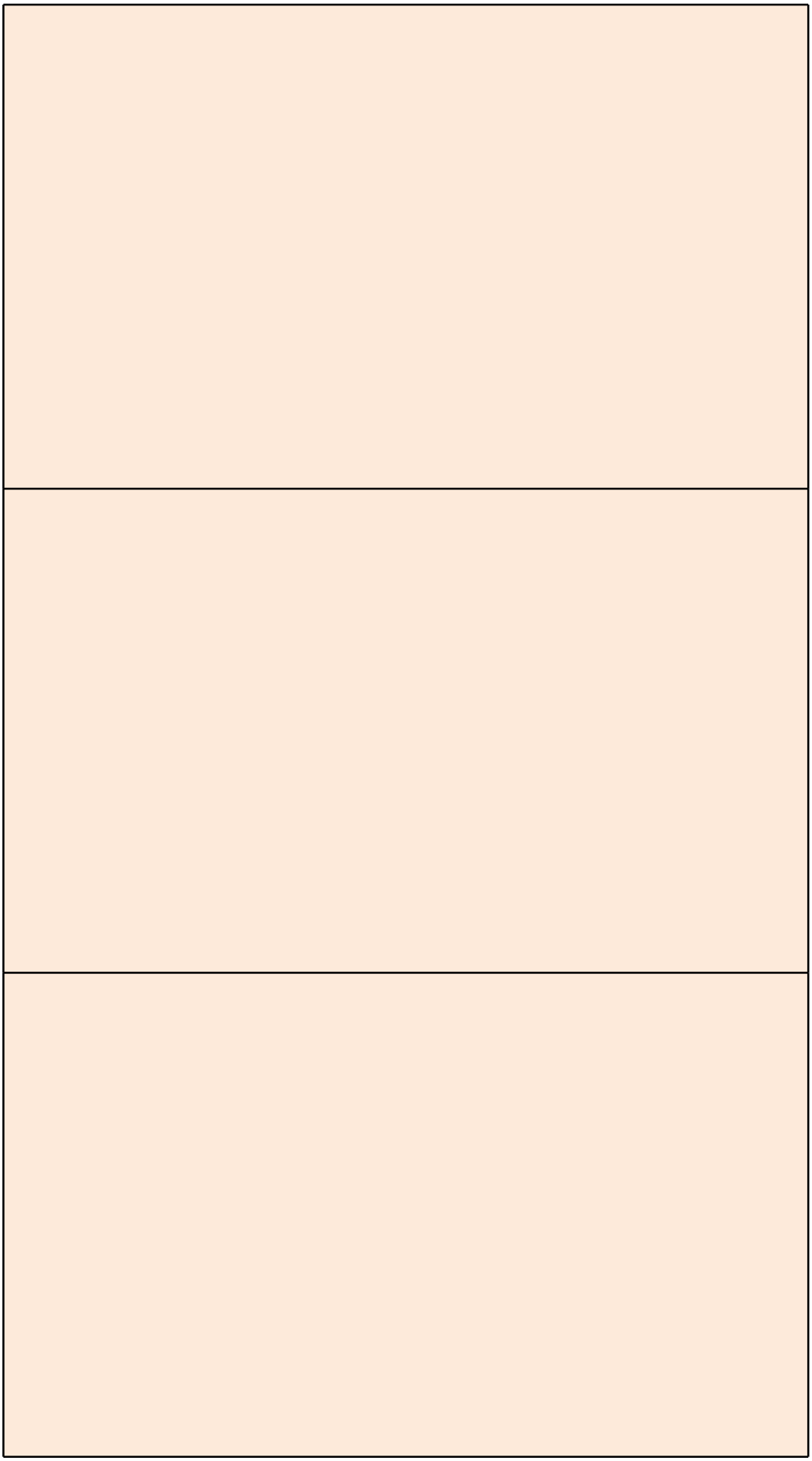


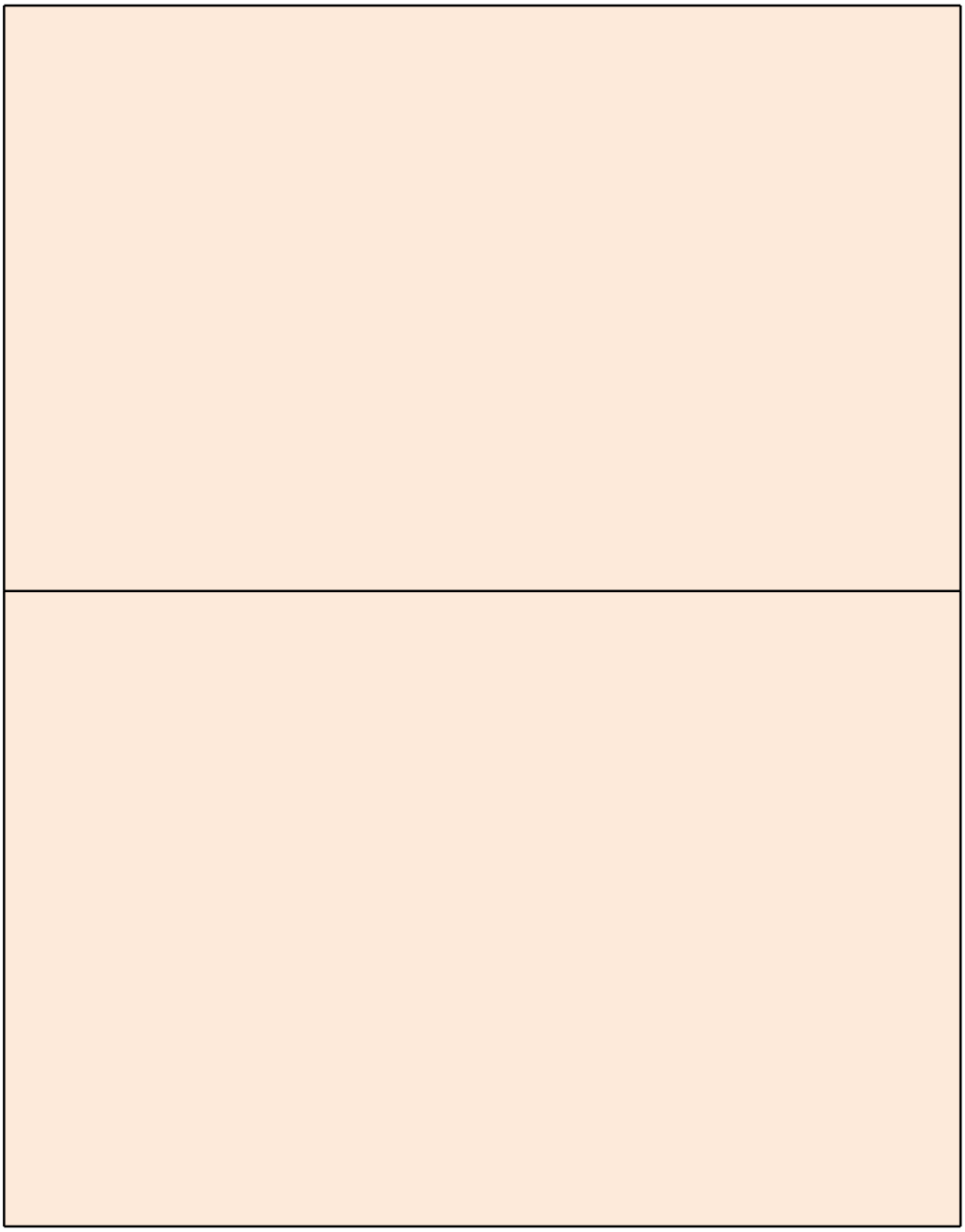


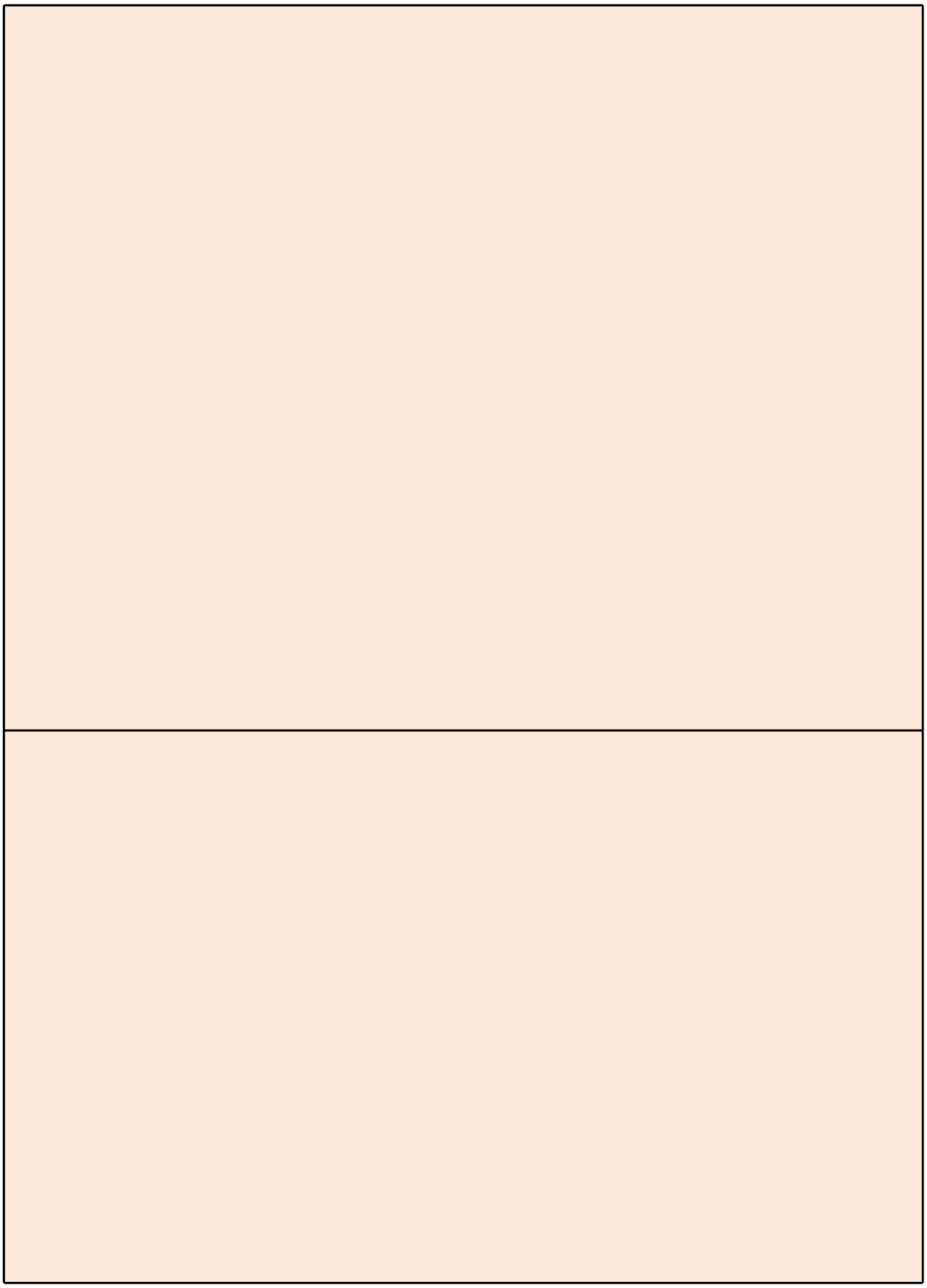


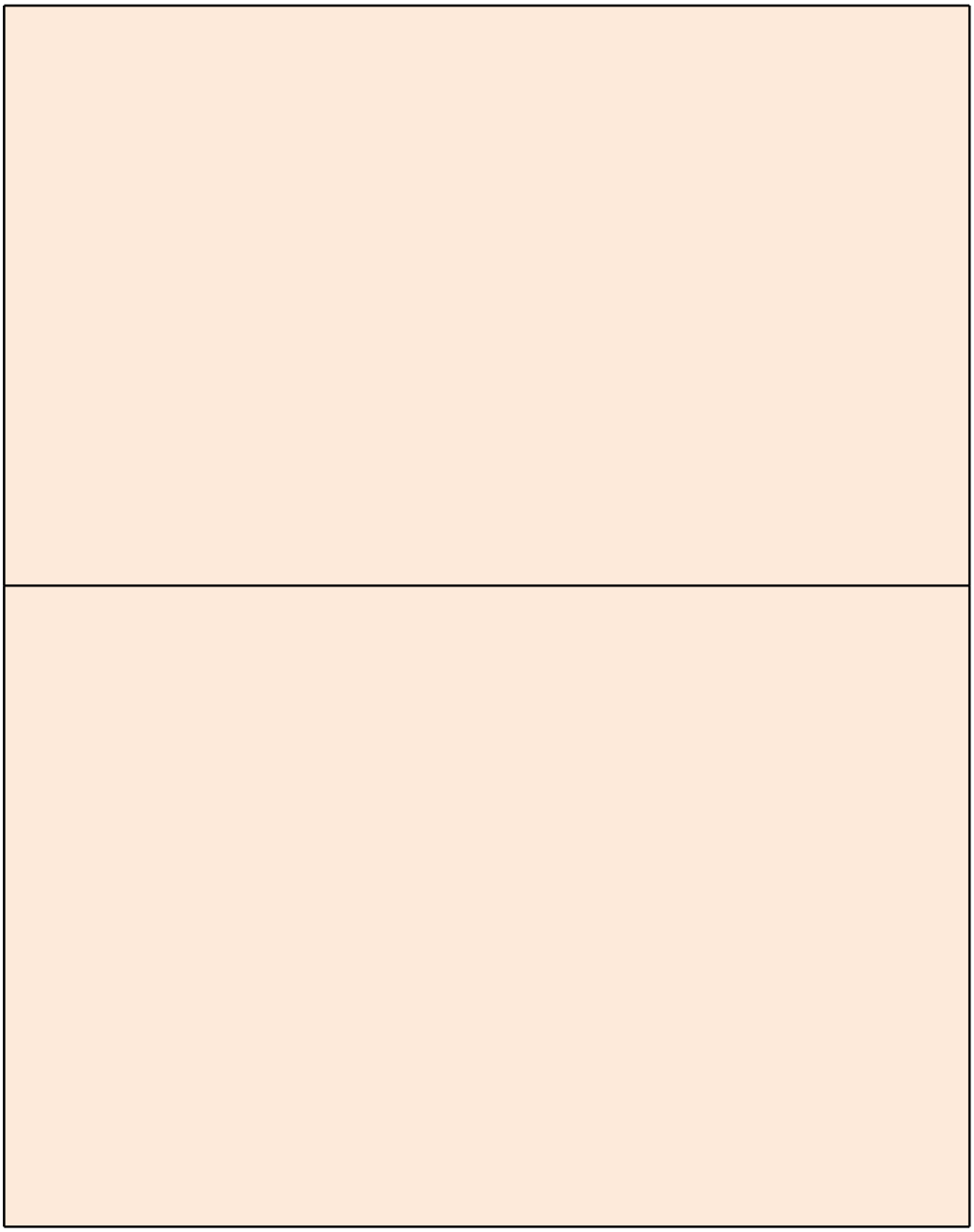


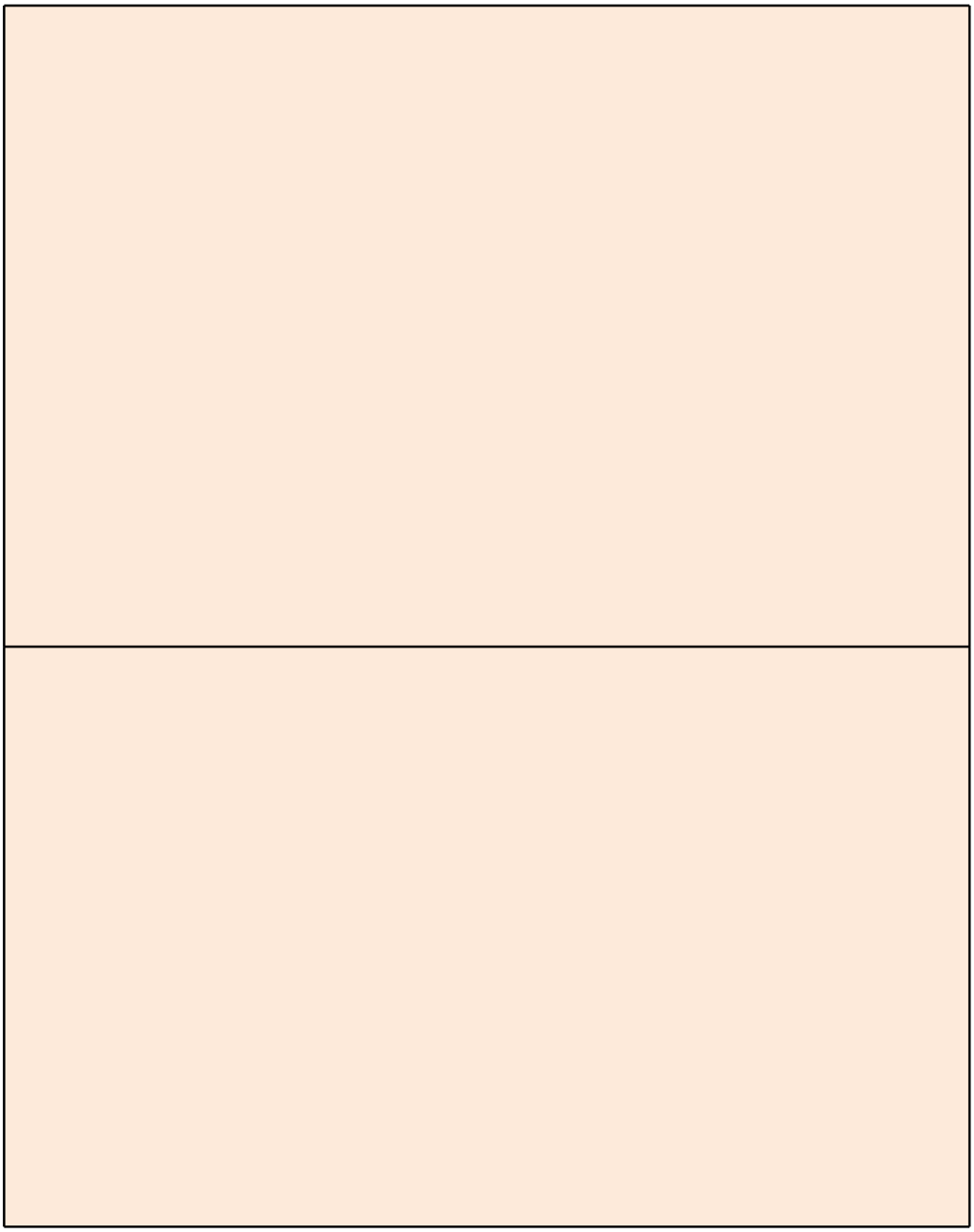


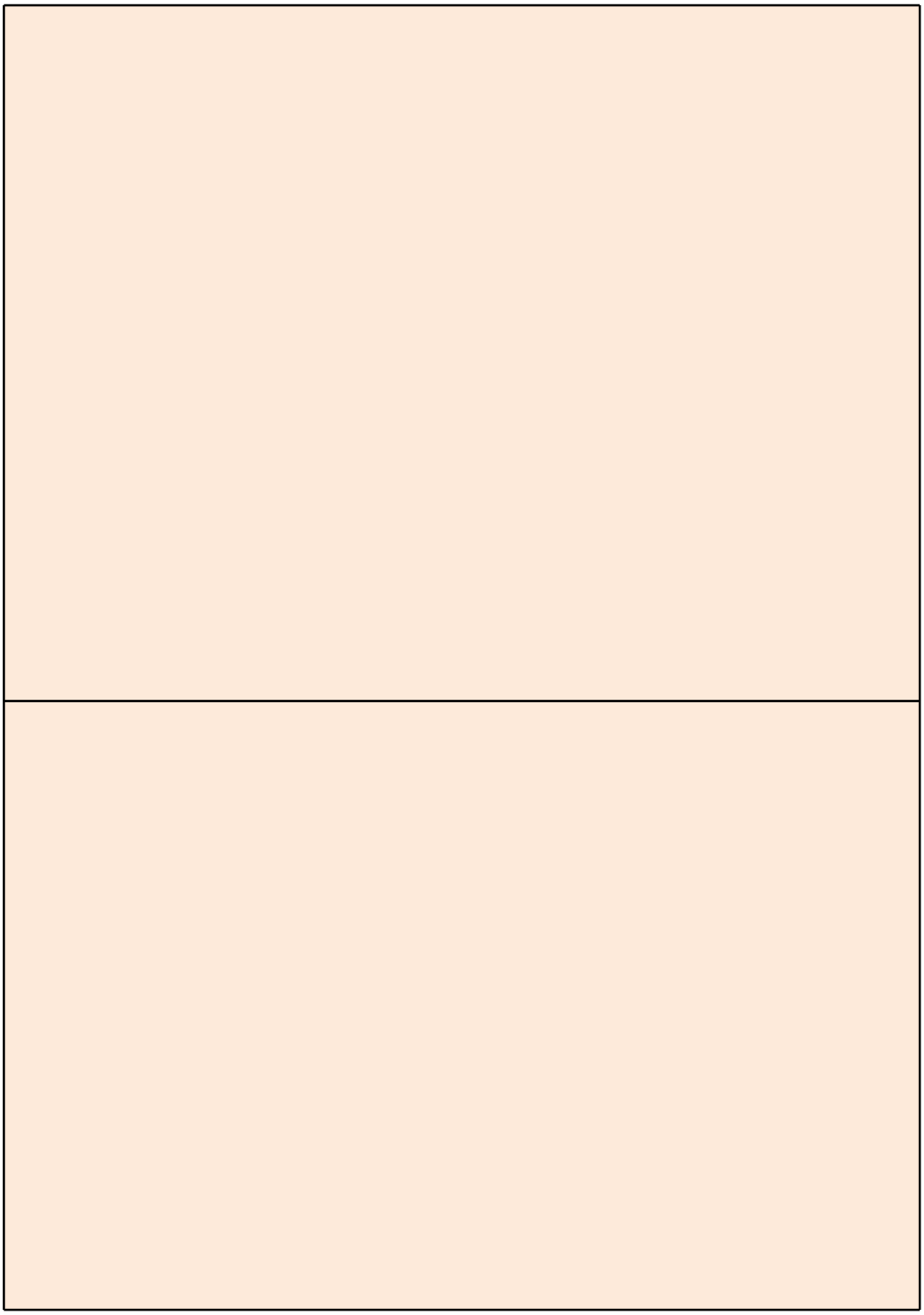


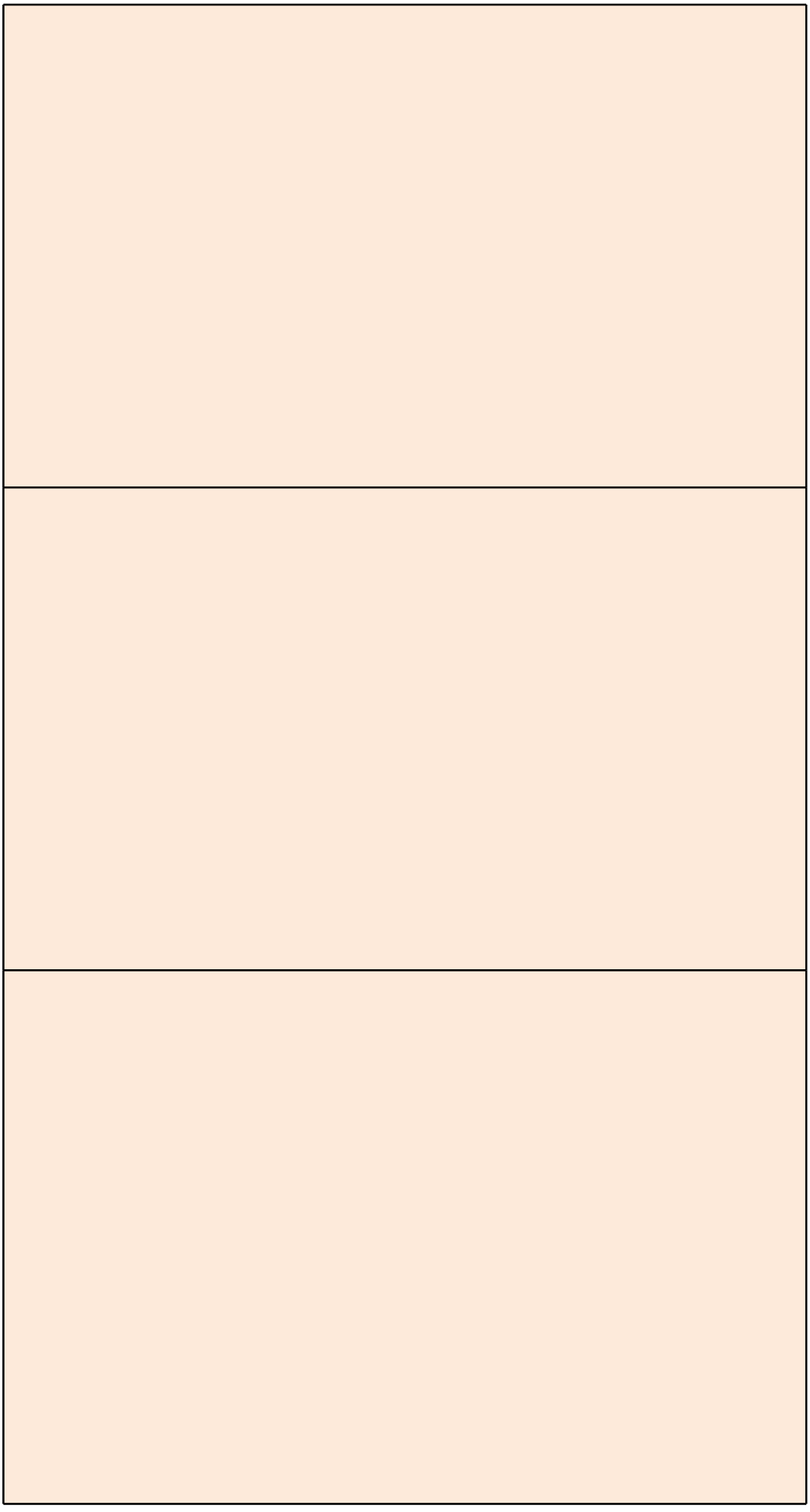


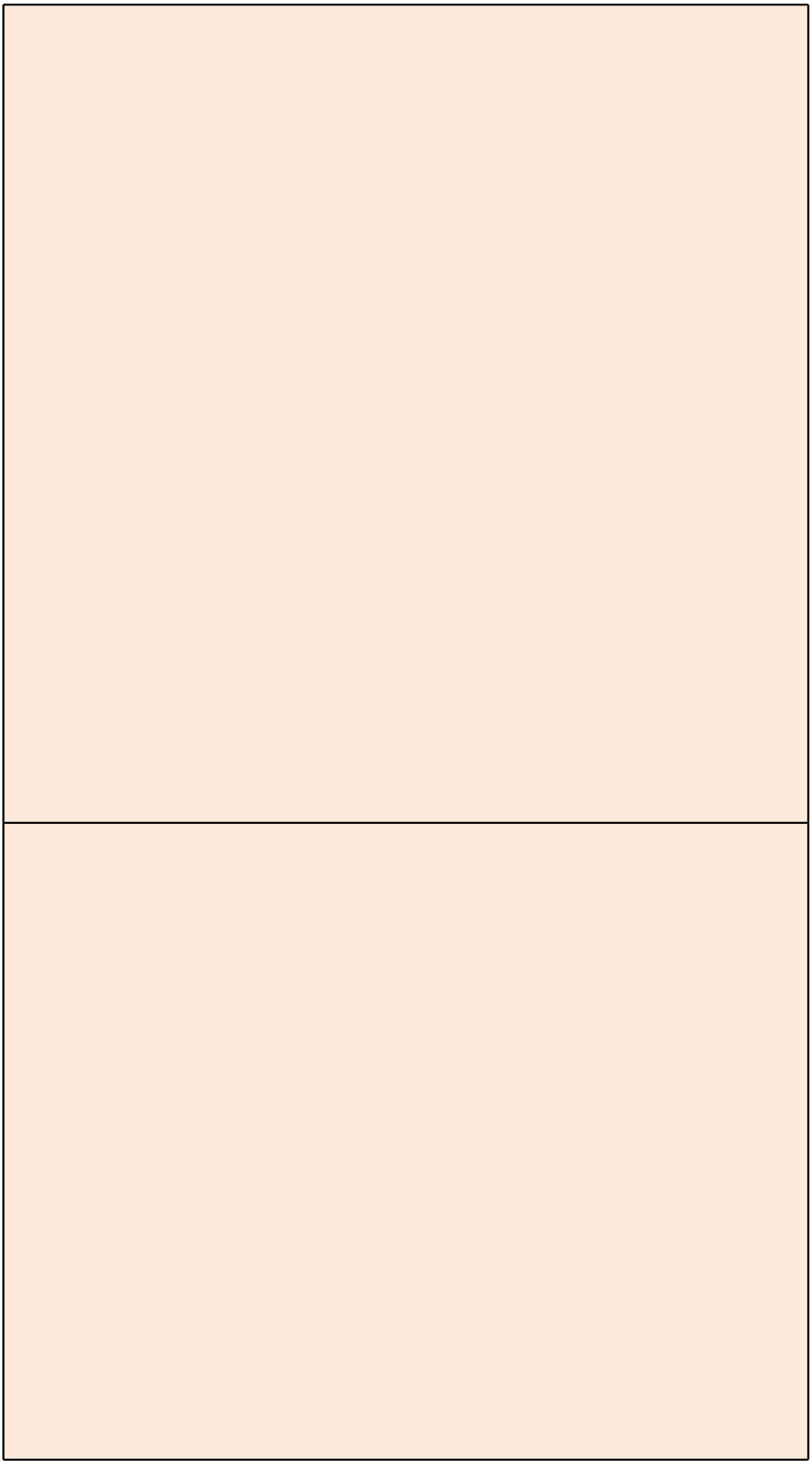


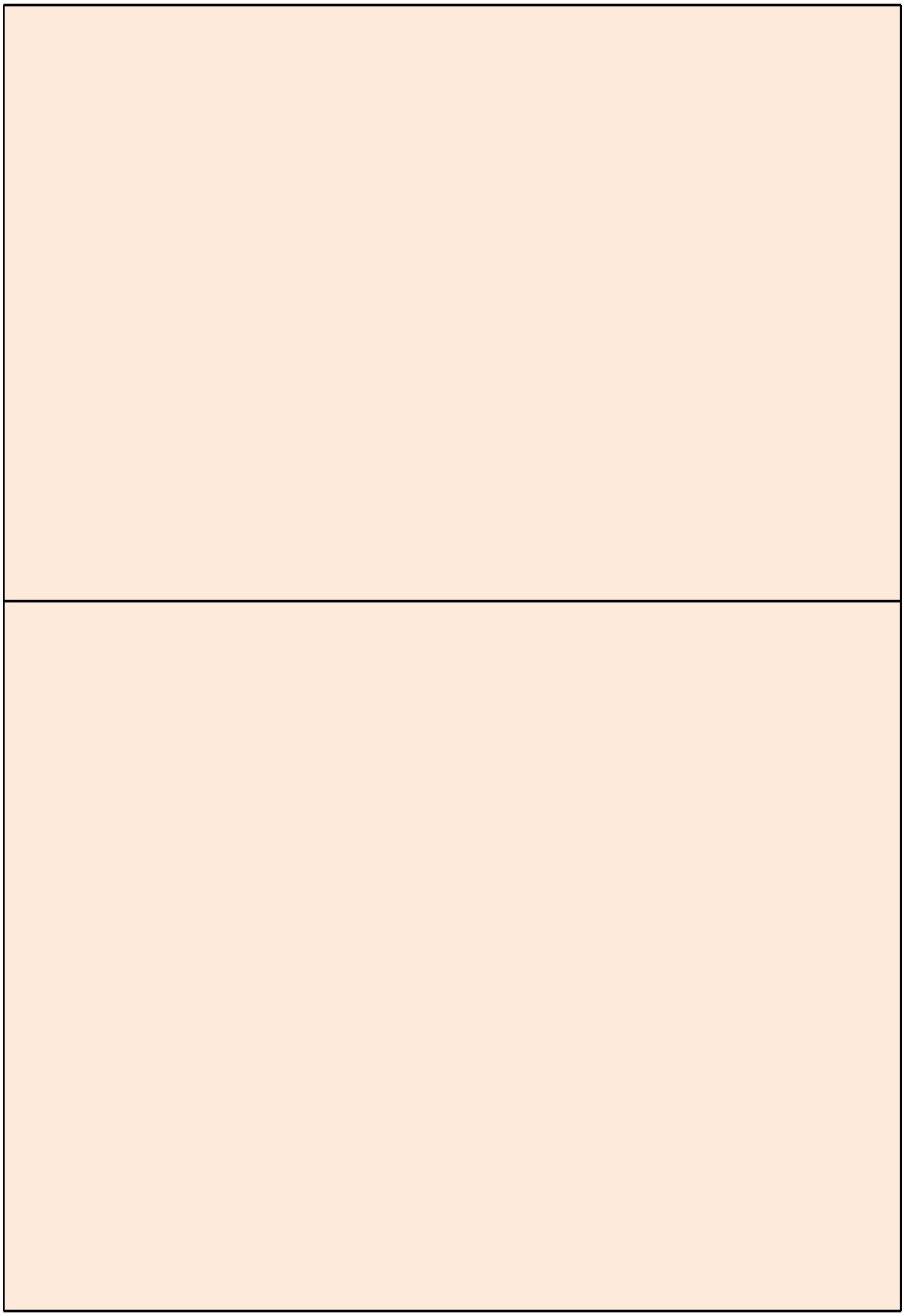


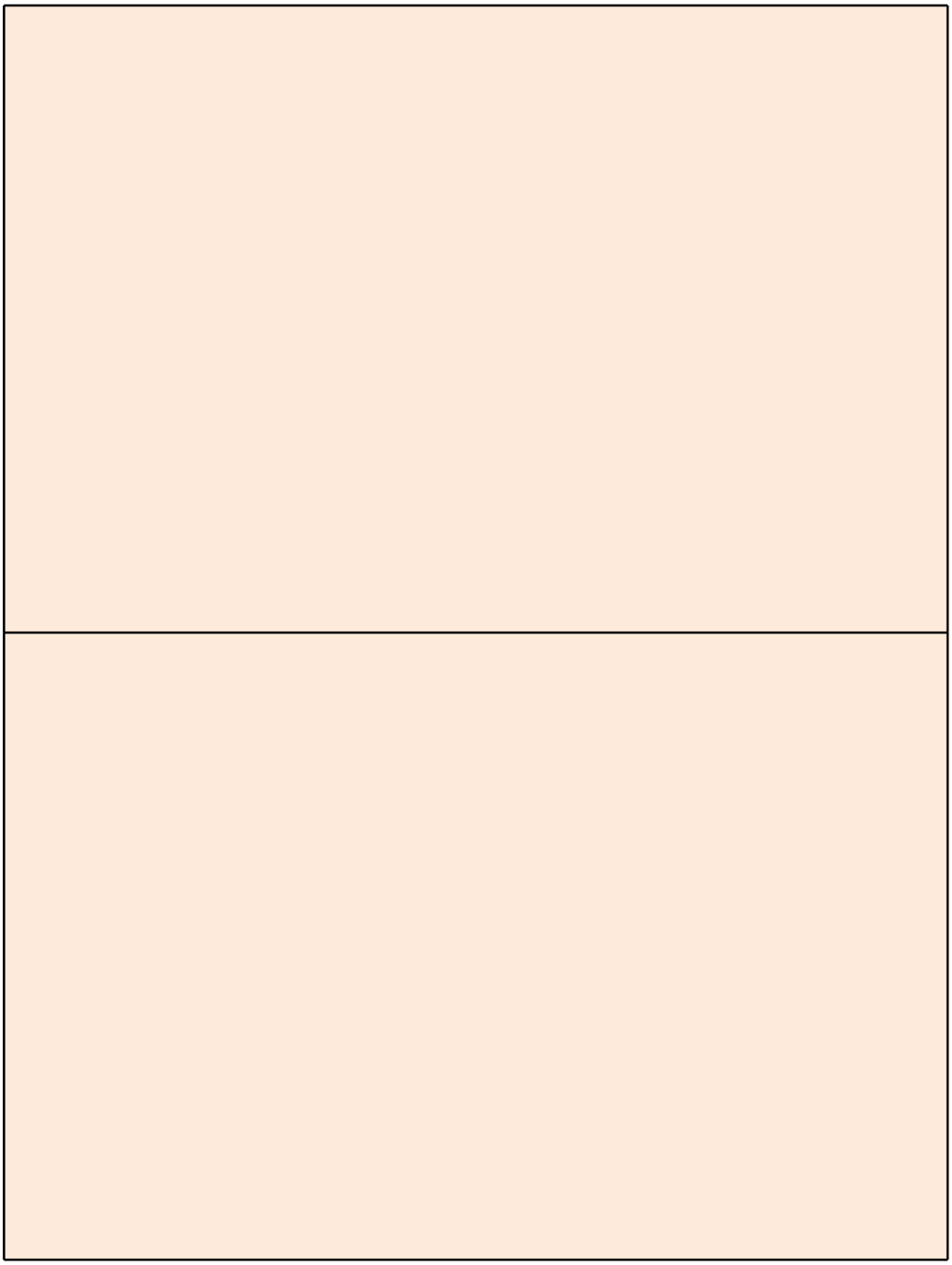


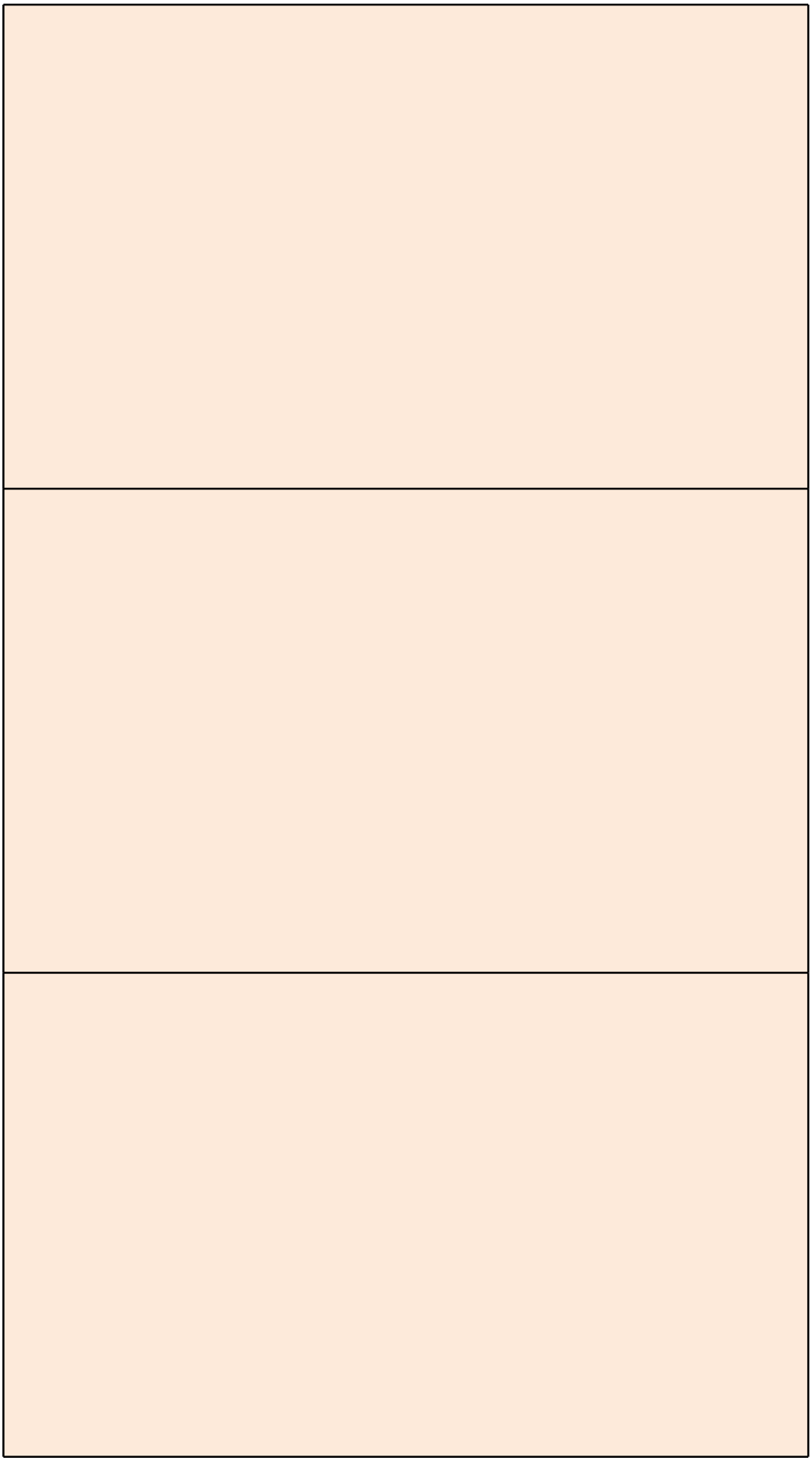


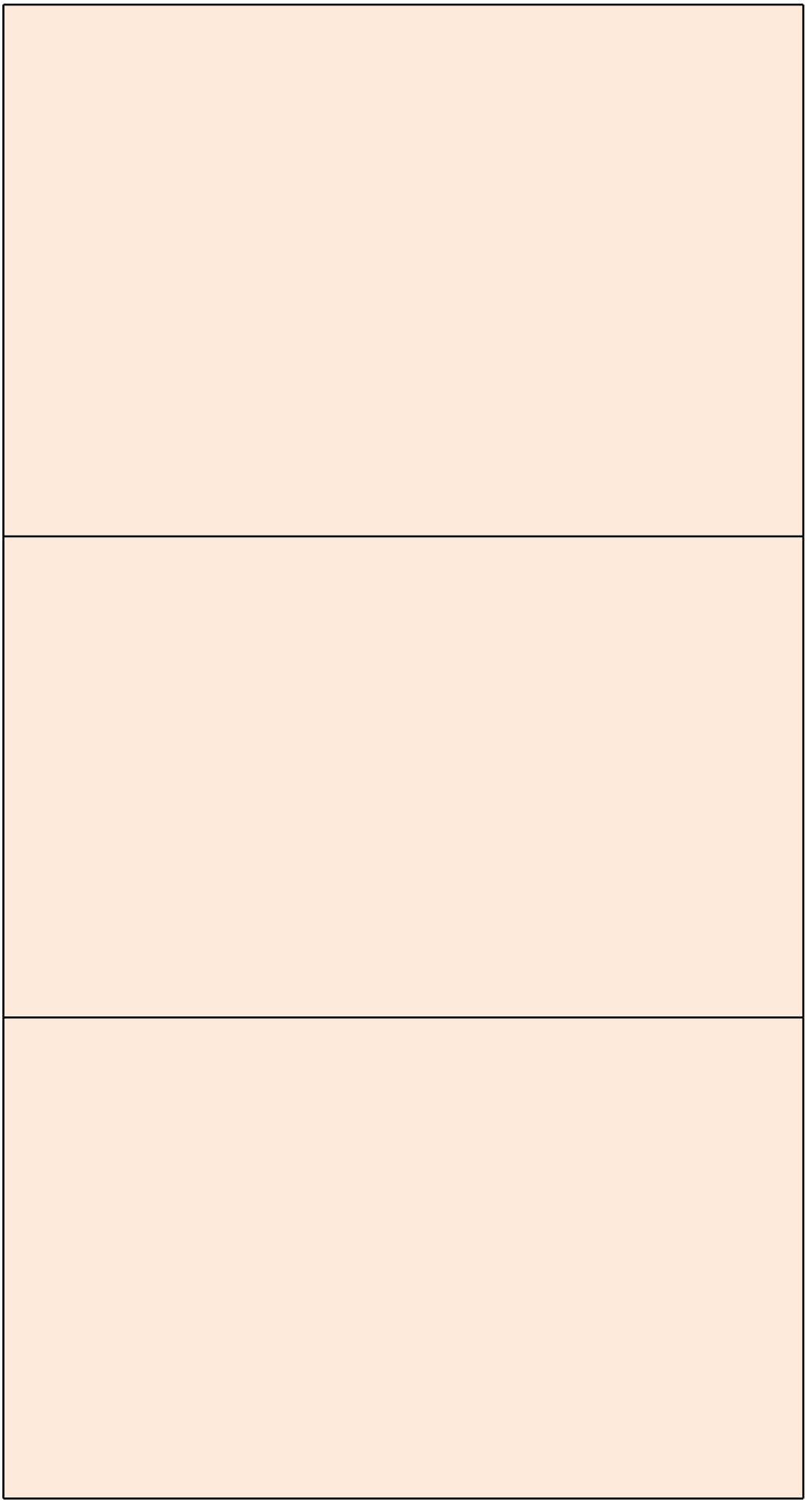


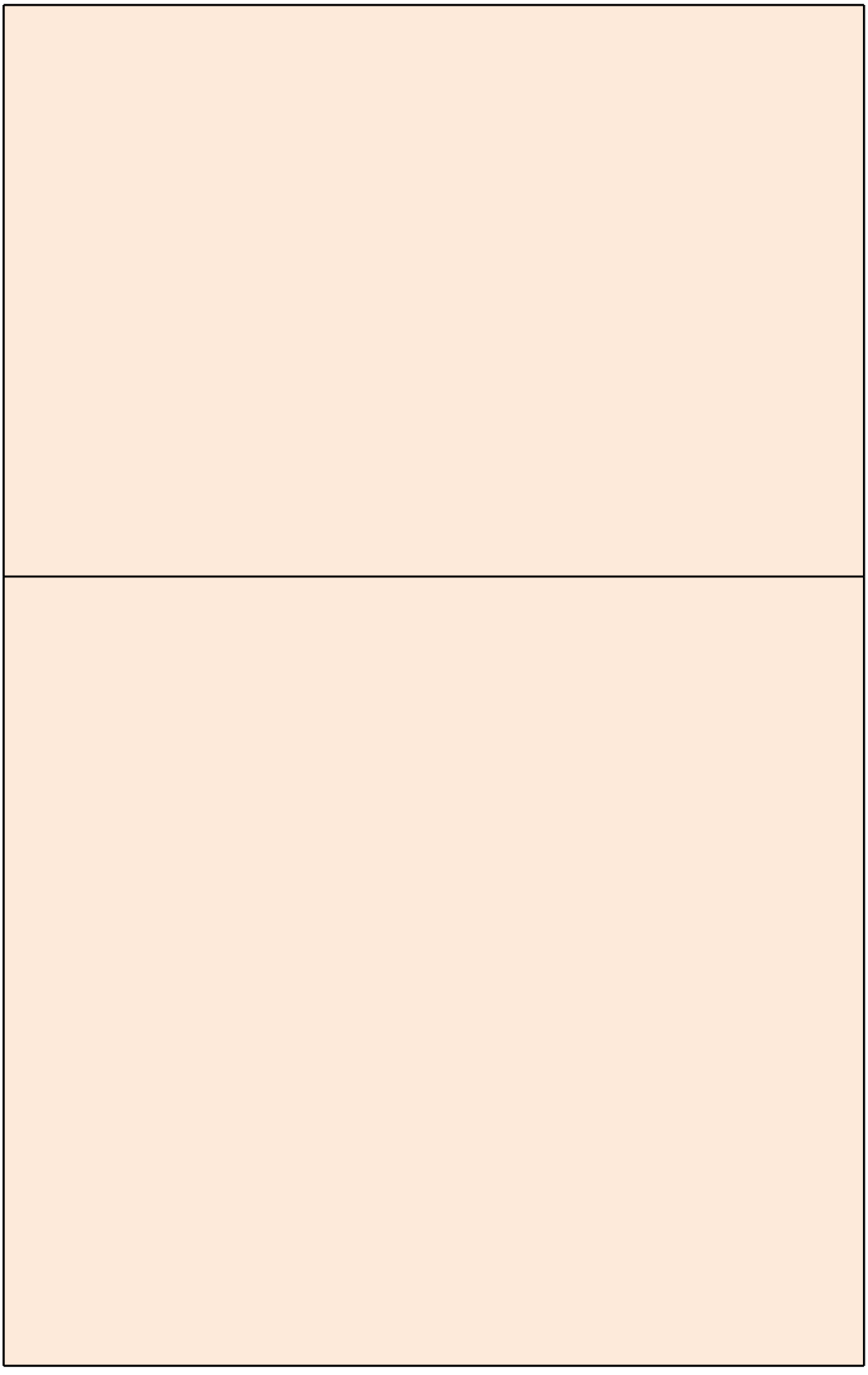


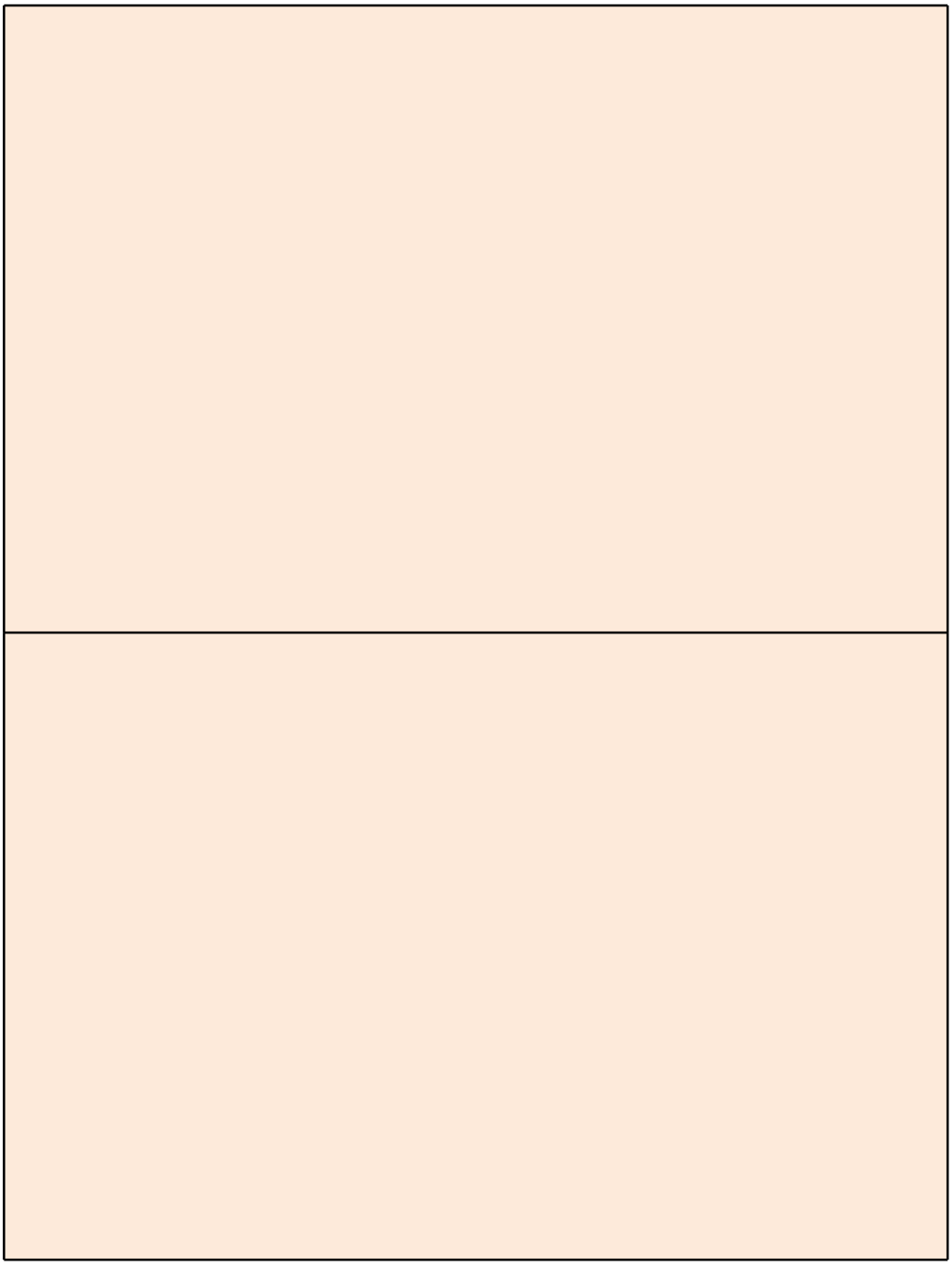


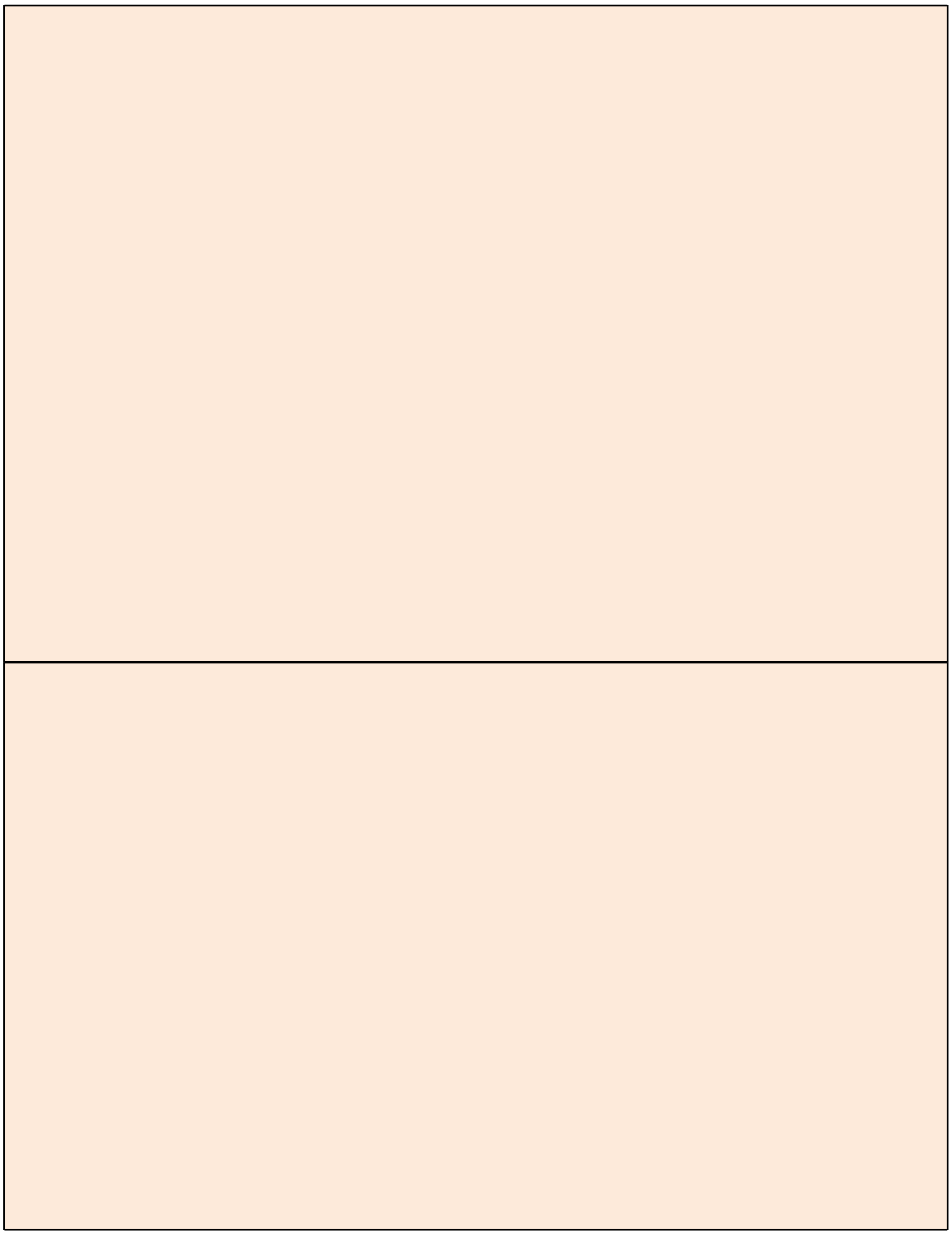


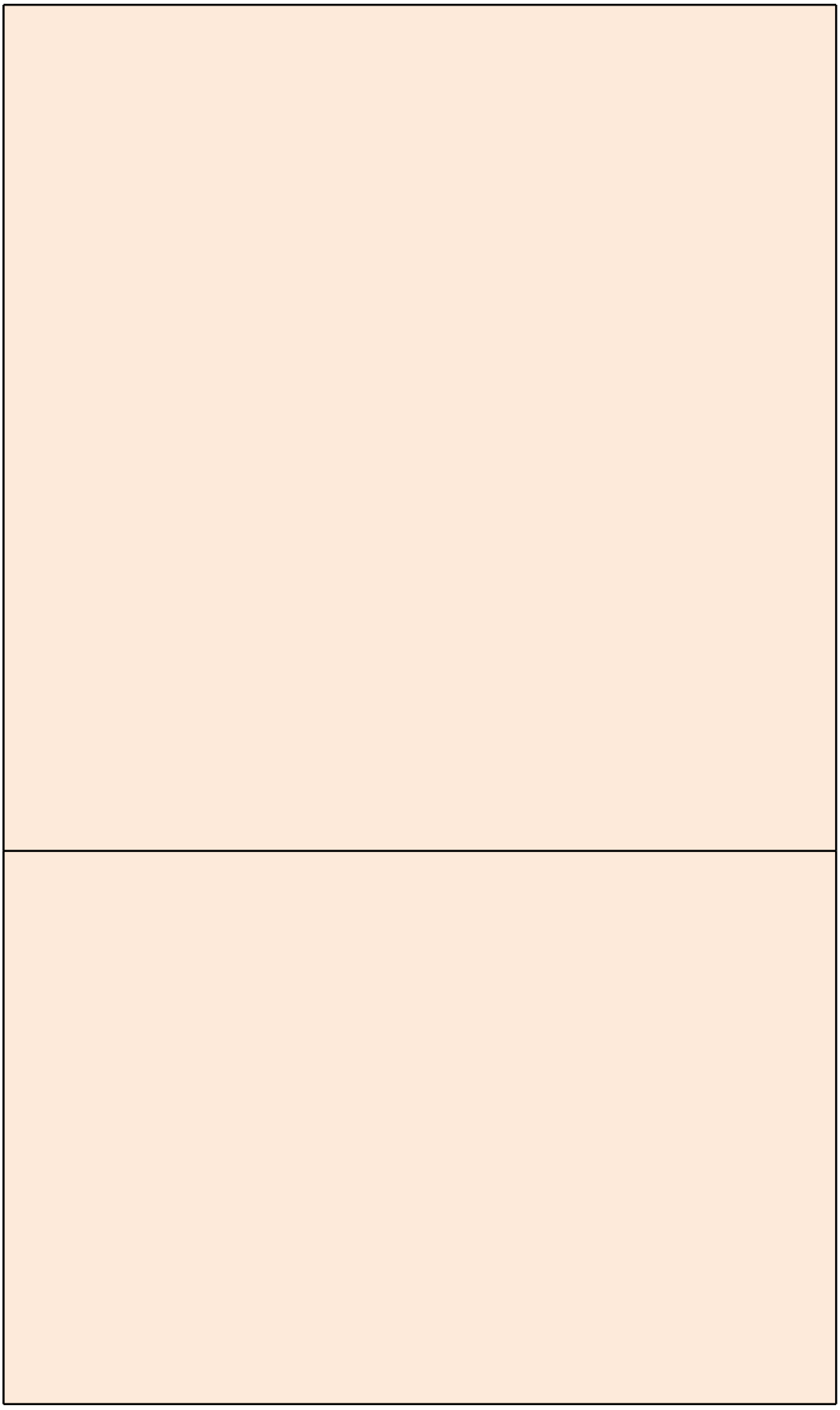


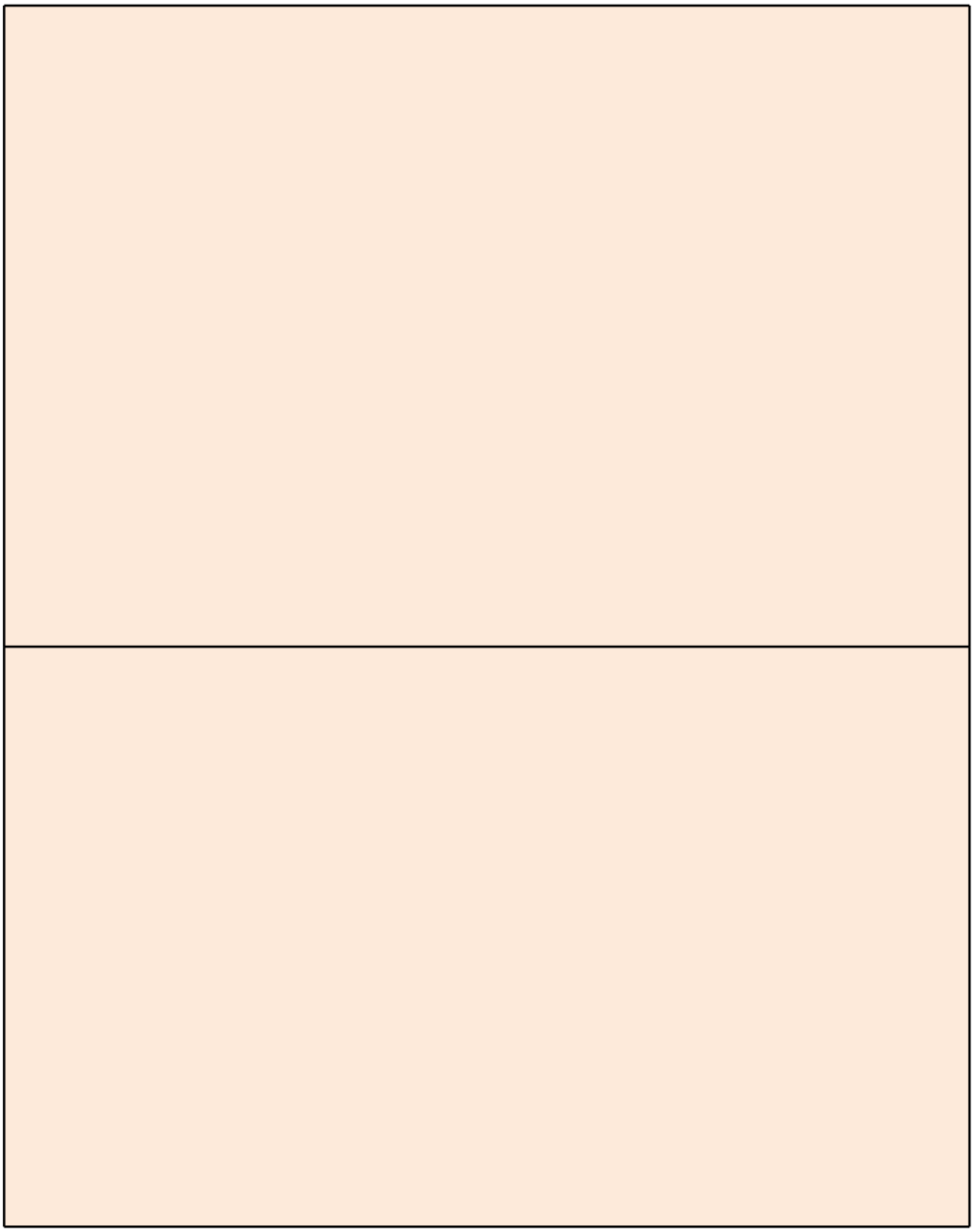


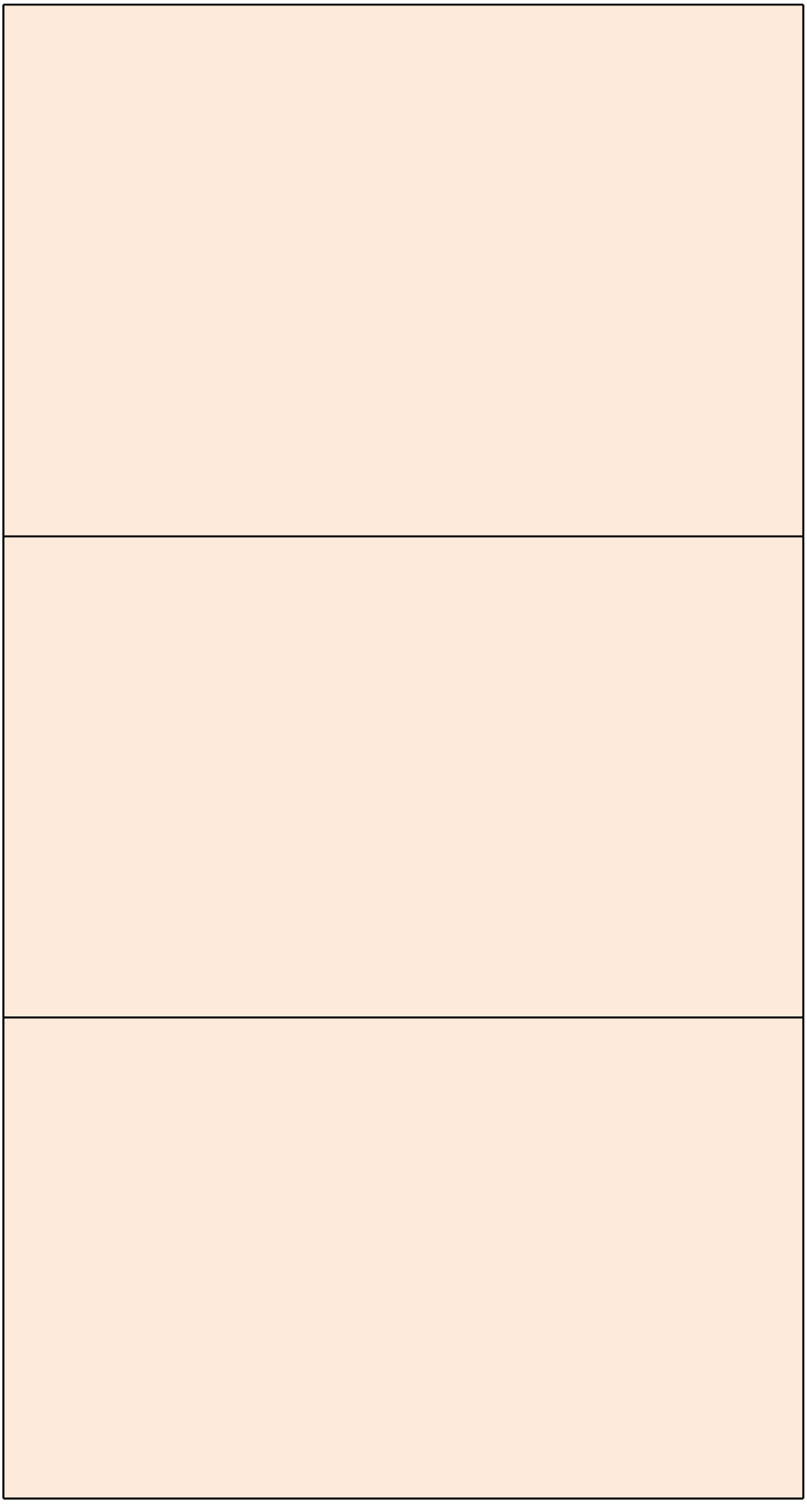


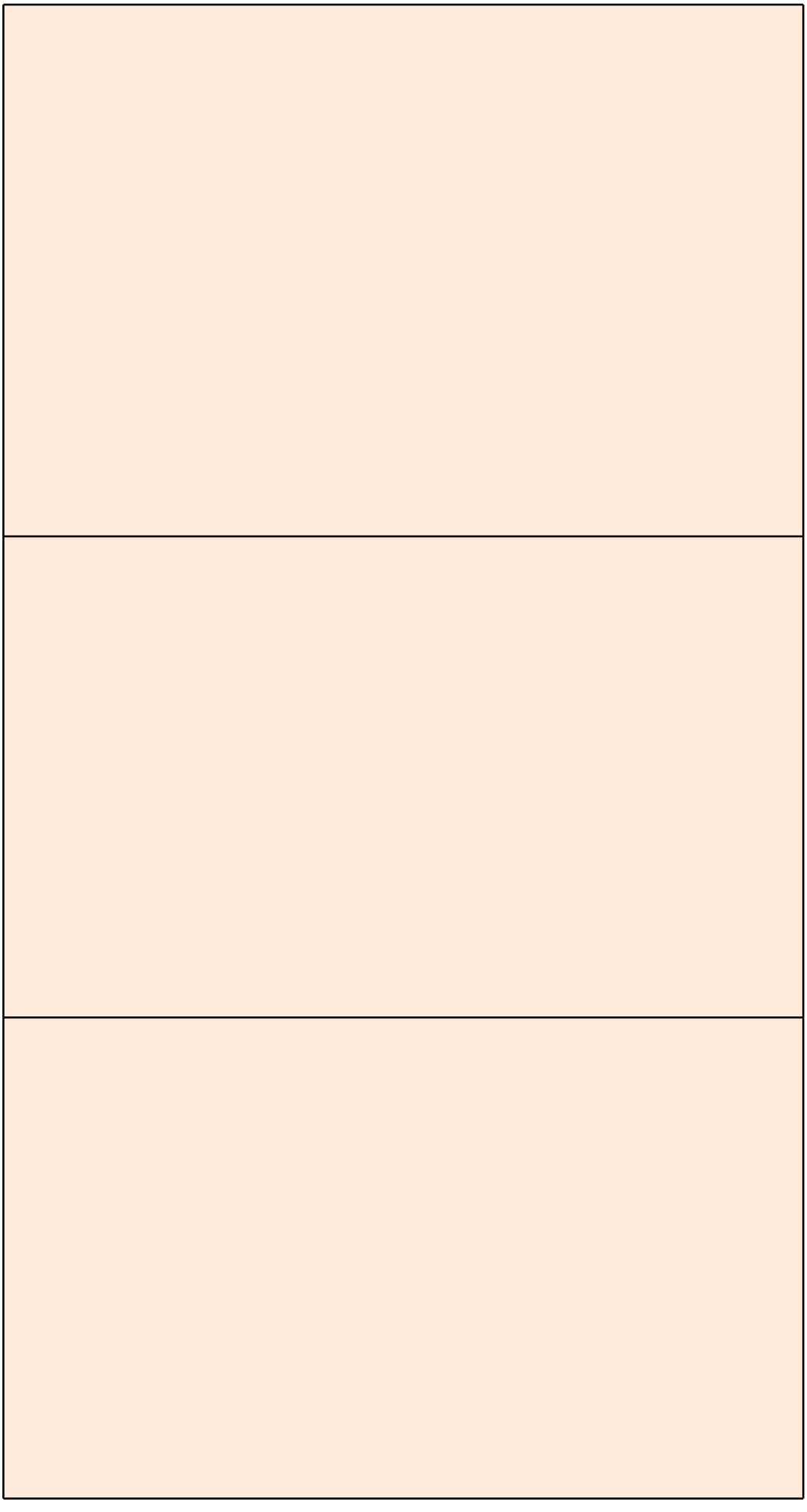


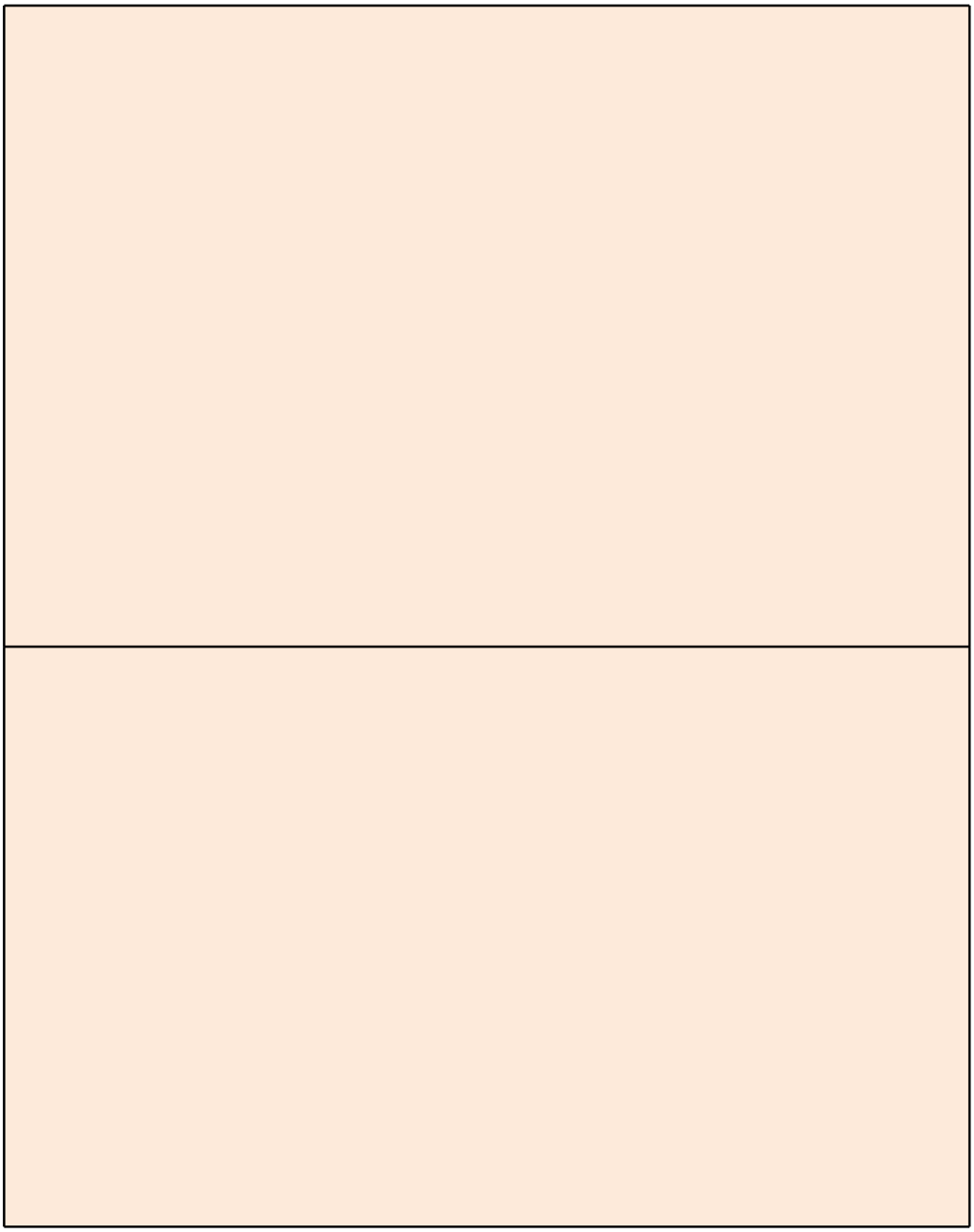


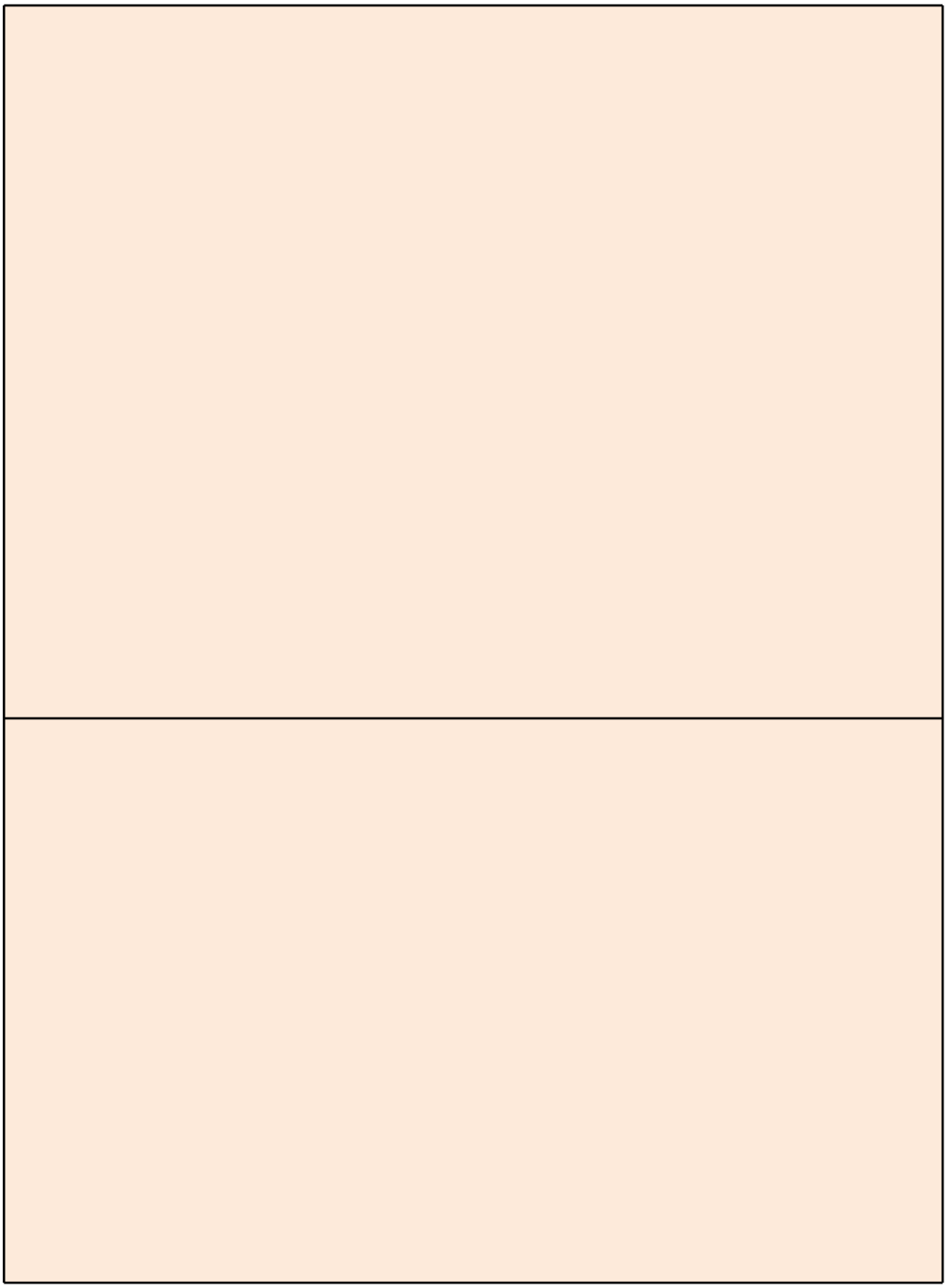


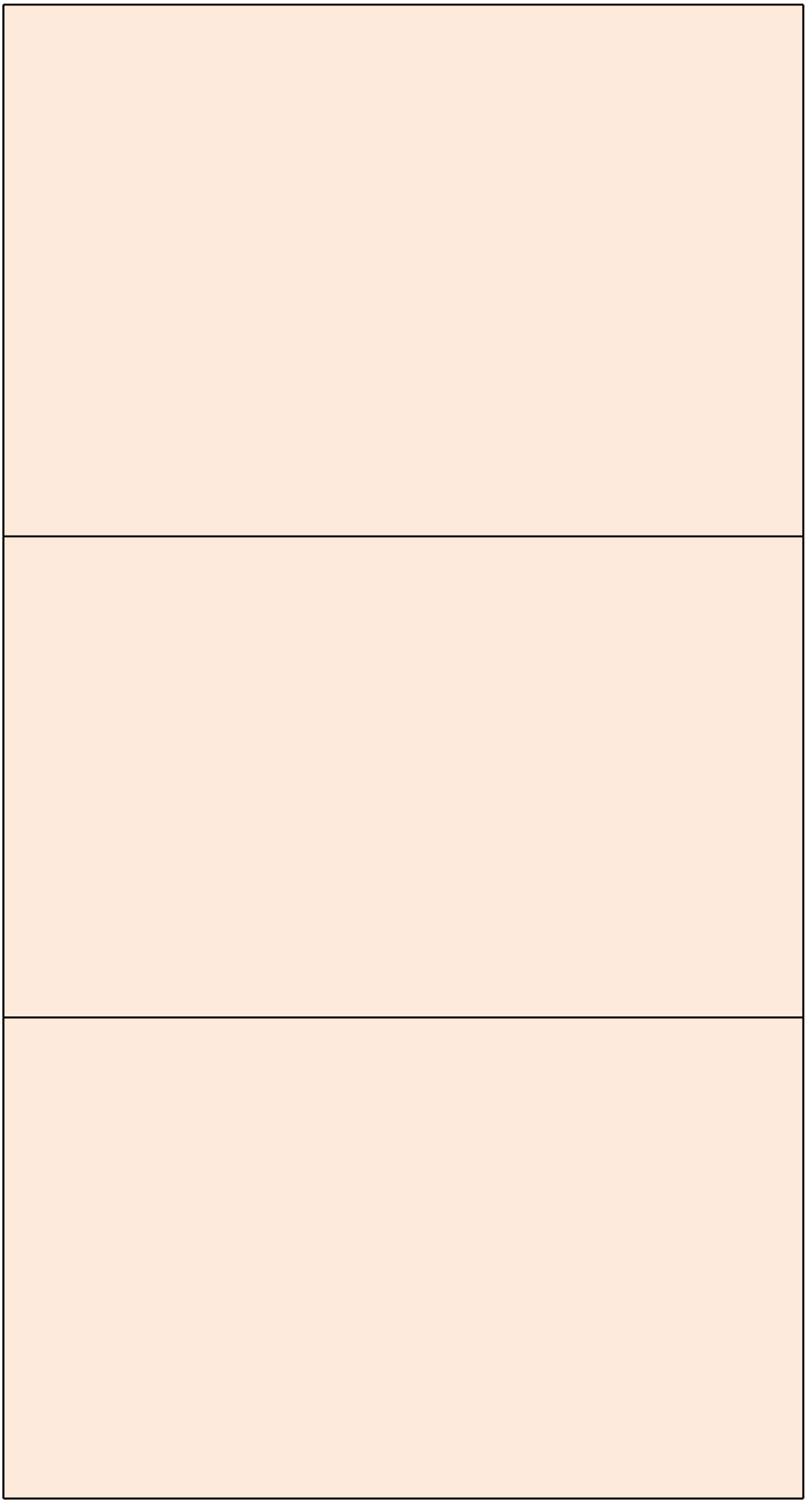


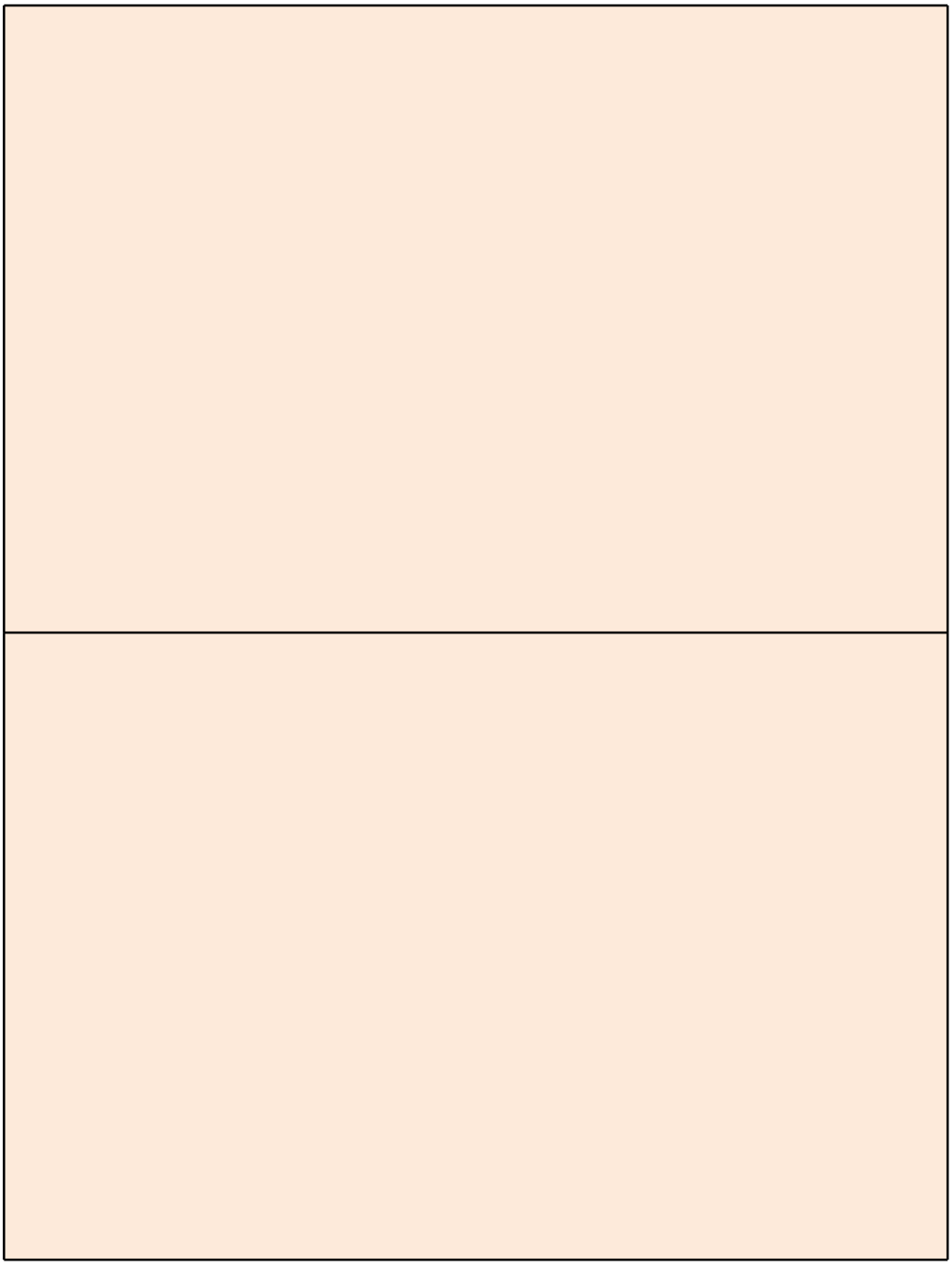


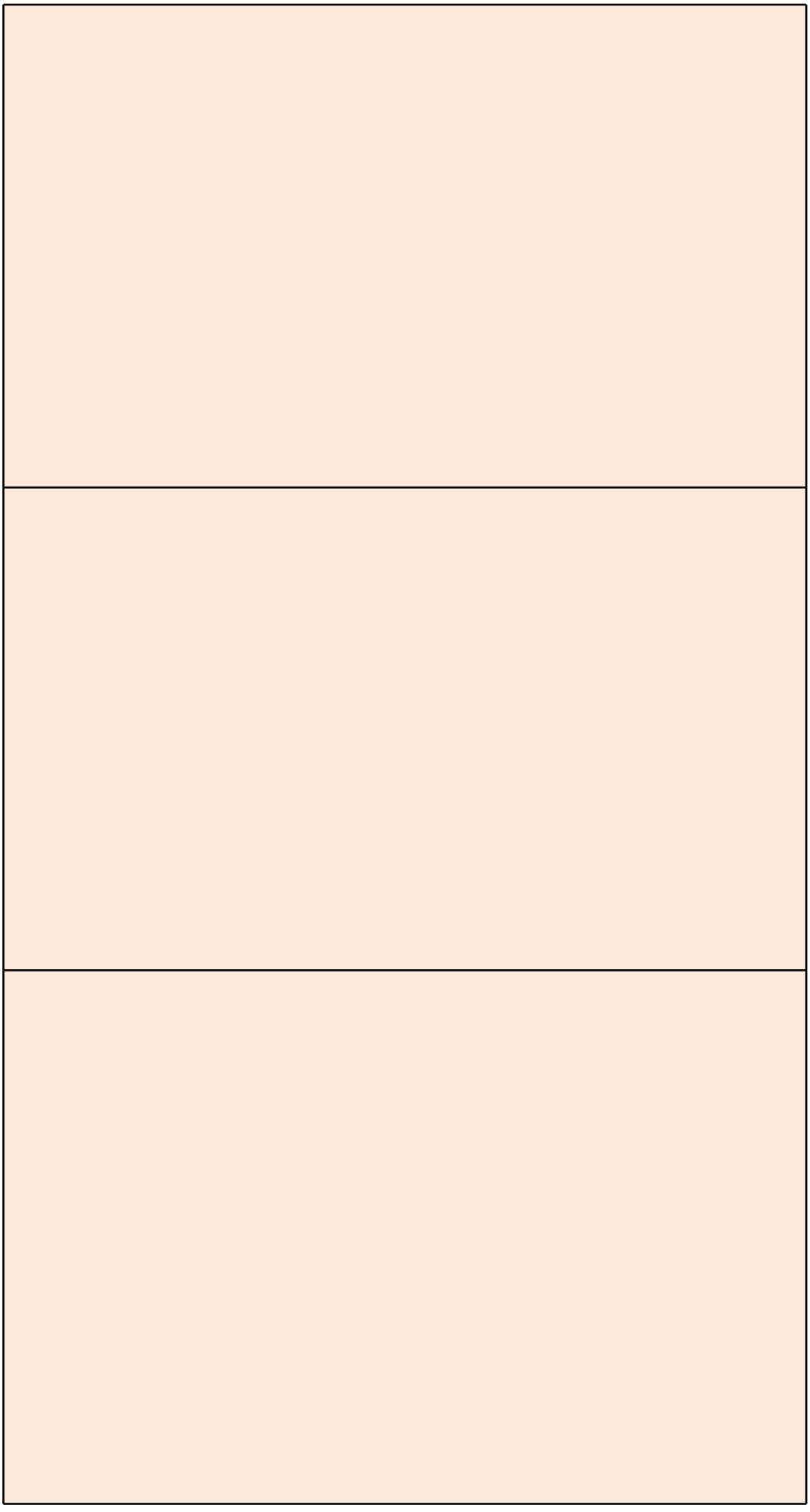


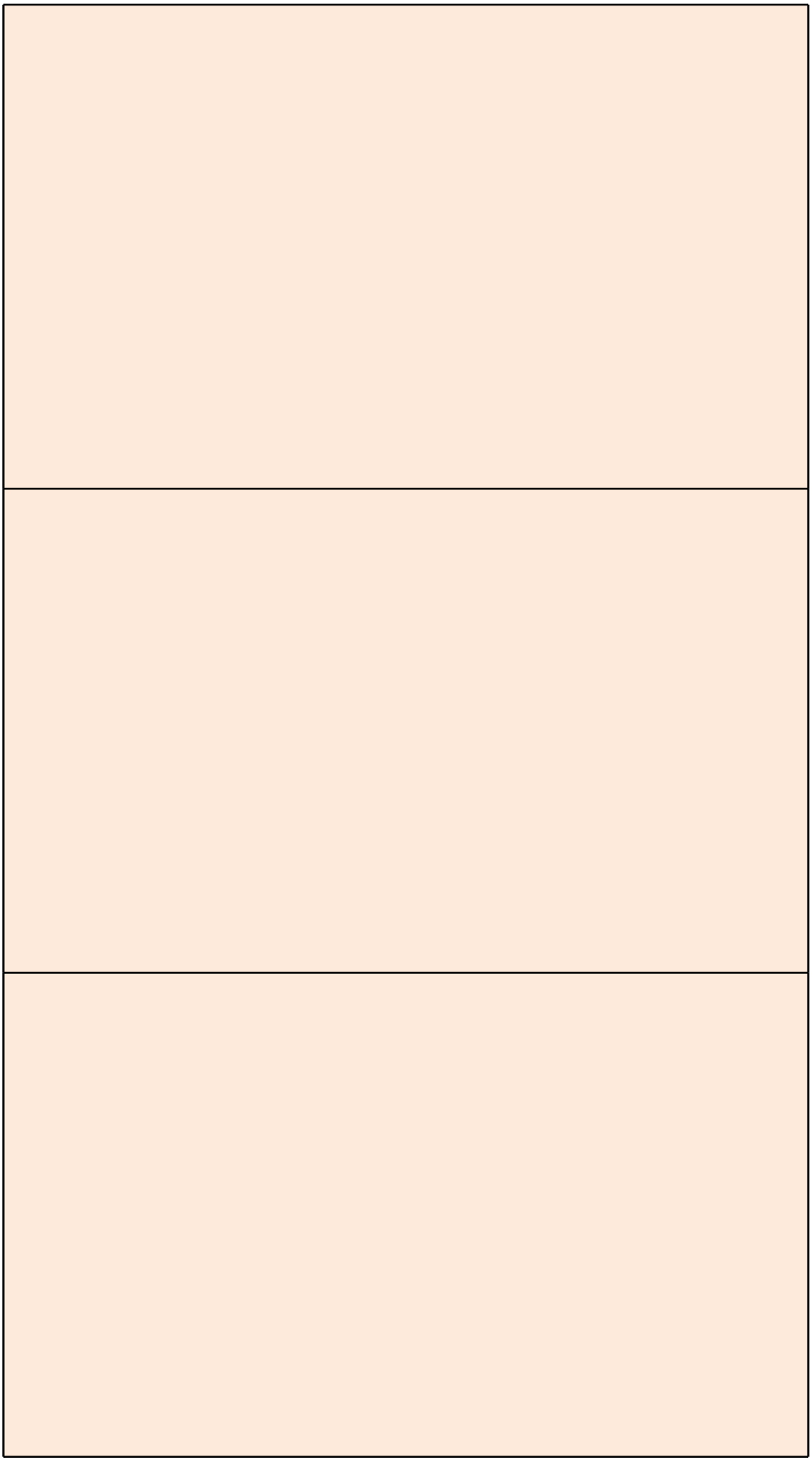




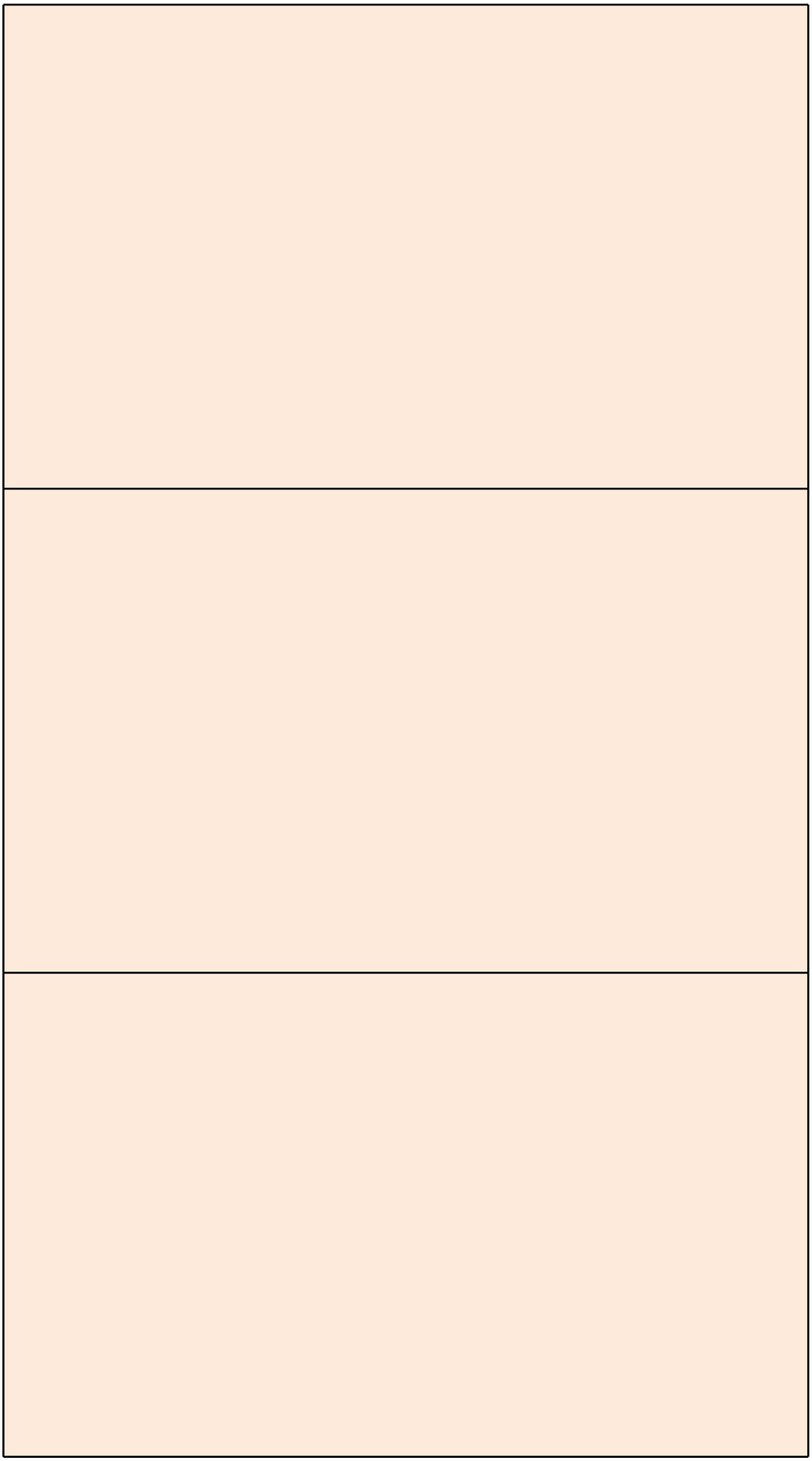


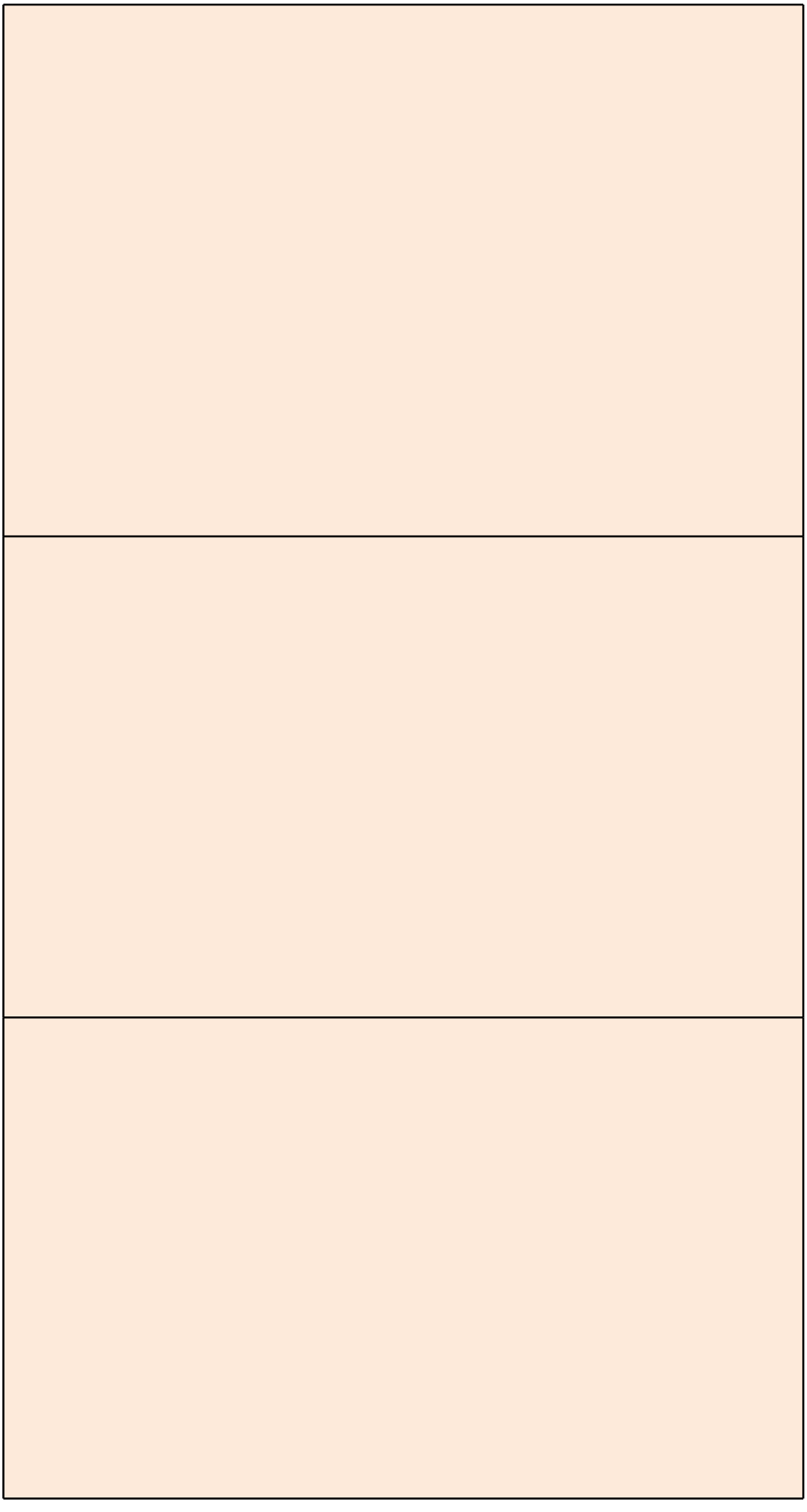


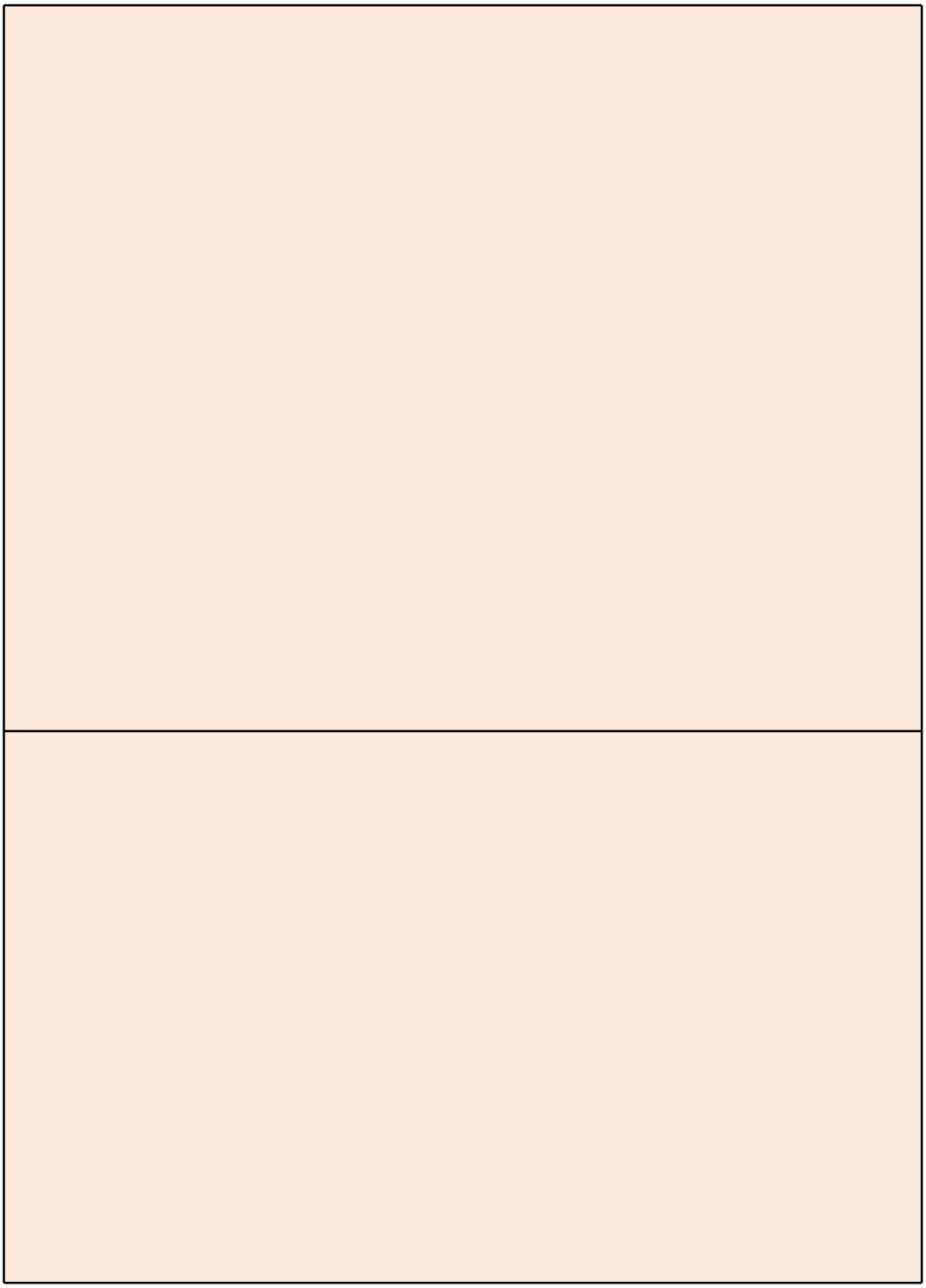


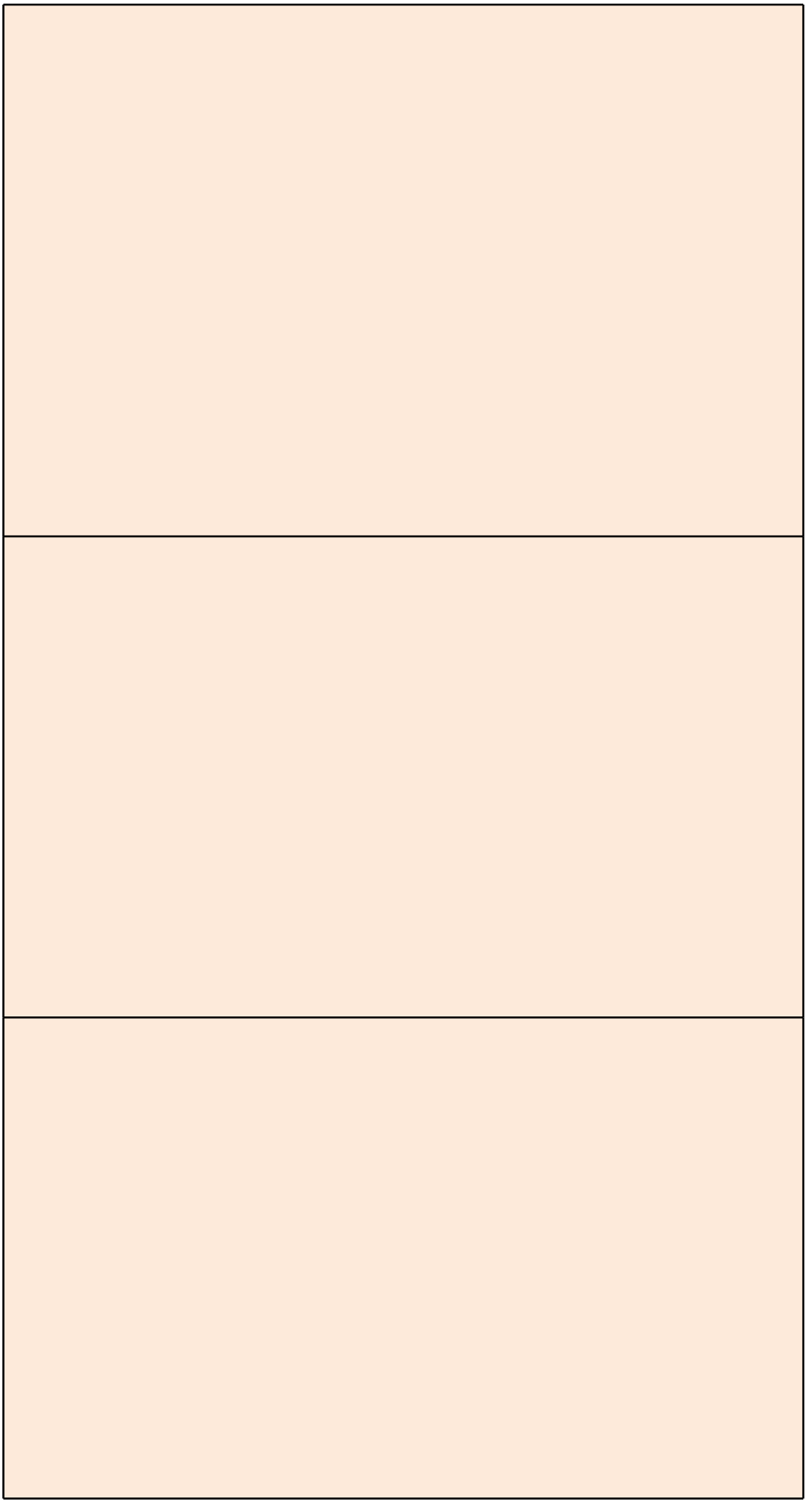


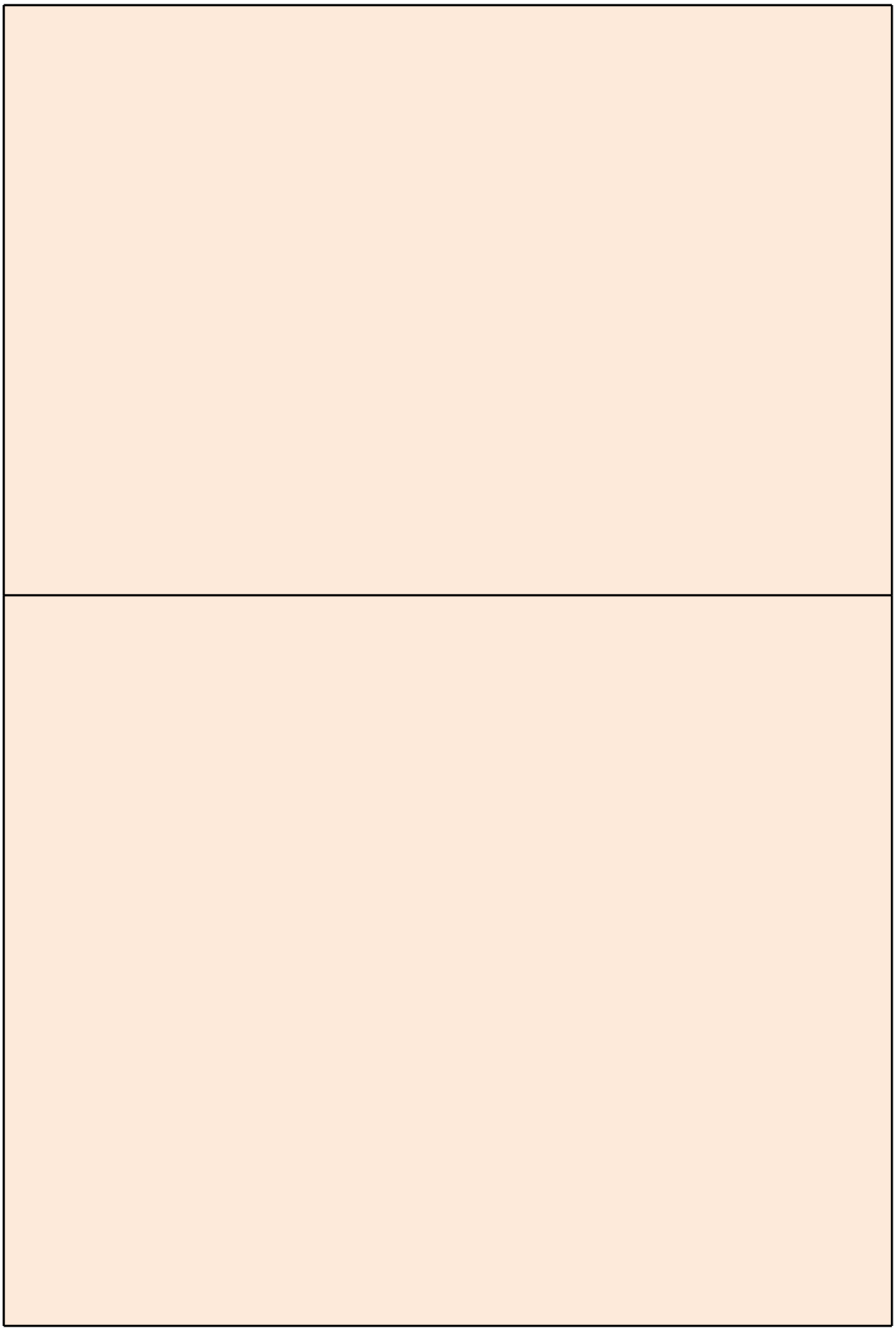
6) turvallisuustarkastusta ei edellytetä uhka- ja hätätilanteissa turvahenkilöiltä, poliisilta, Rajavartiolaitokselta, puolustusvoimilta tai pelastusviranomaiselta.

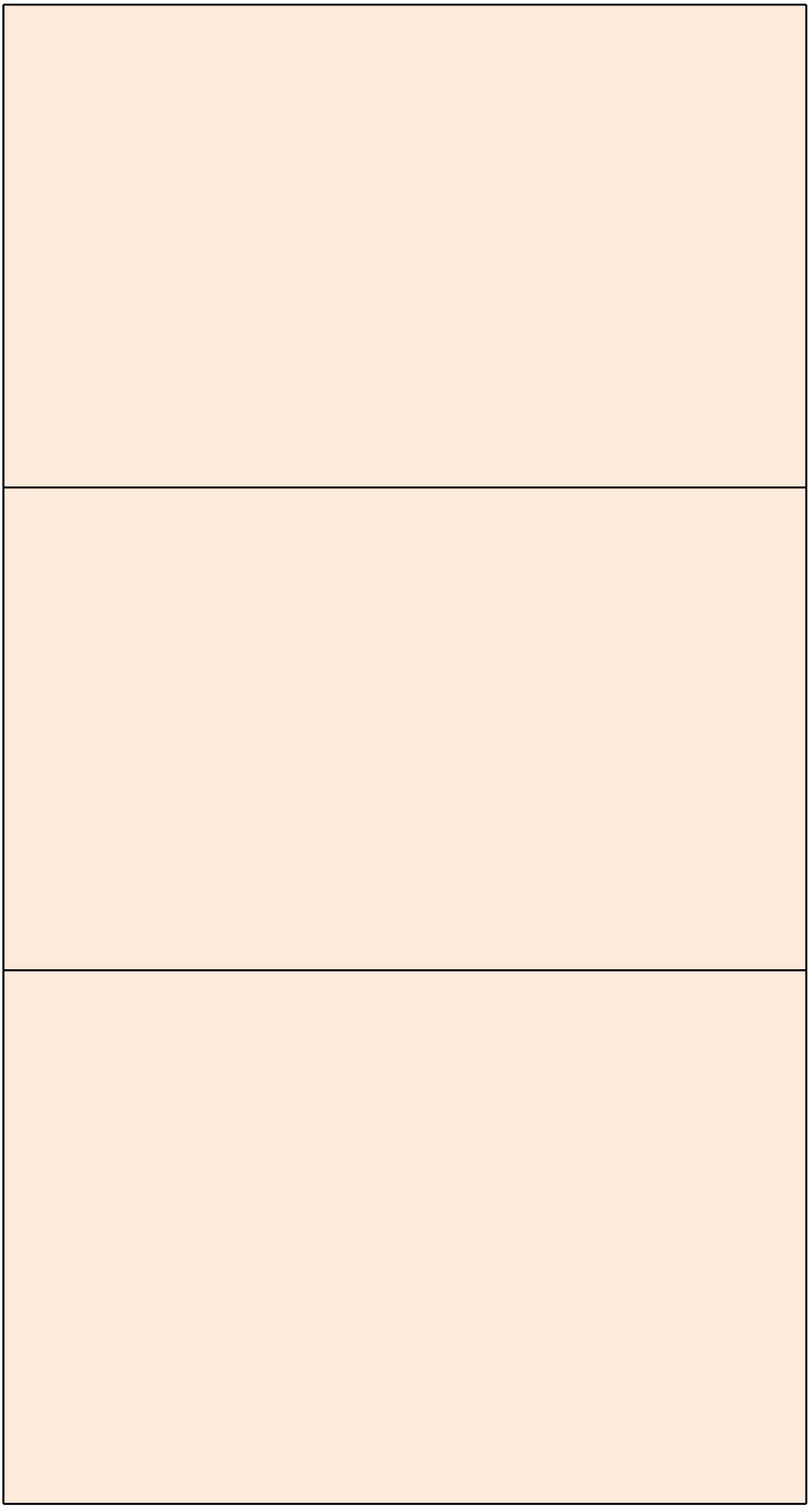


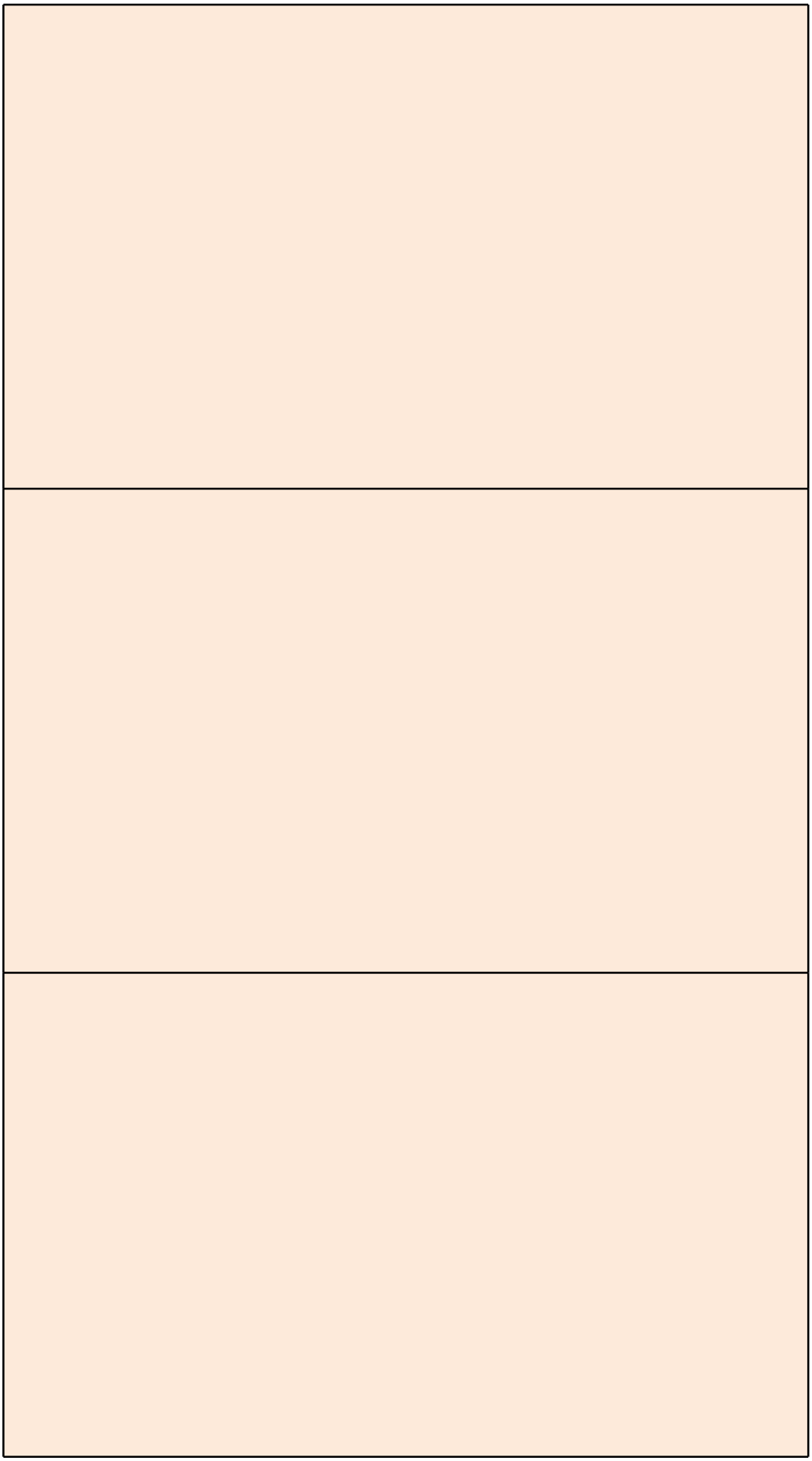


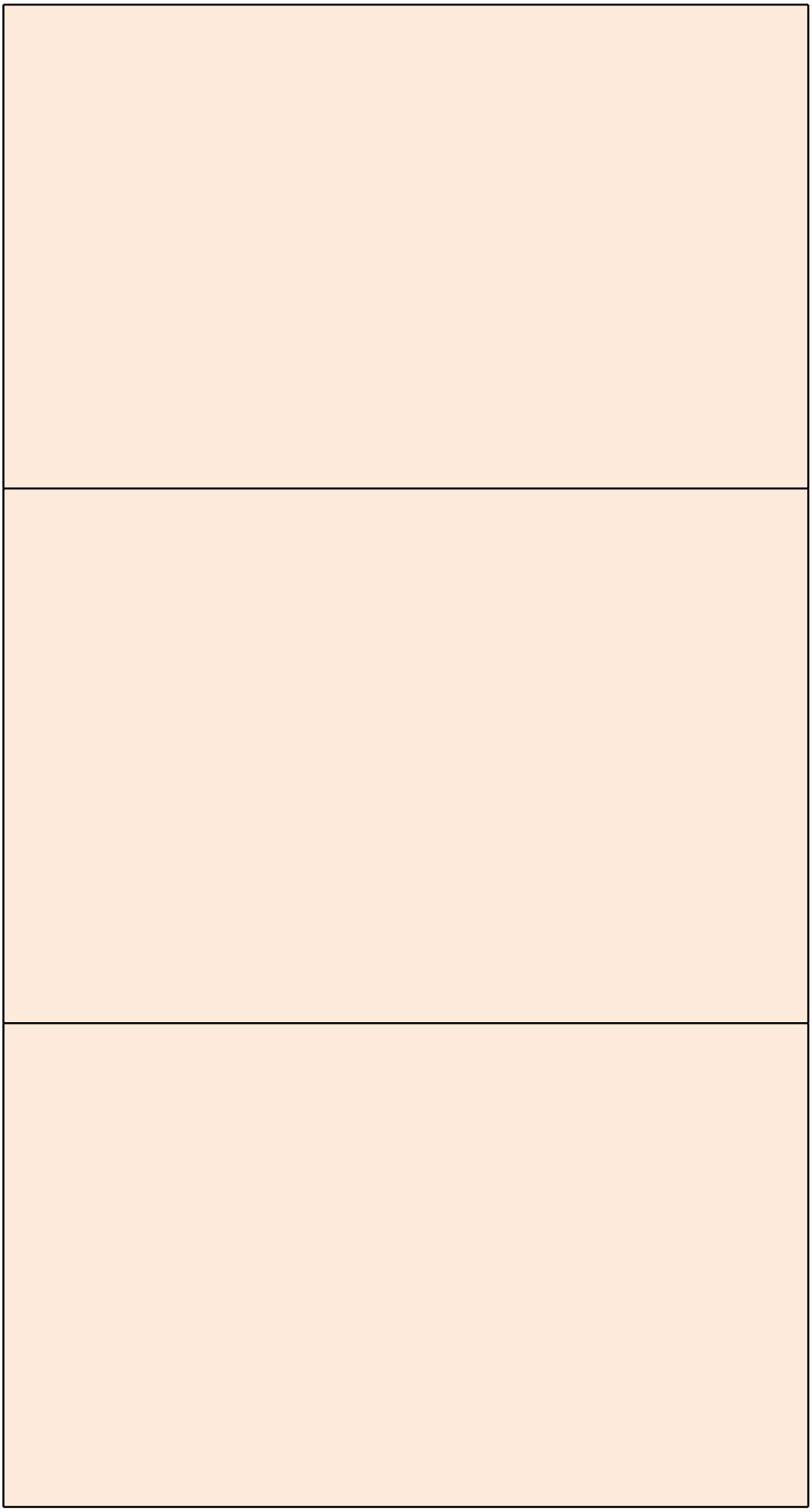


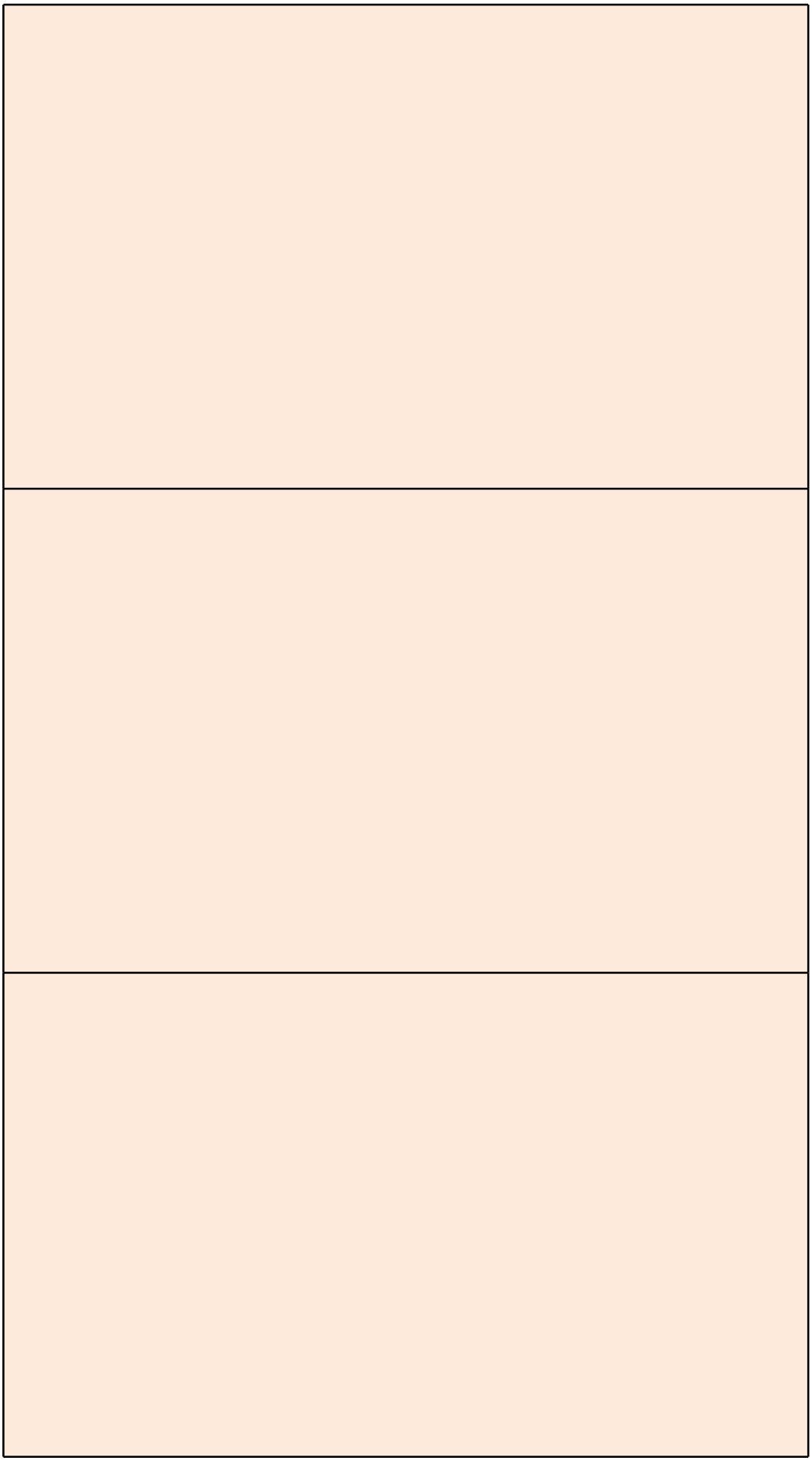


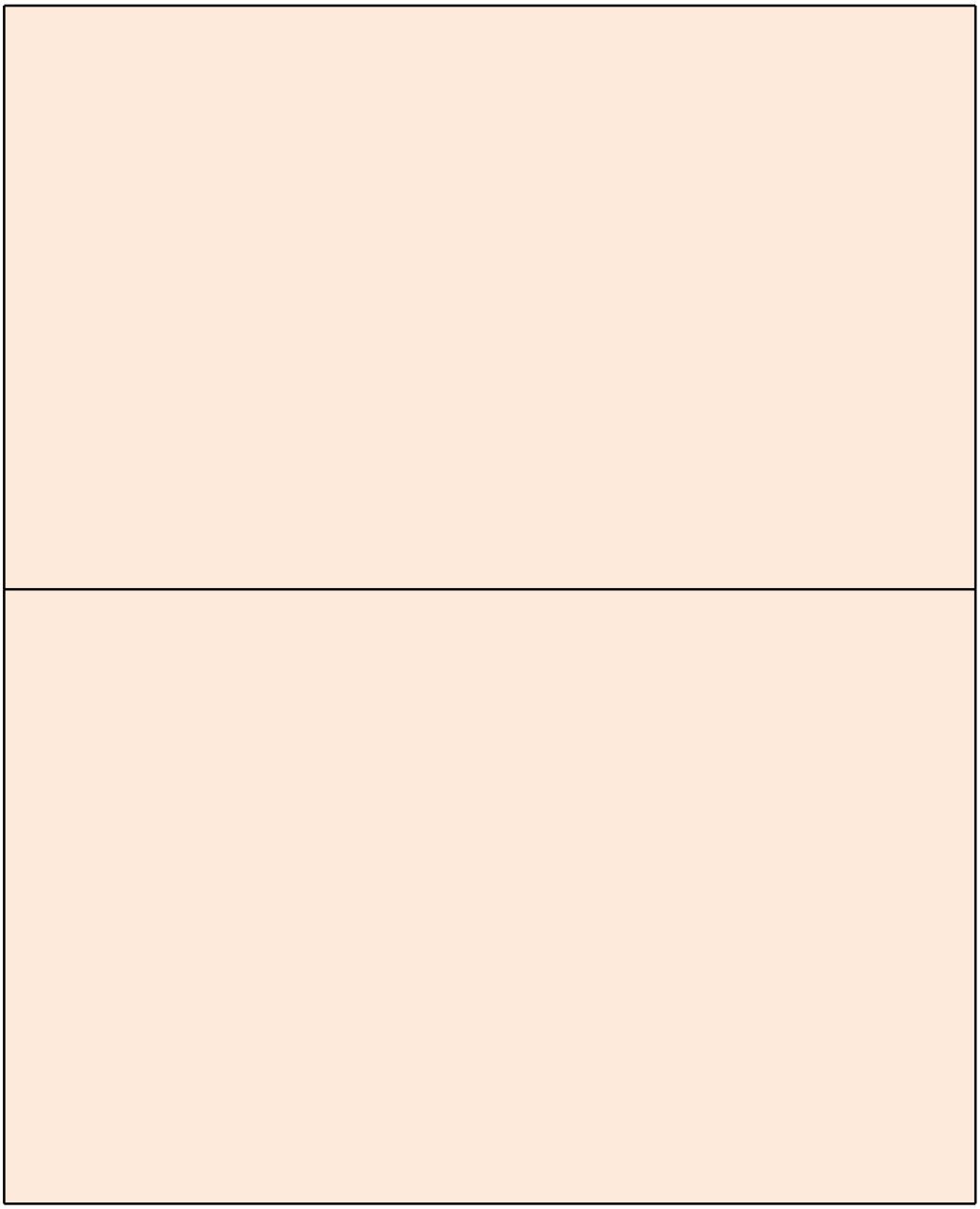


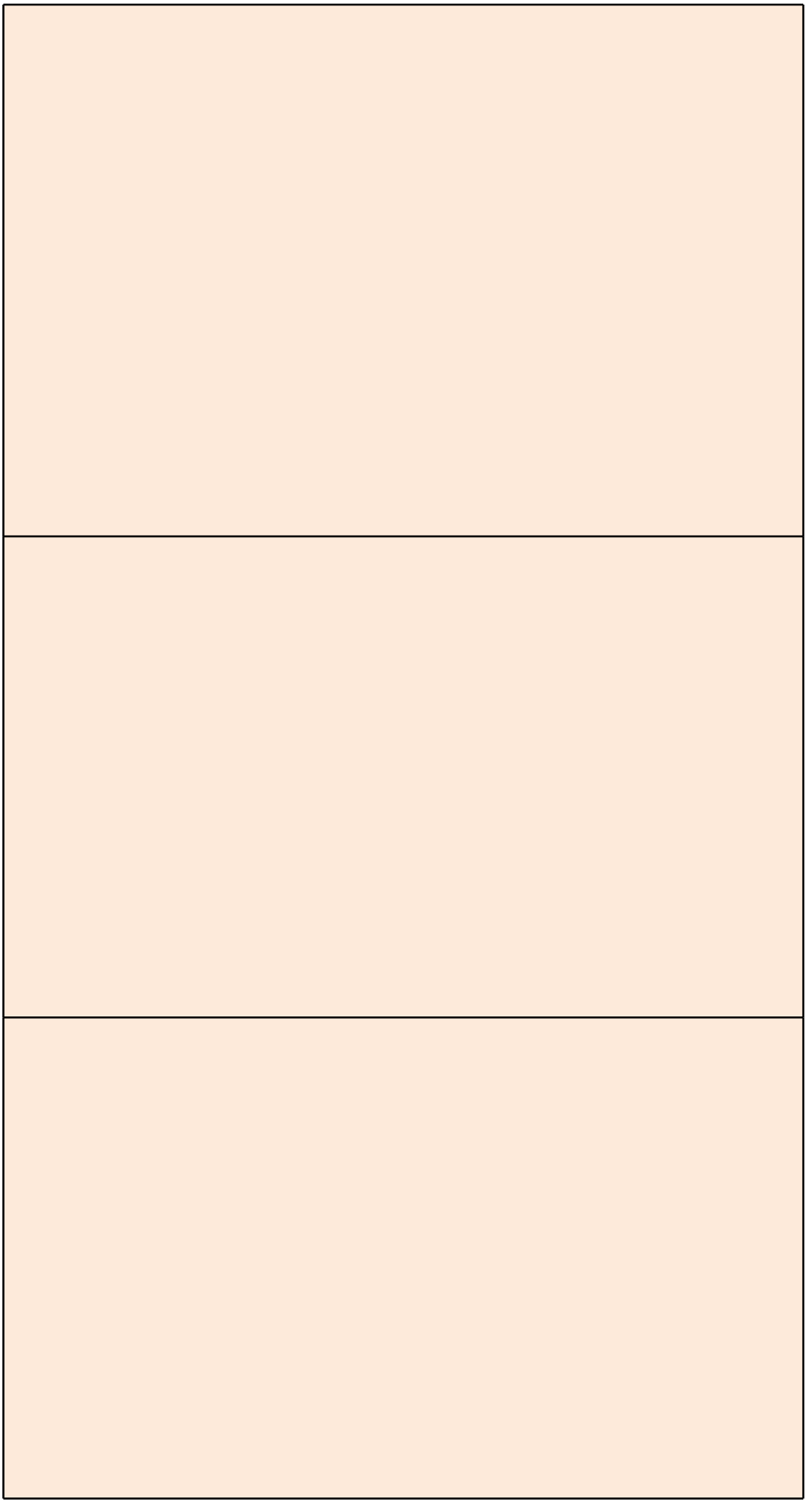


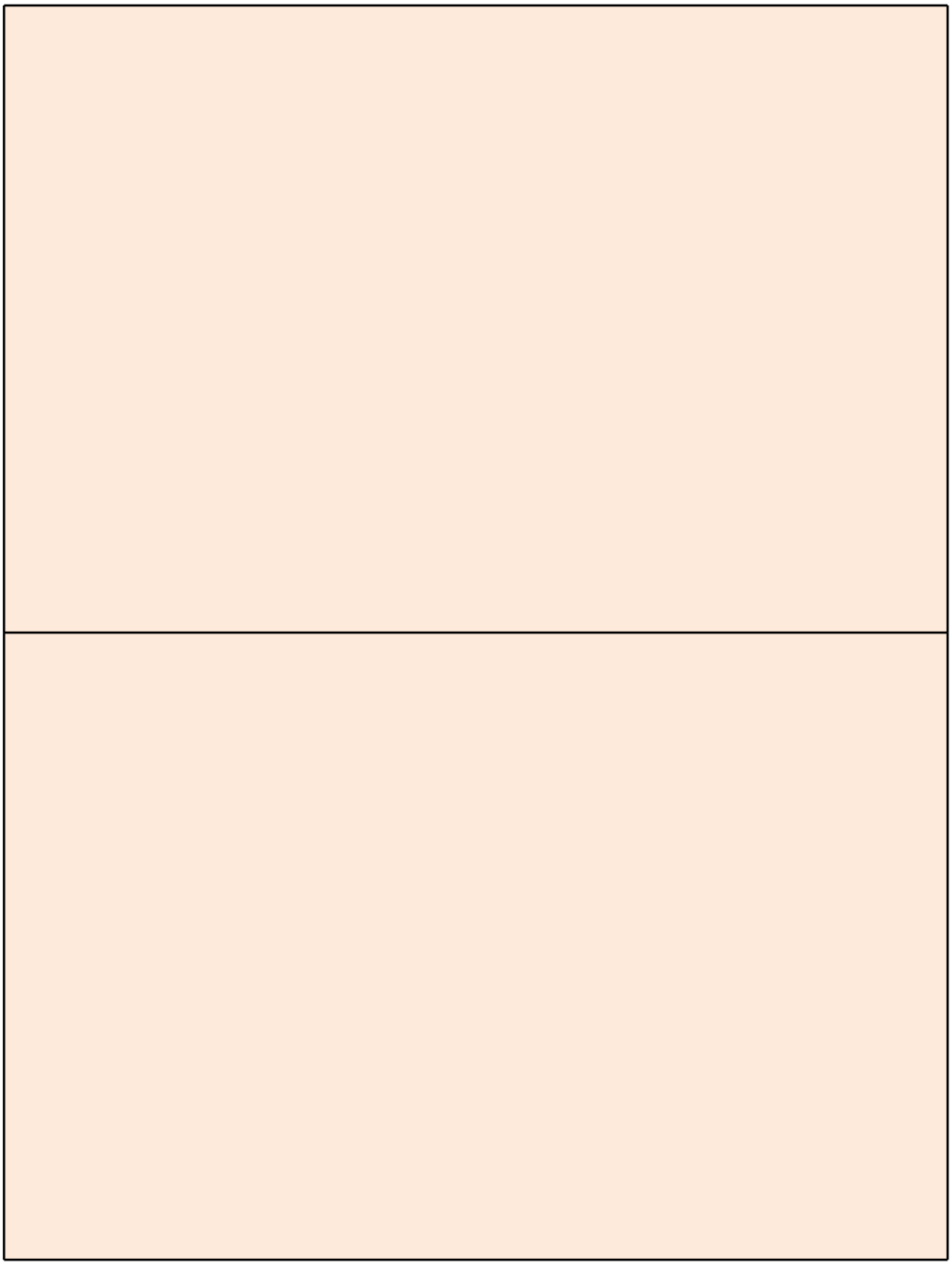


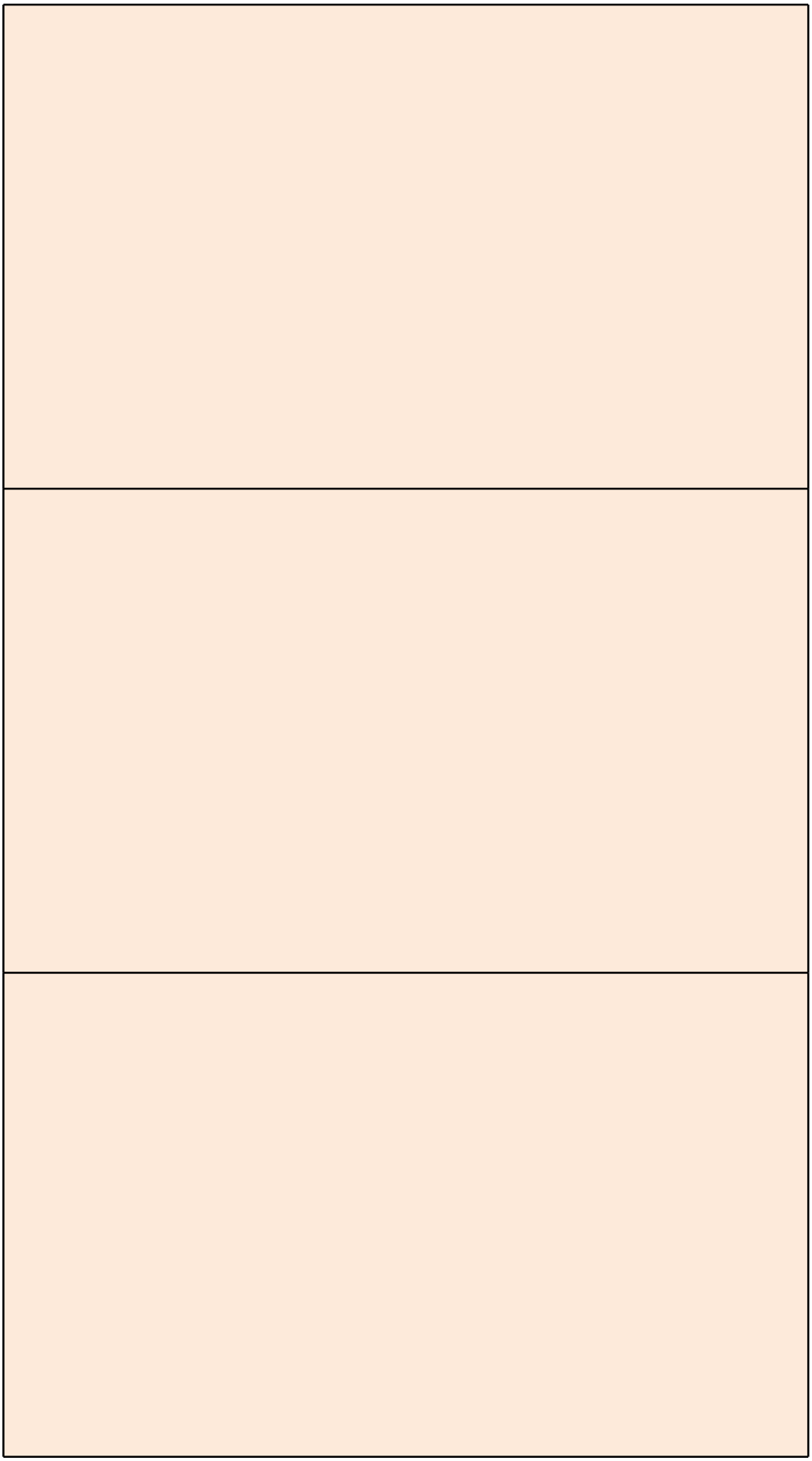


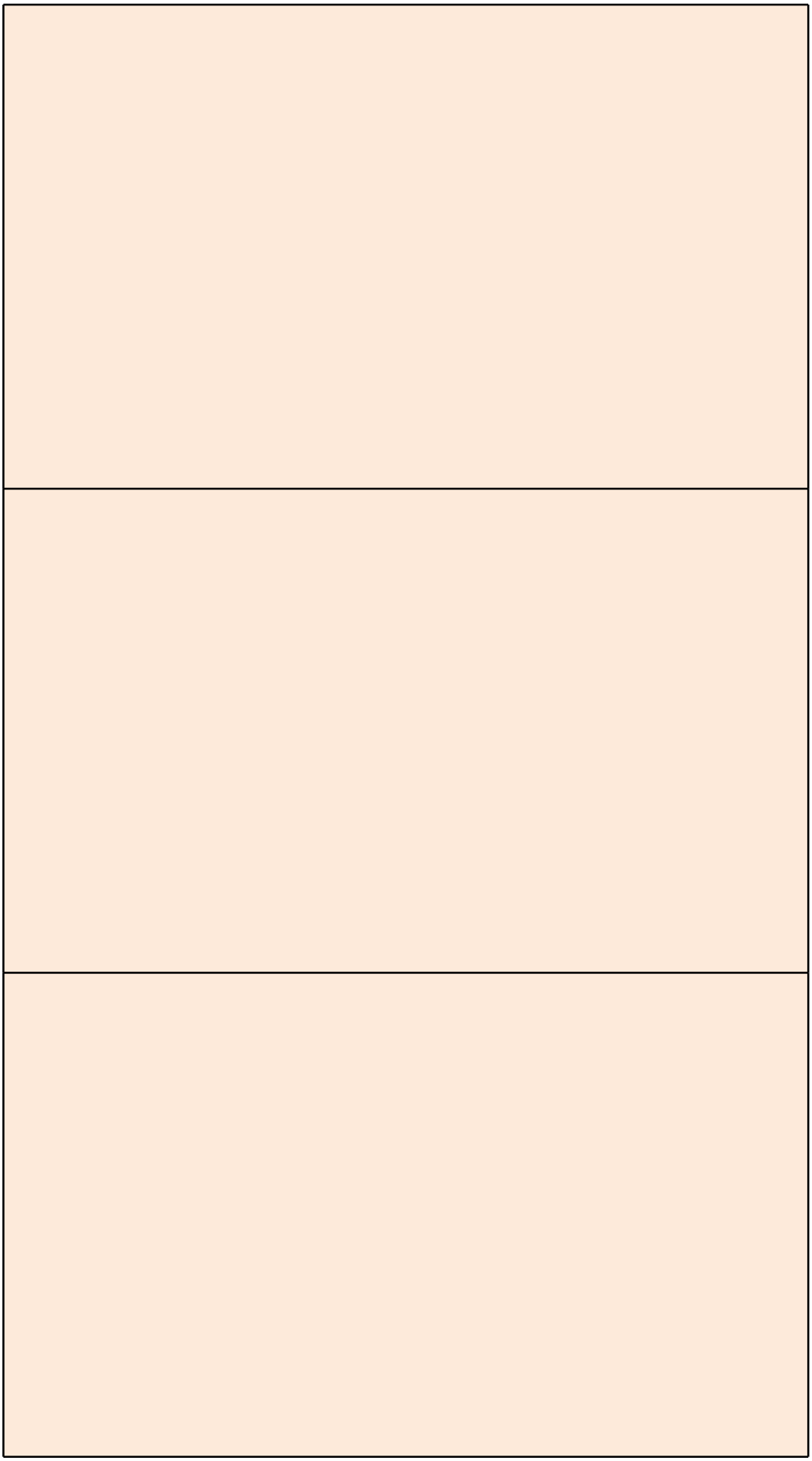


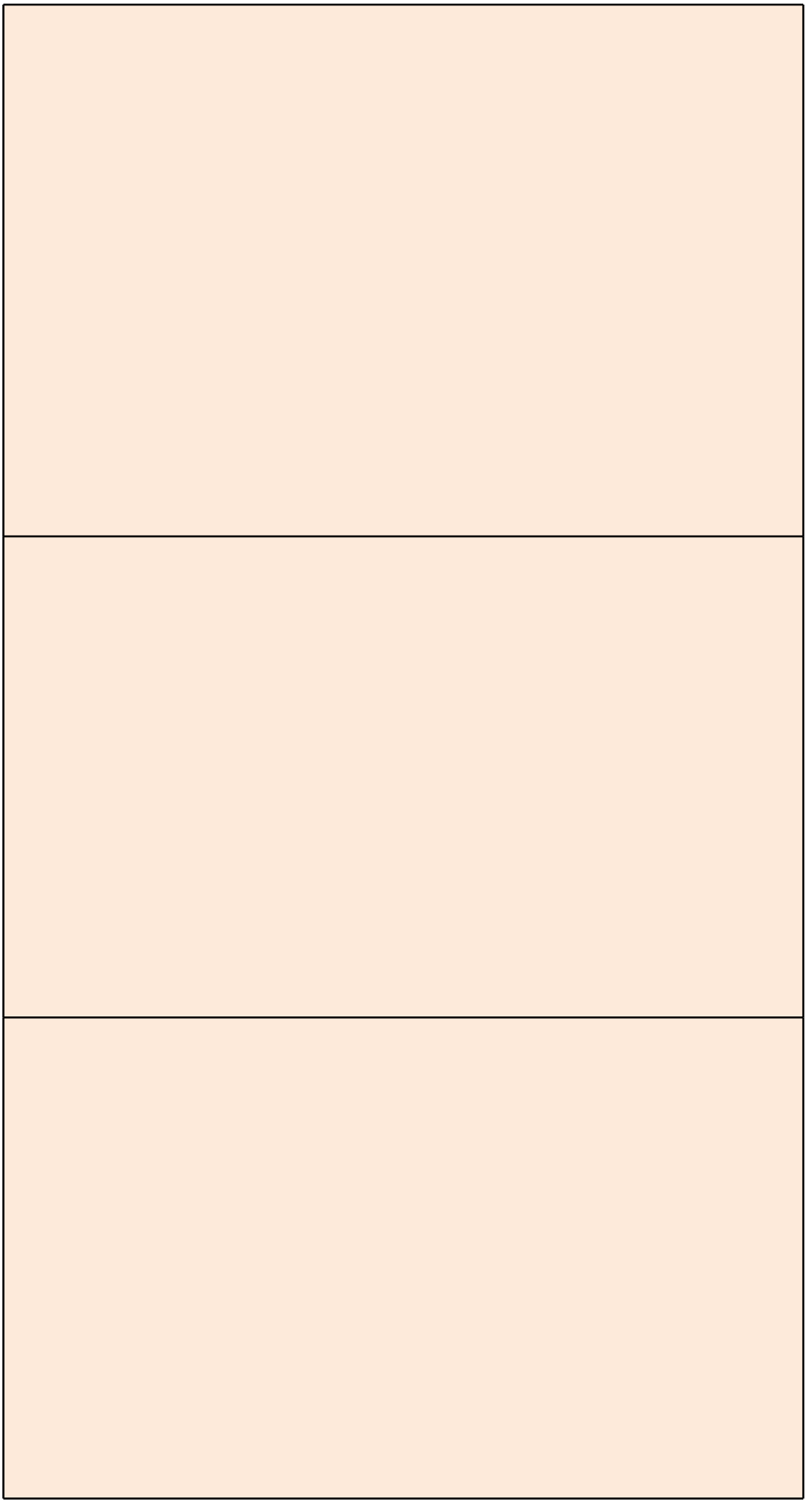


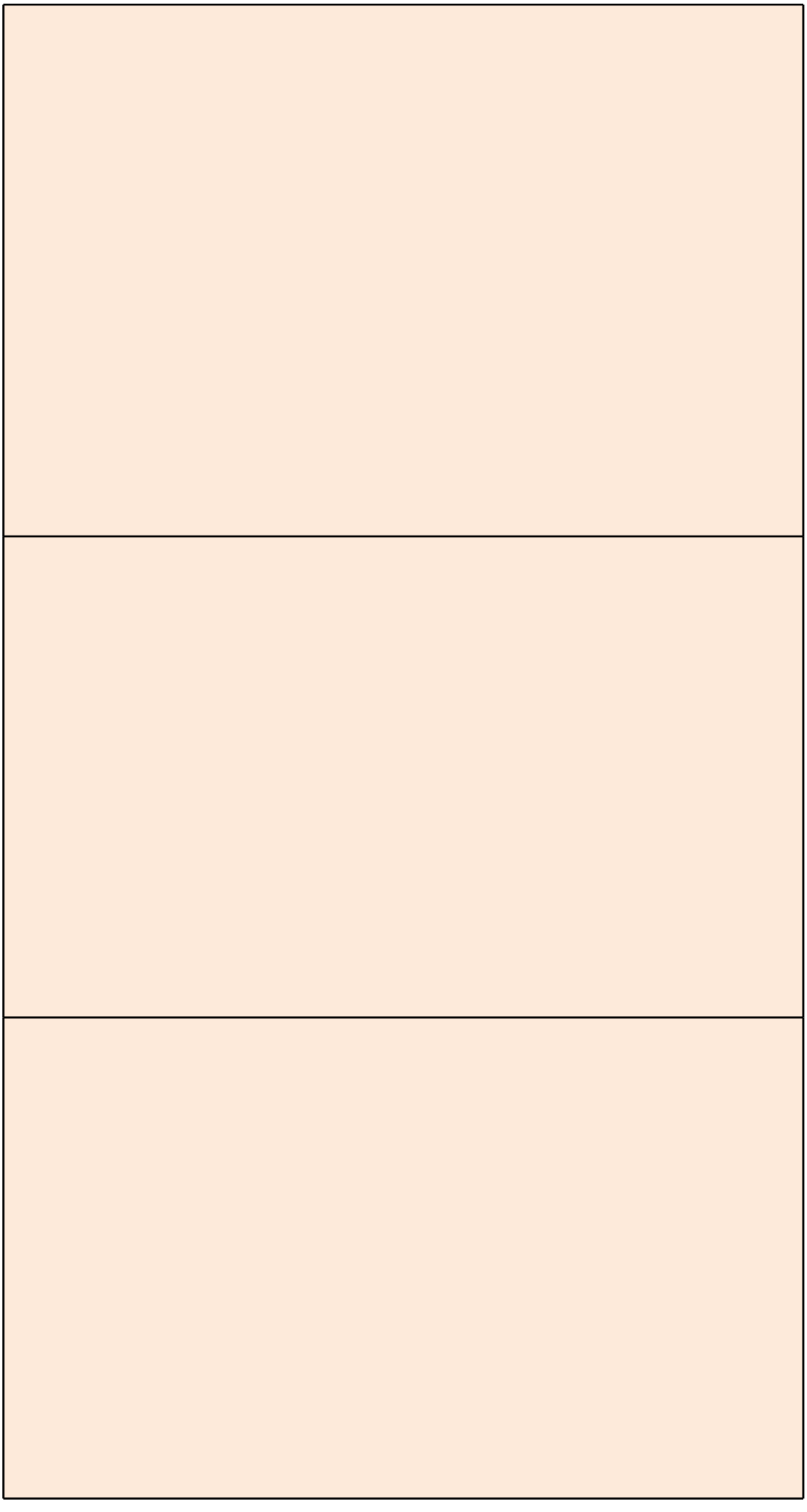


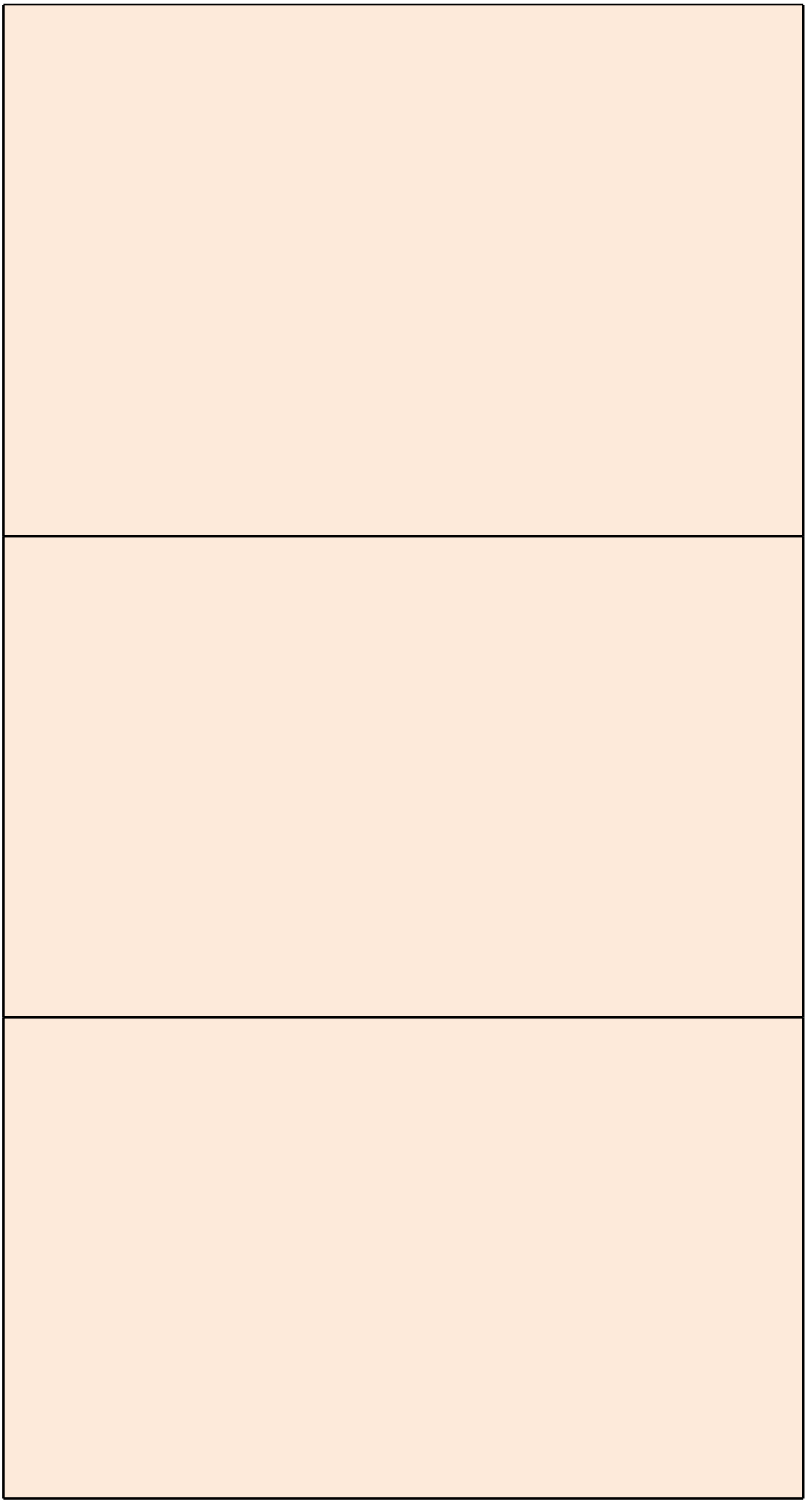


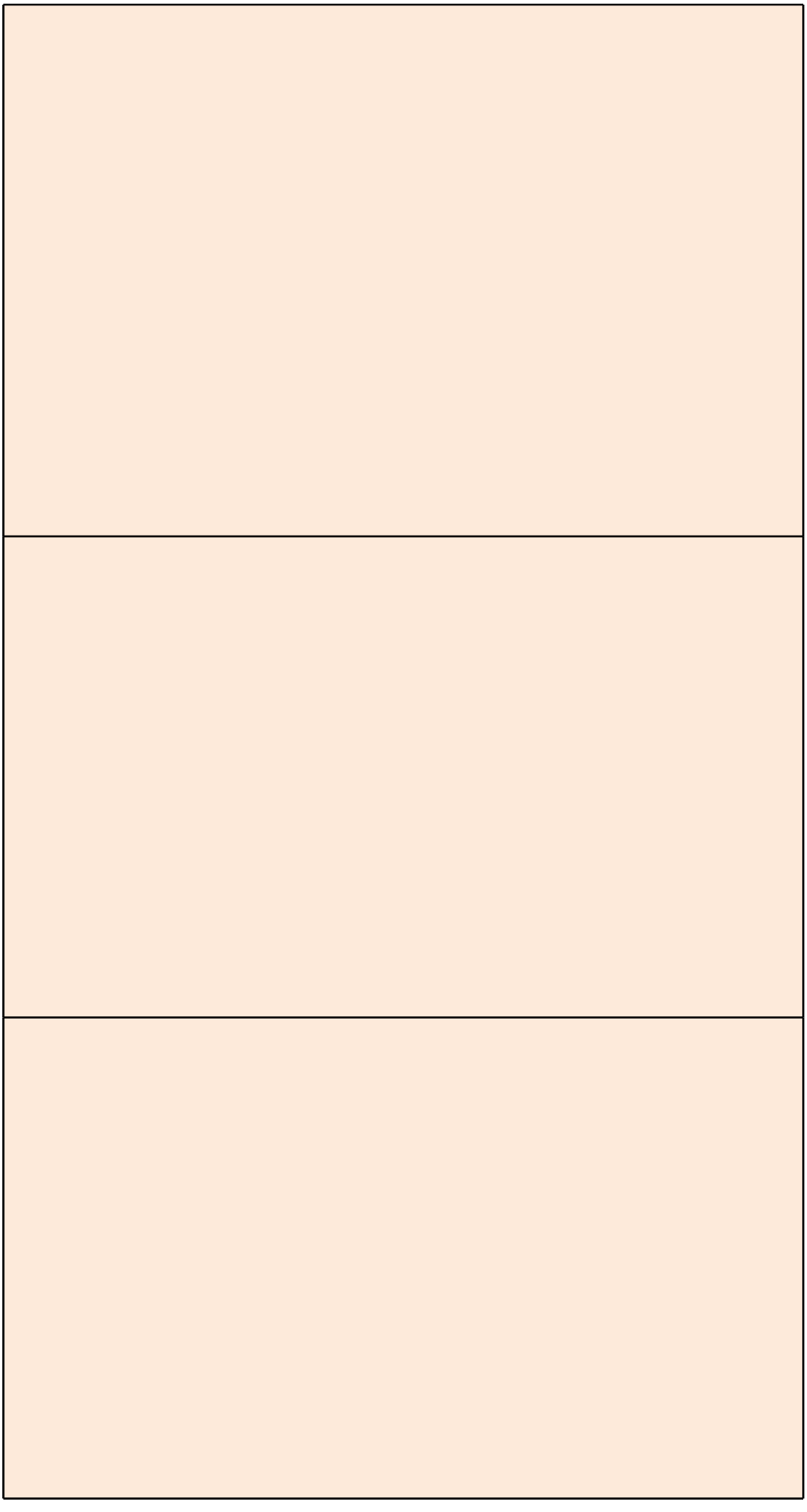


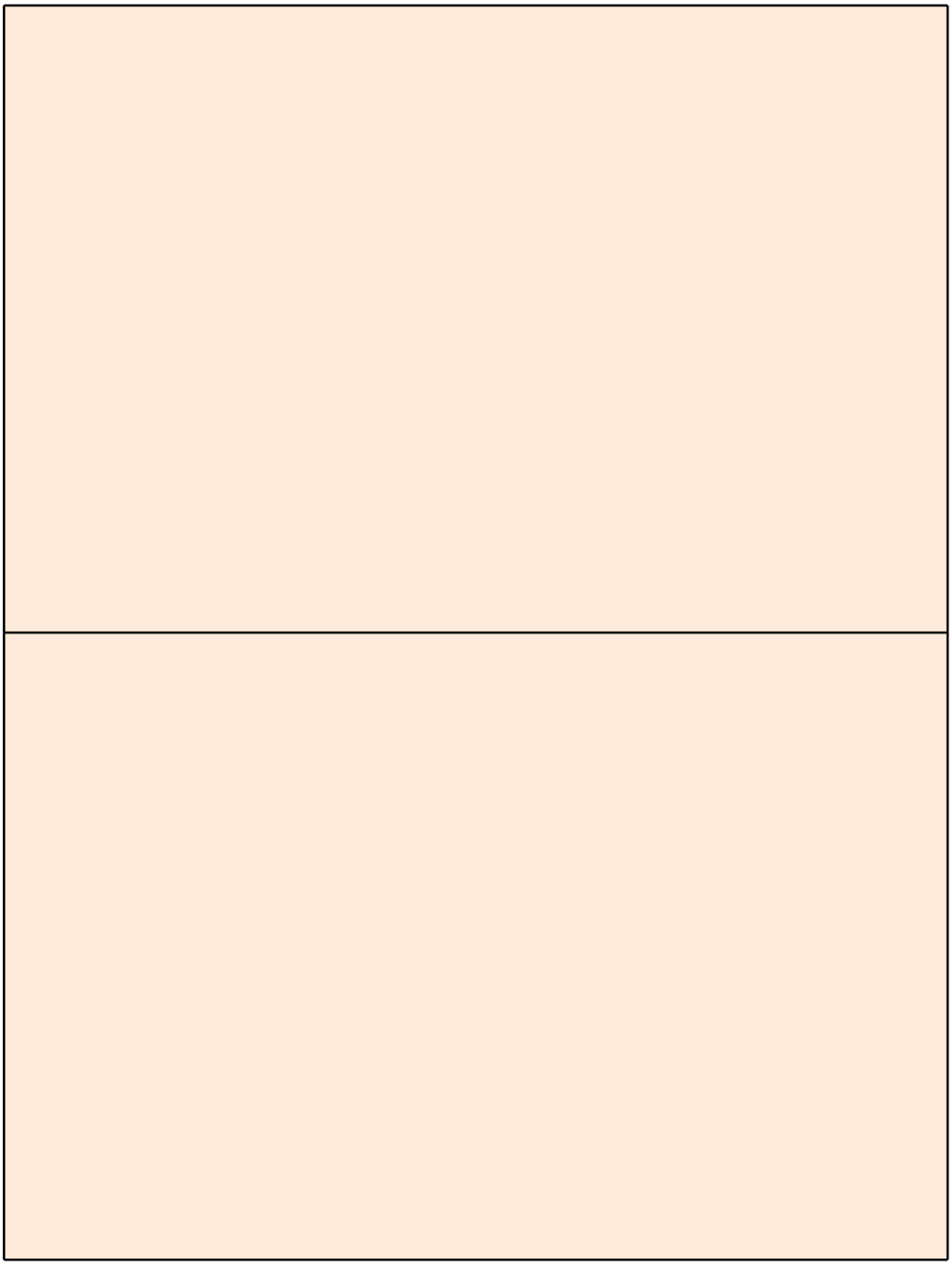


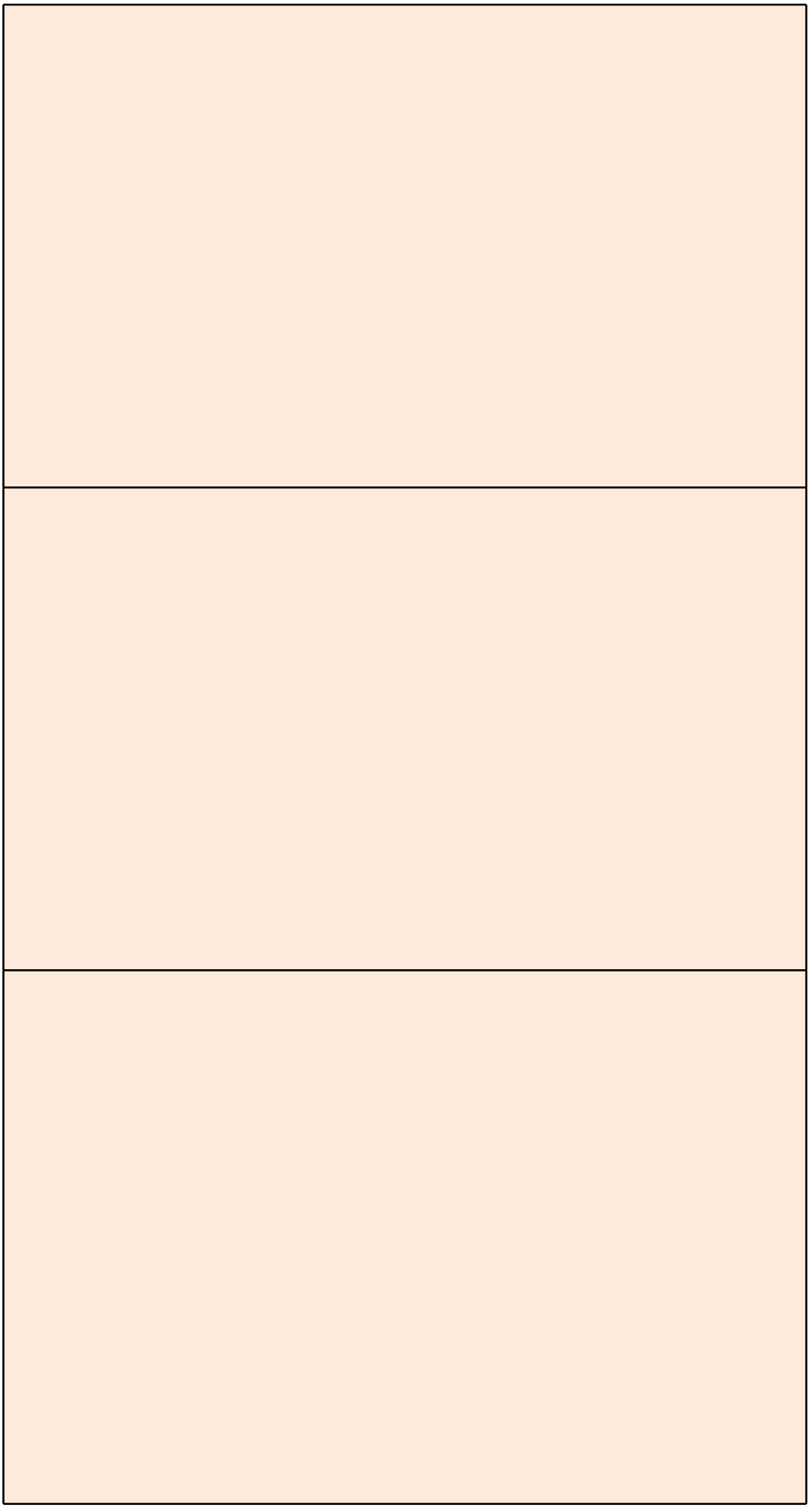


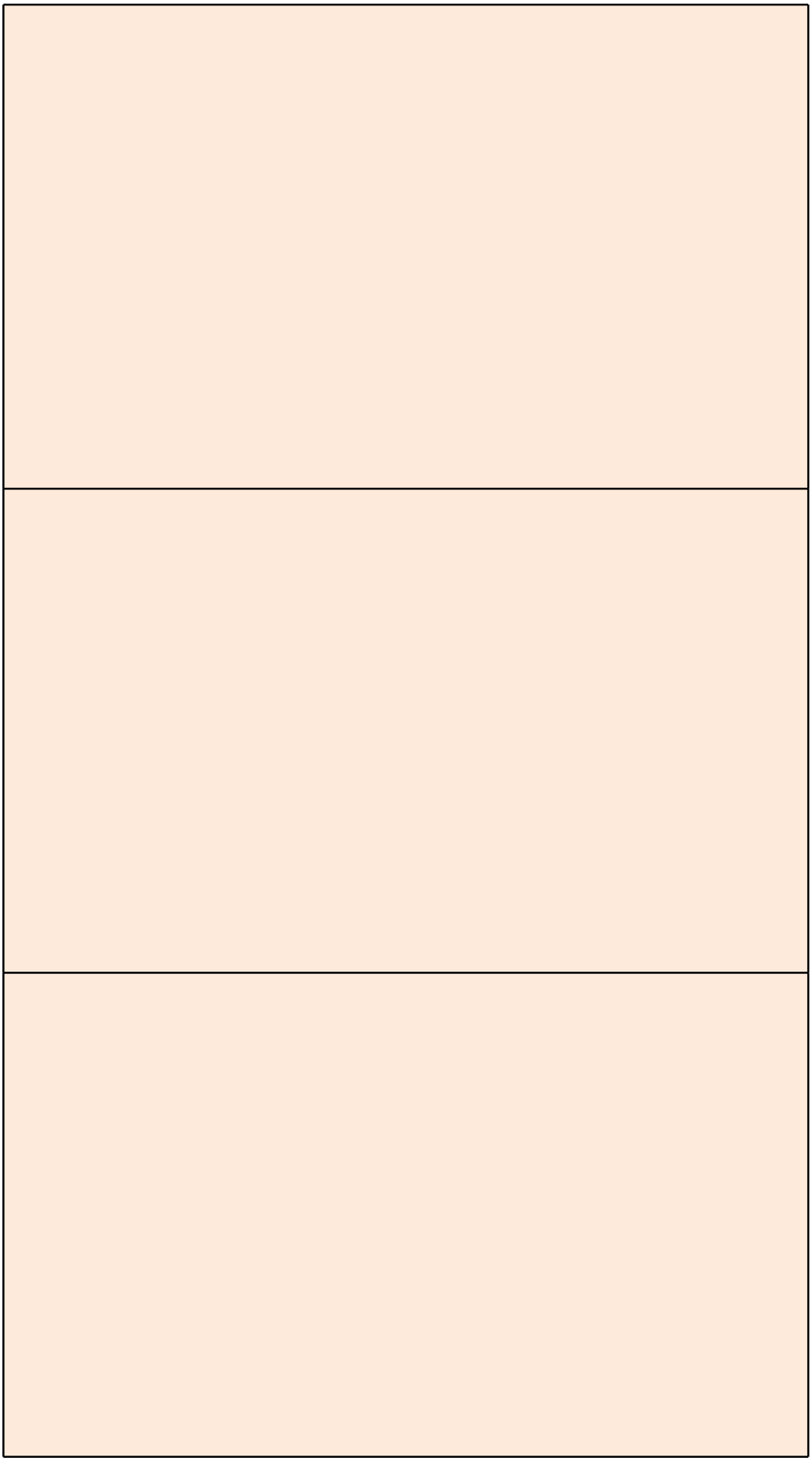


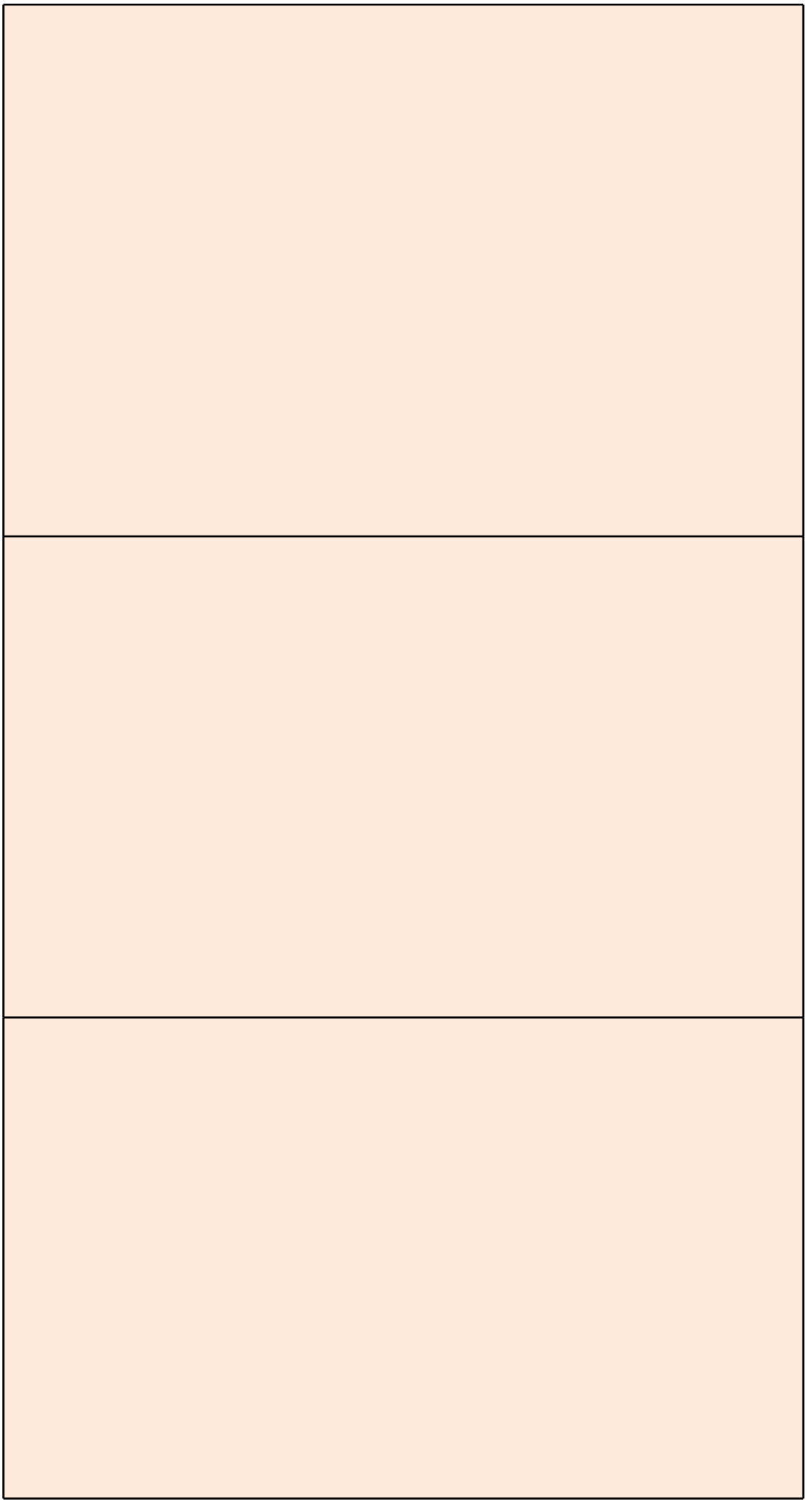


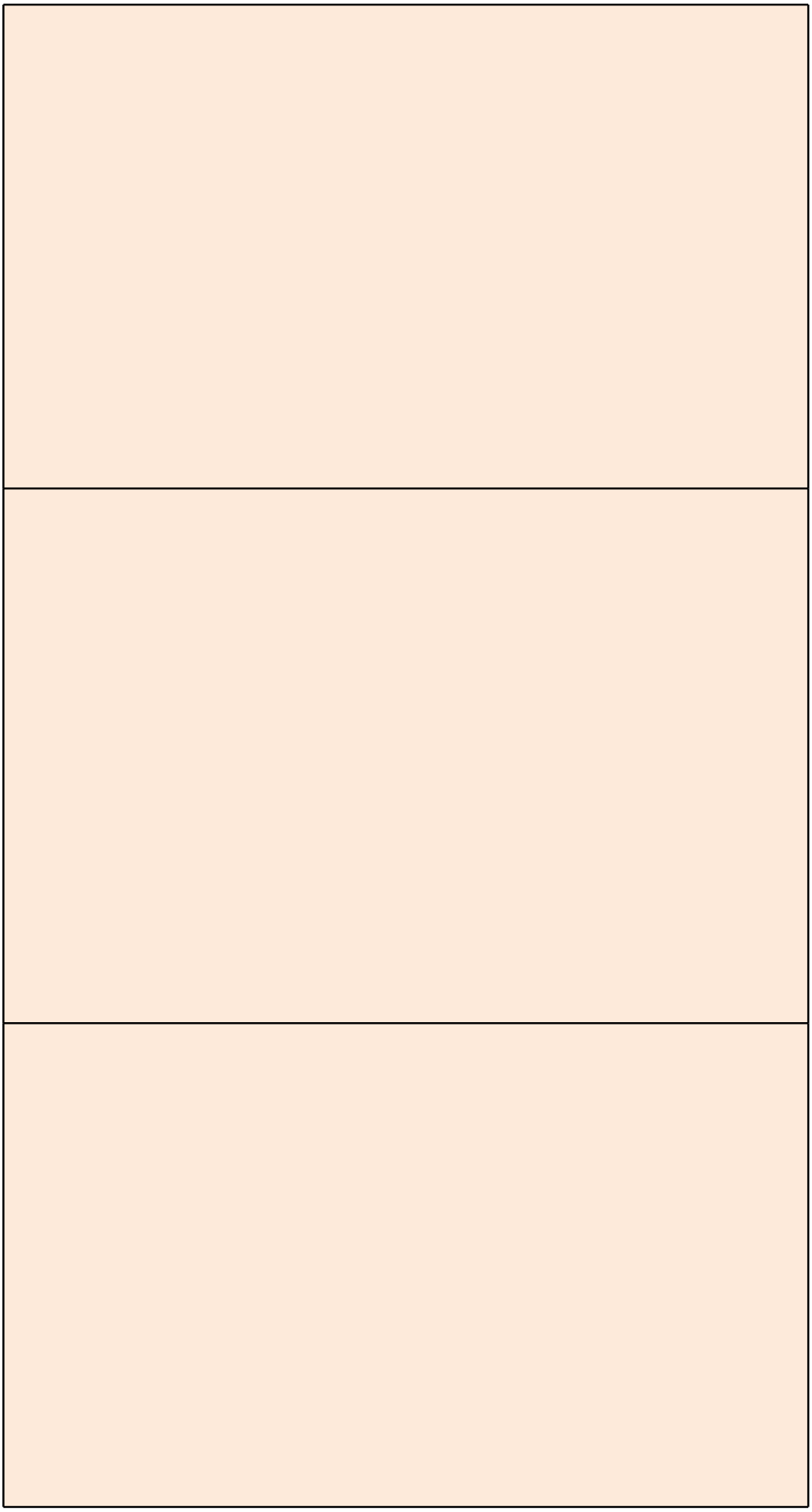


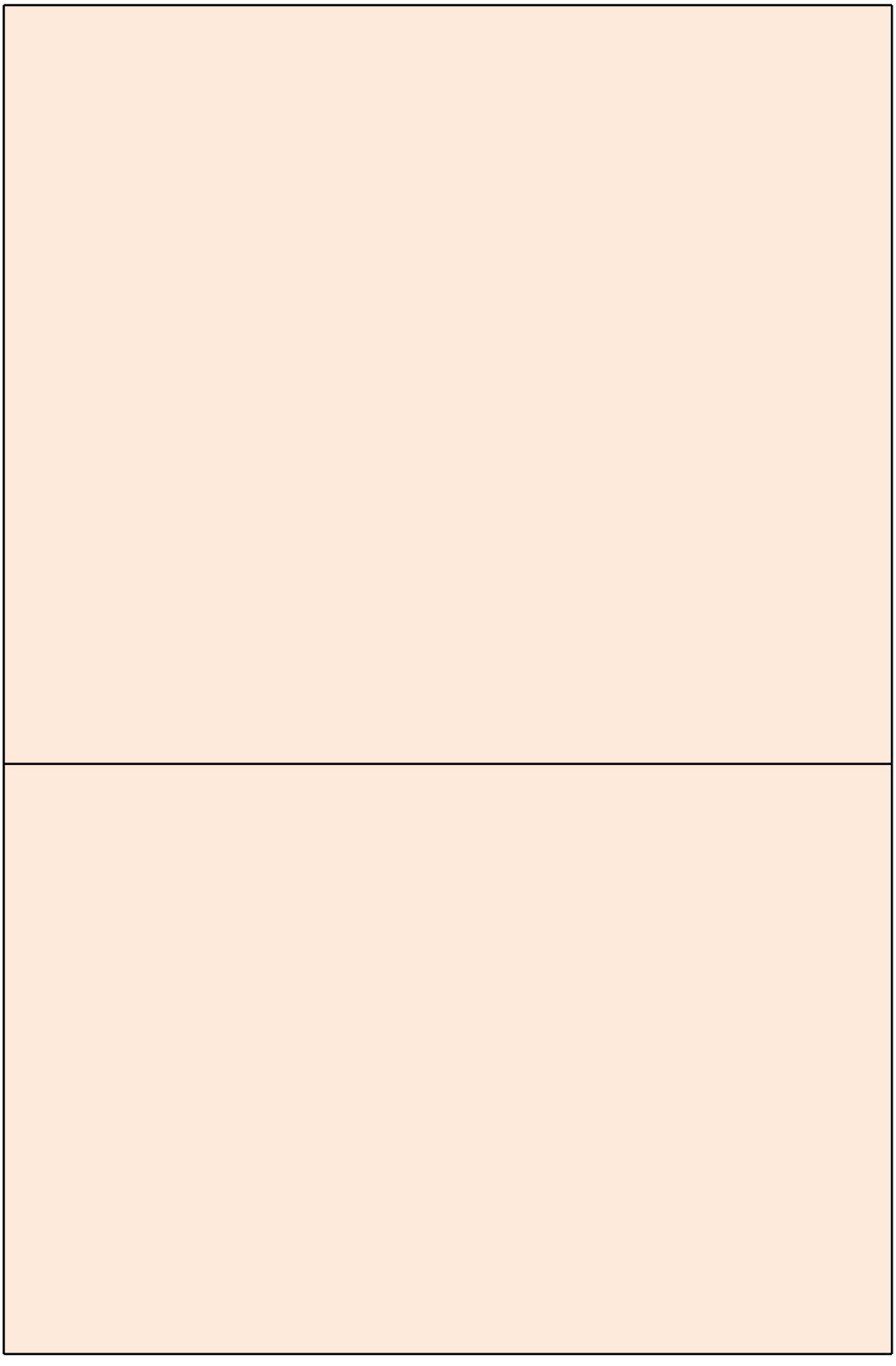


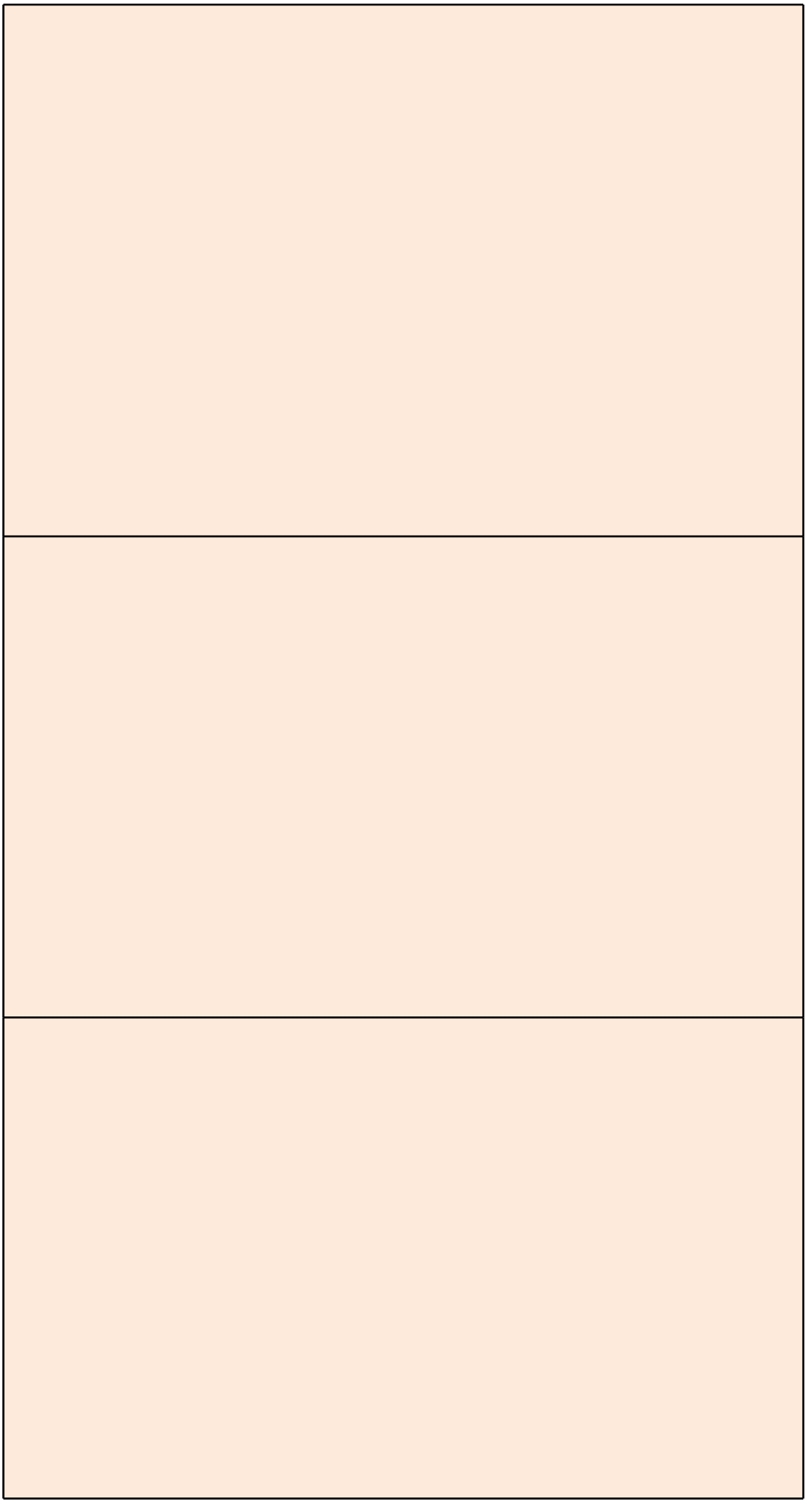


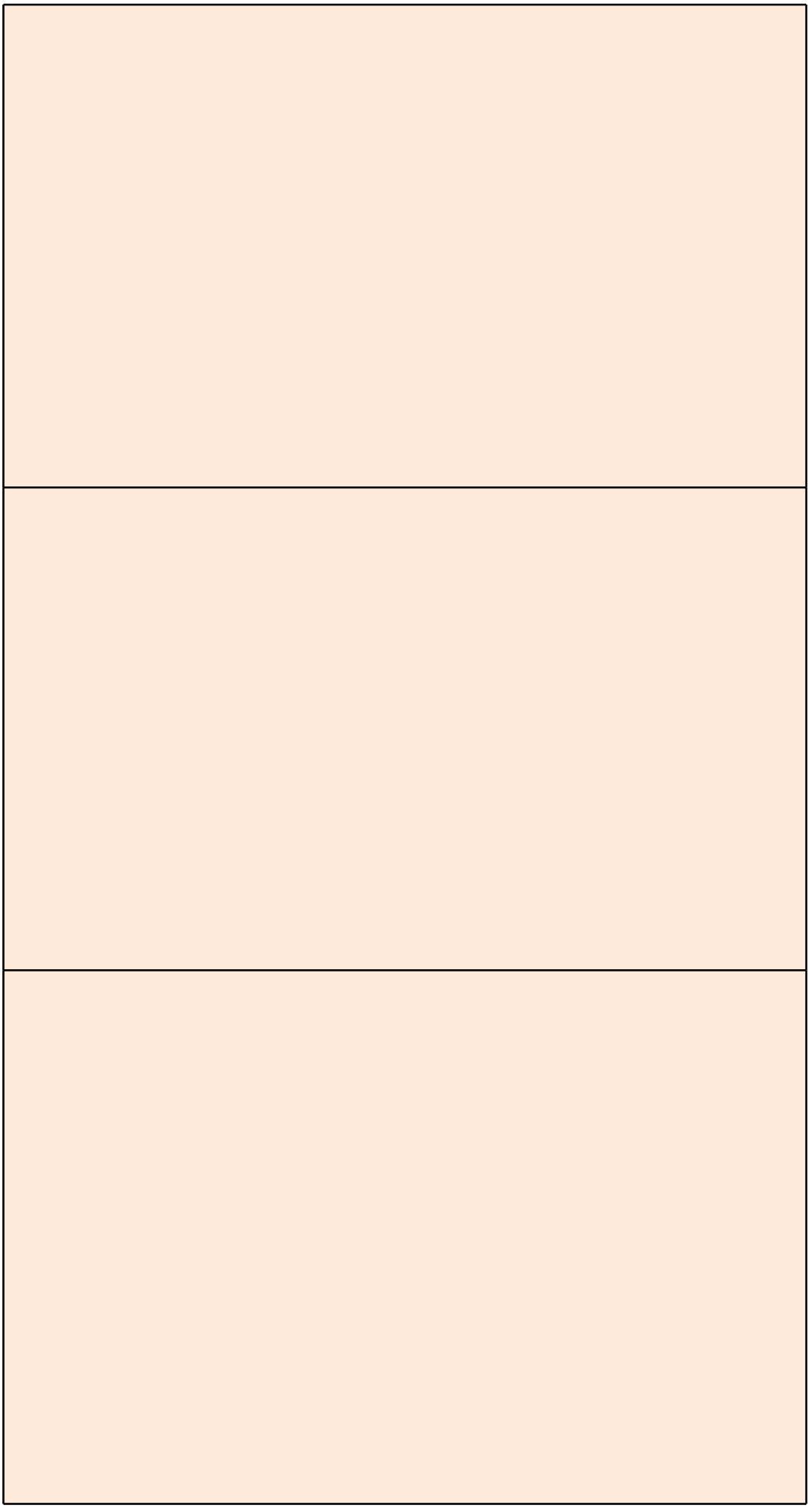


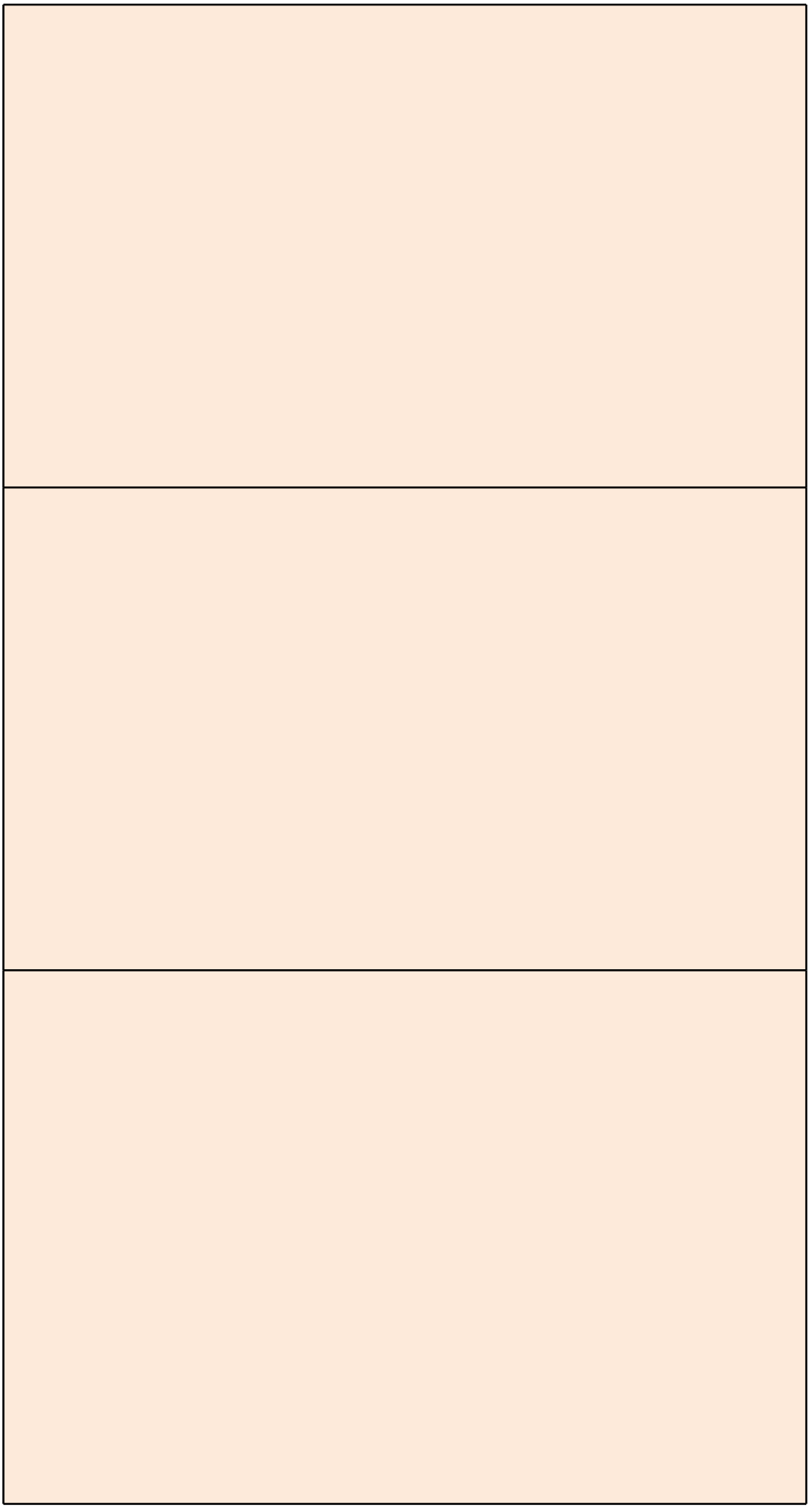


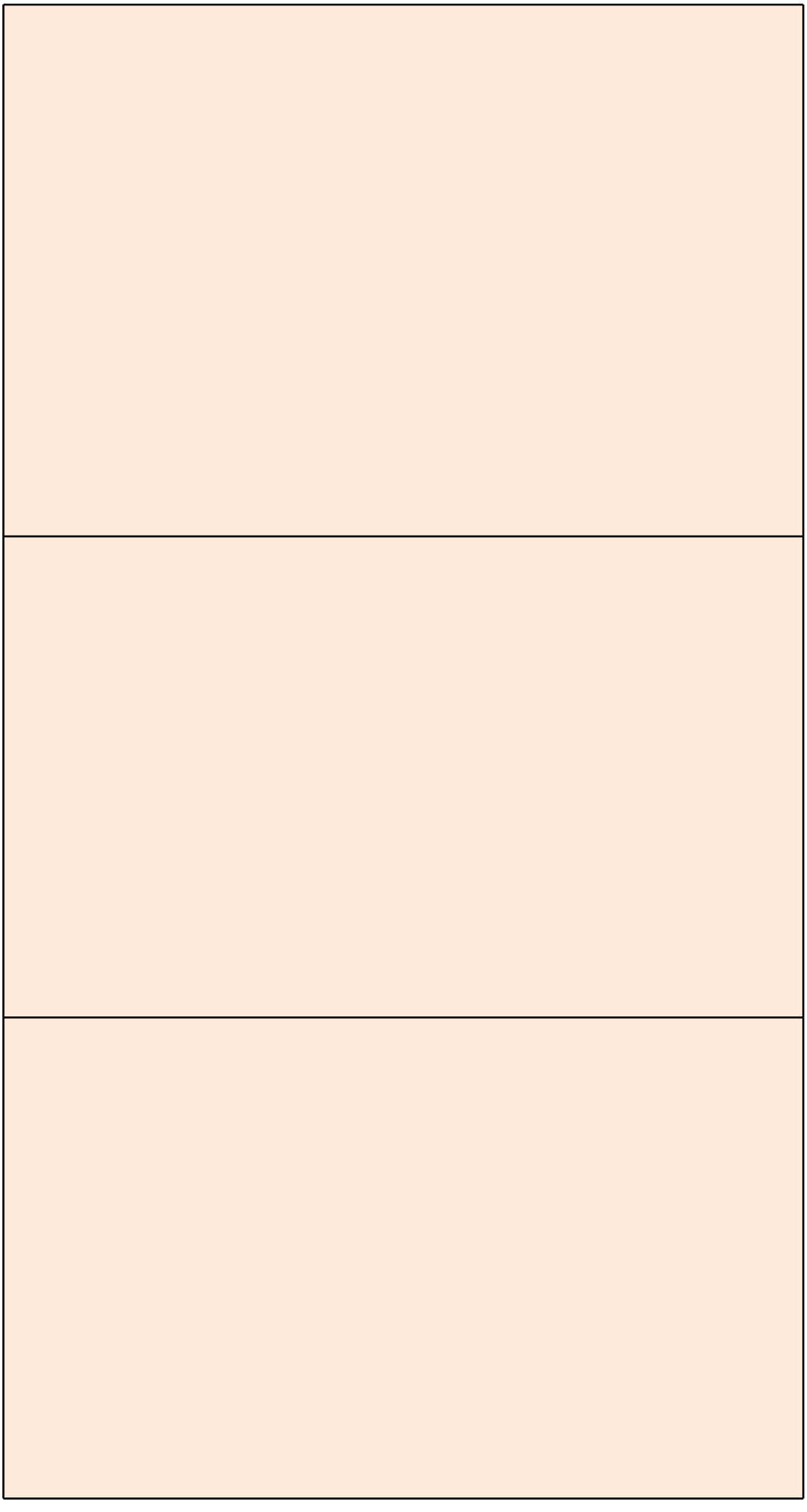


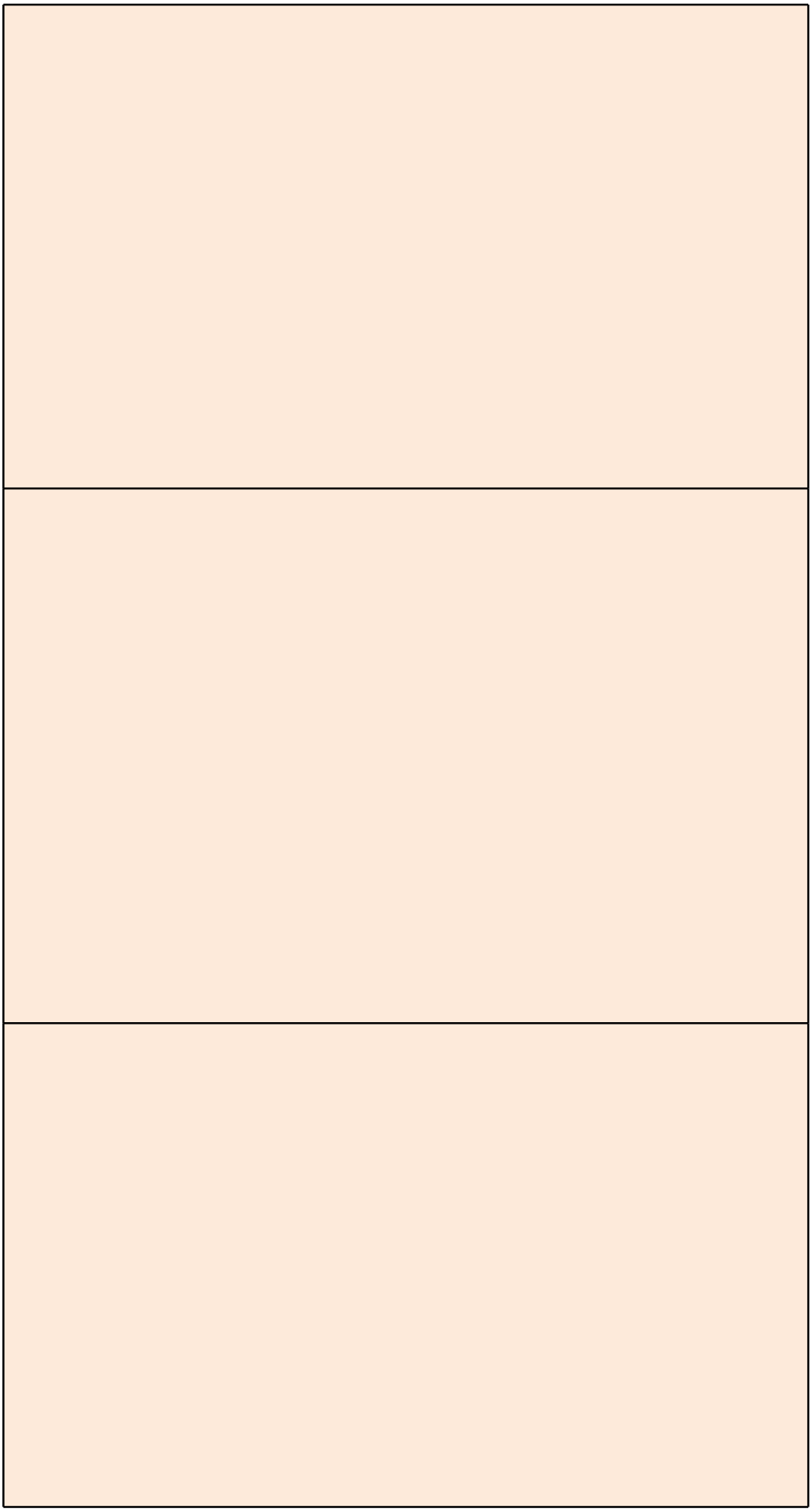


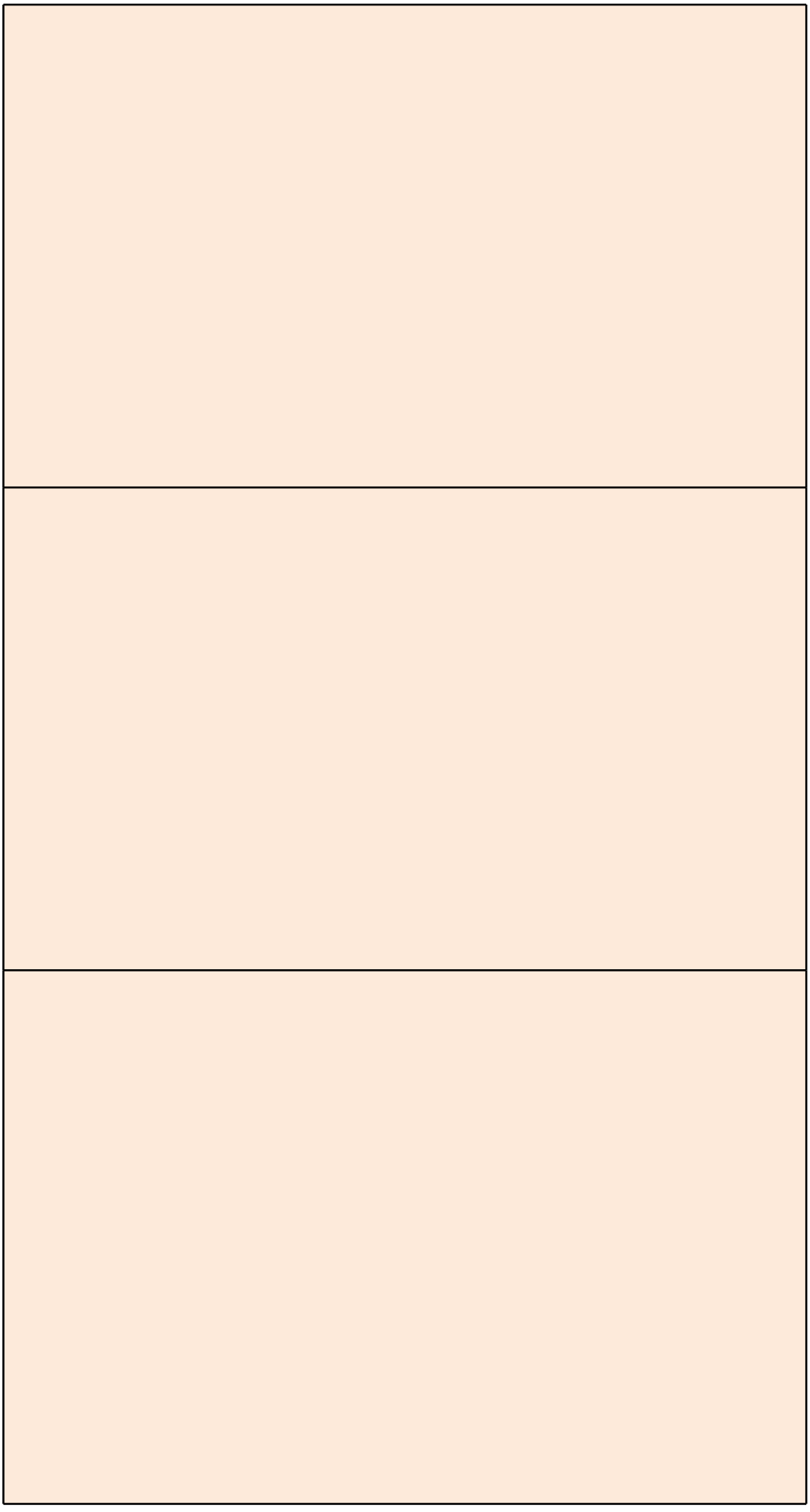


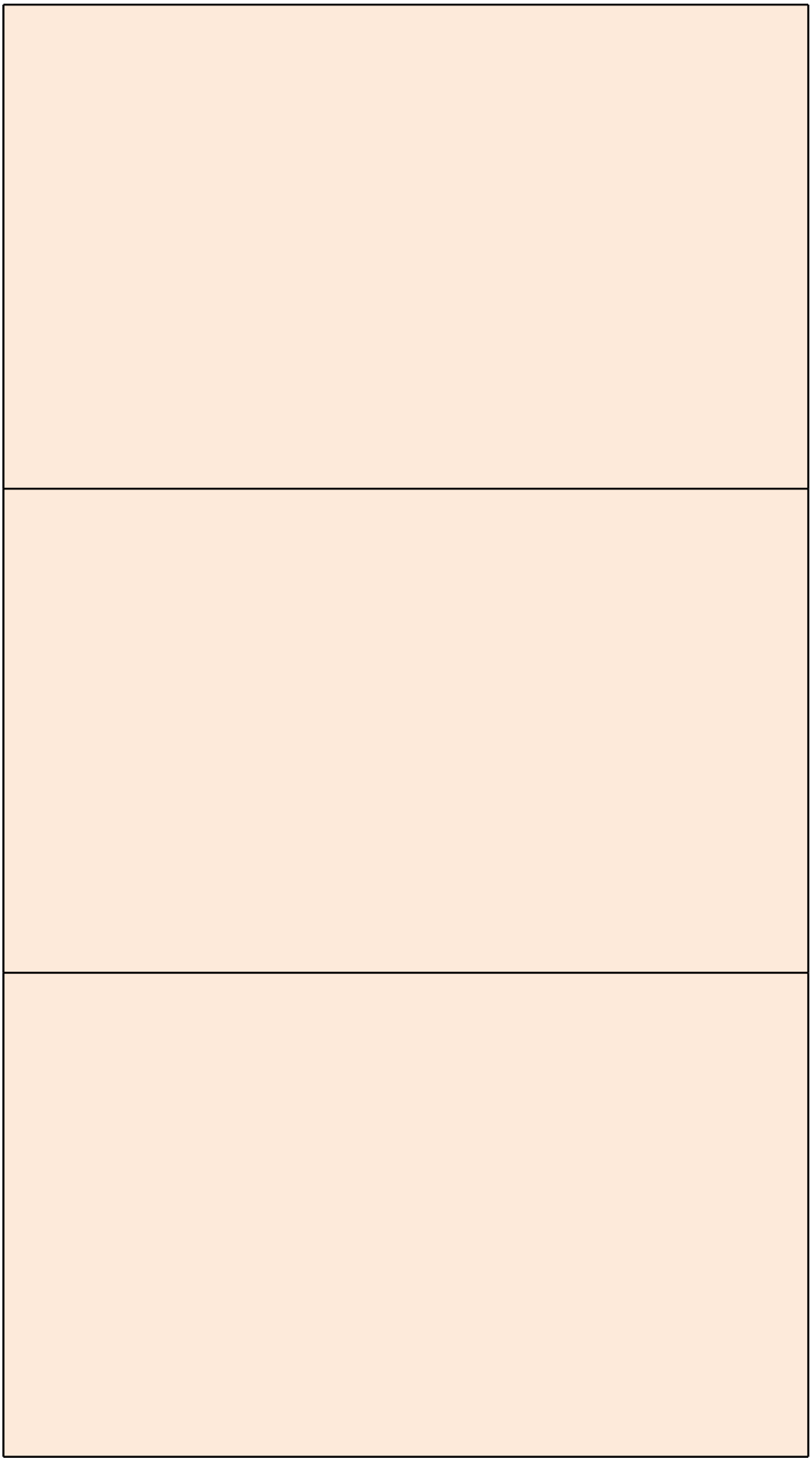


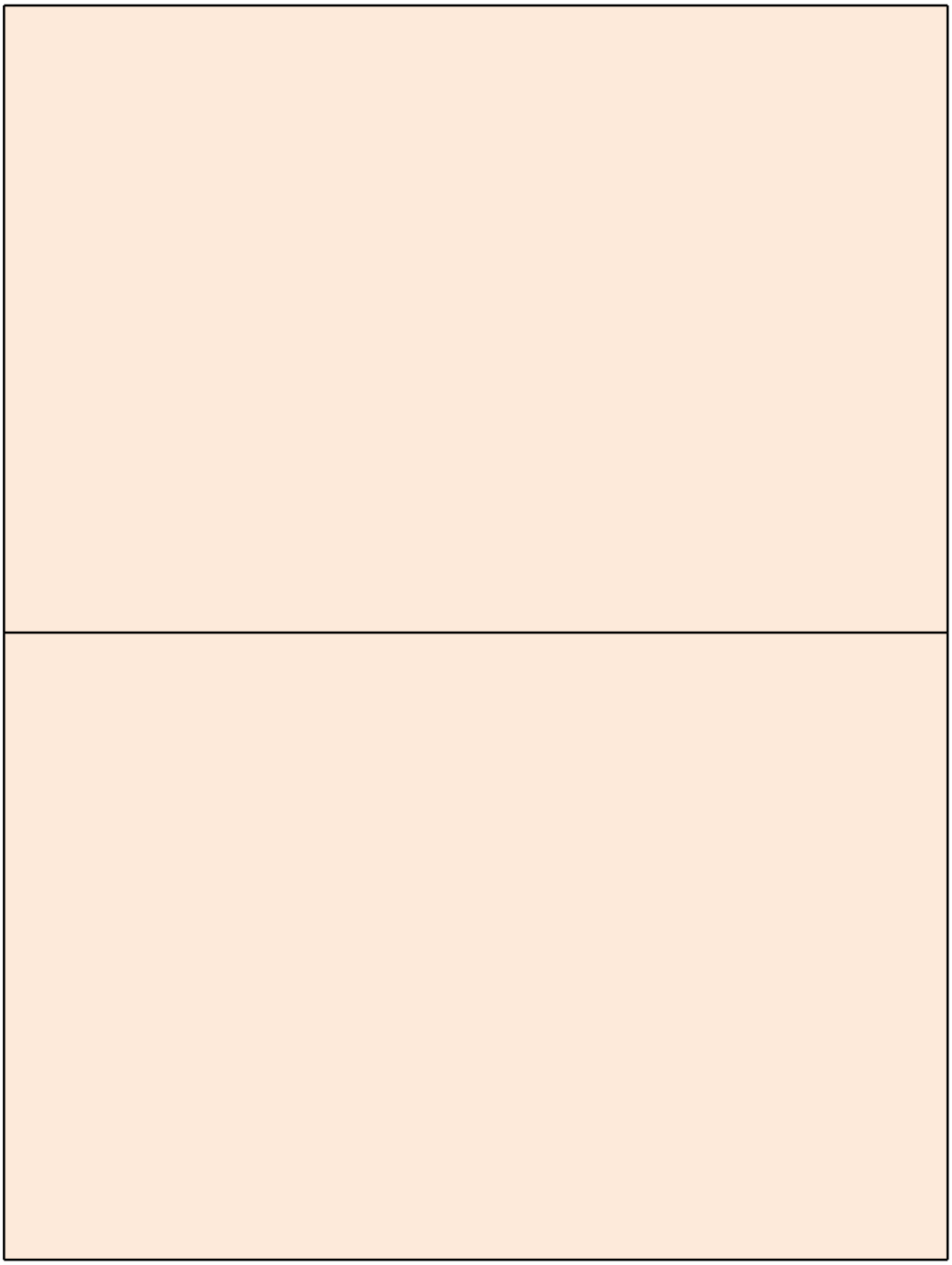


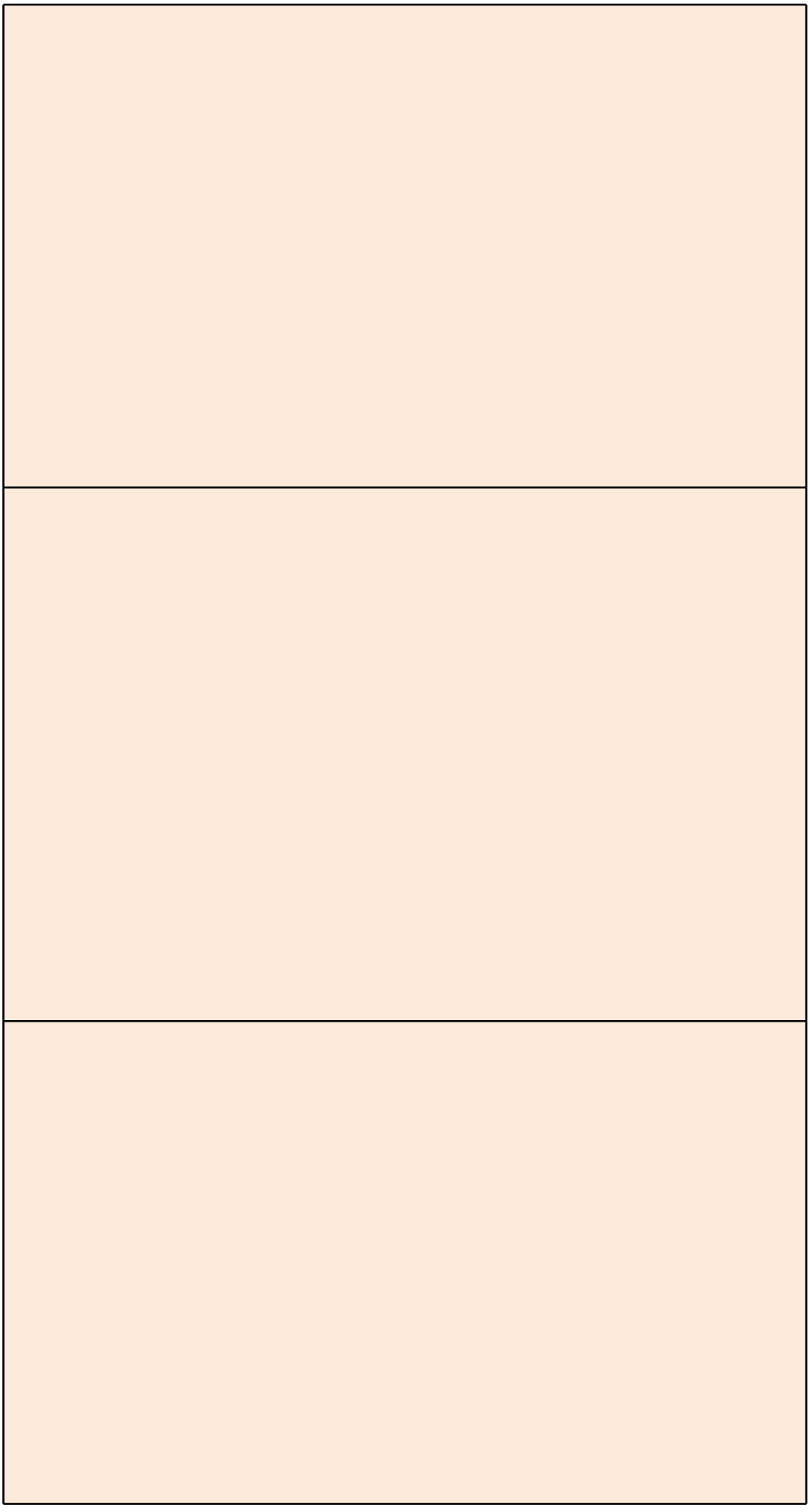


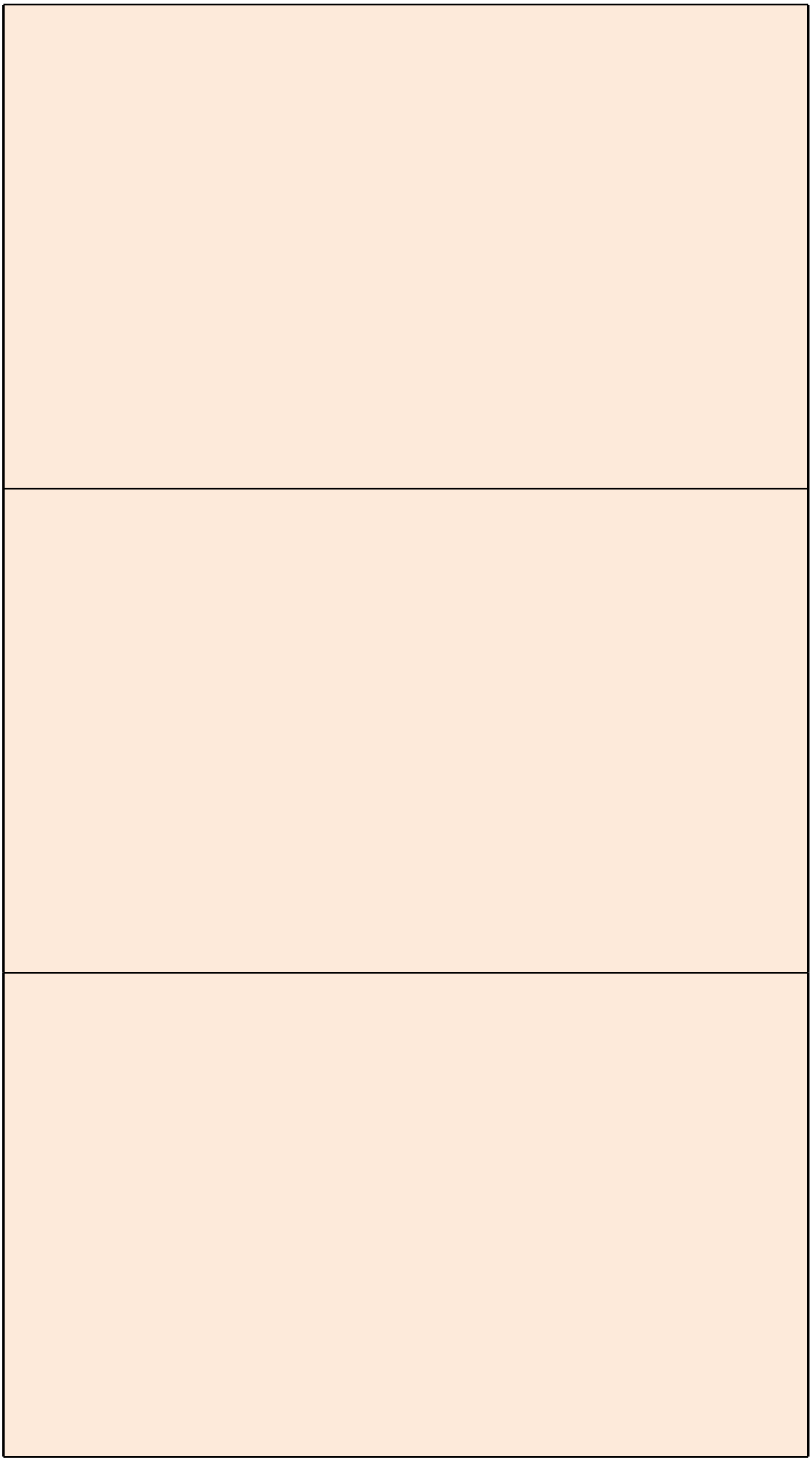


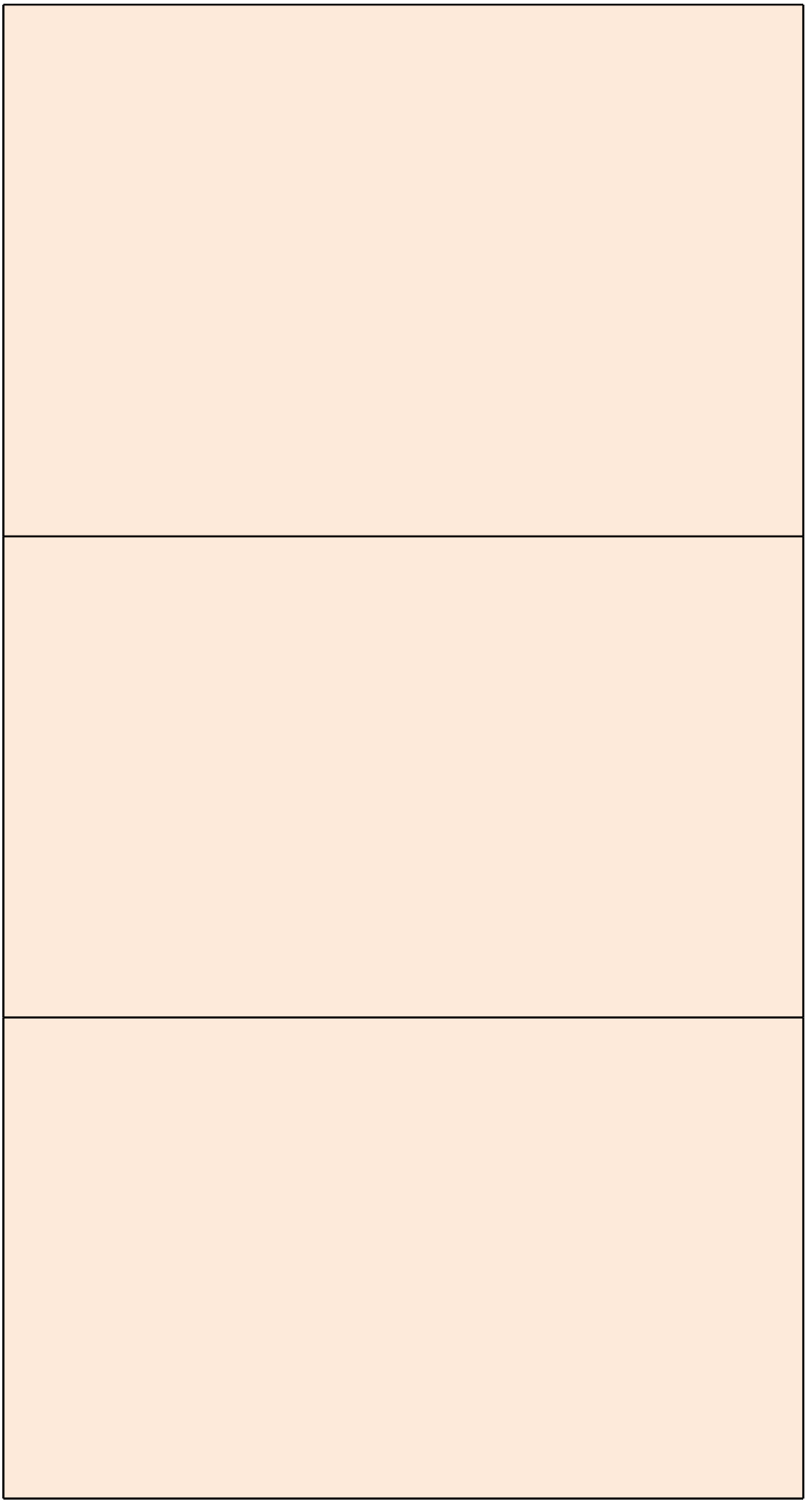


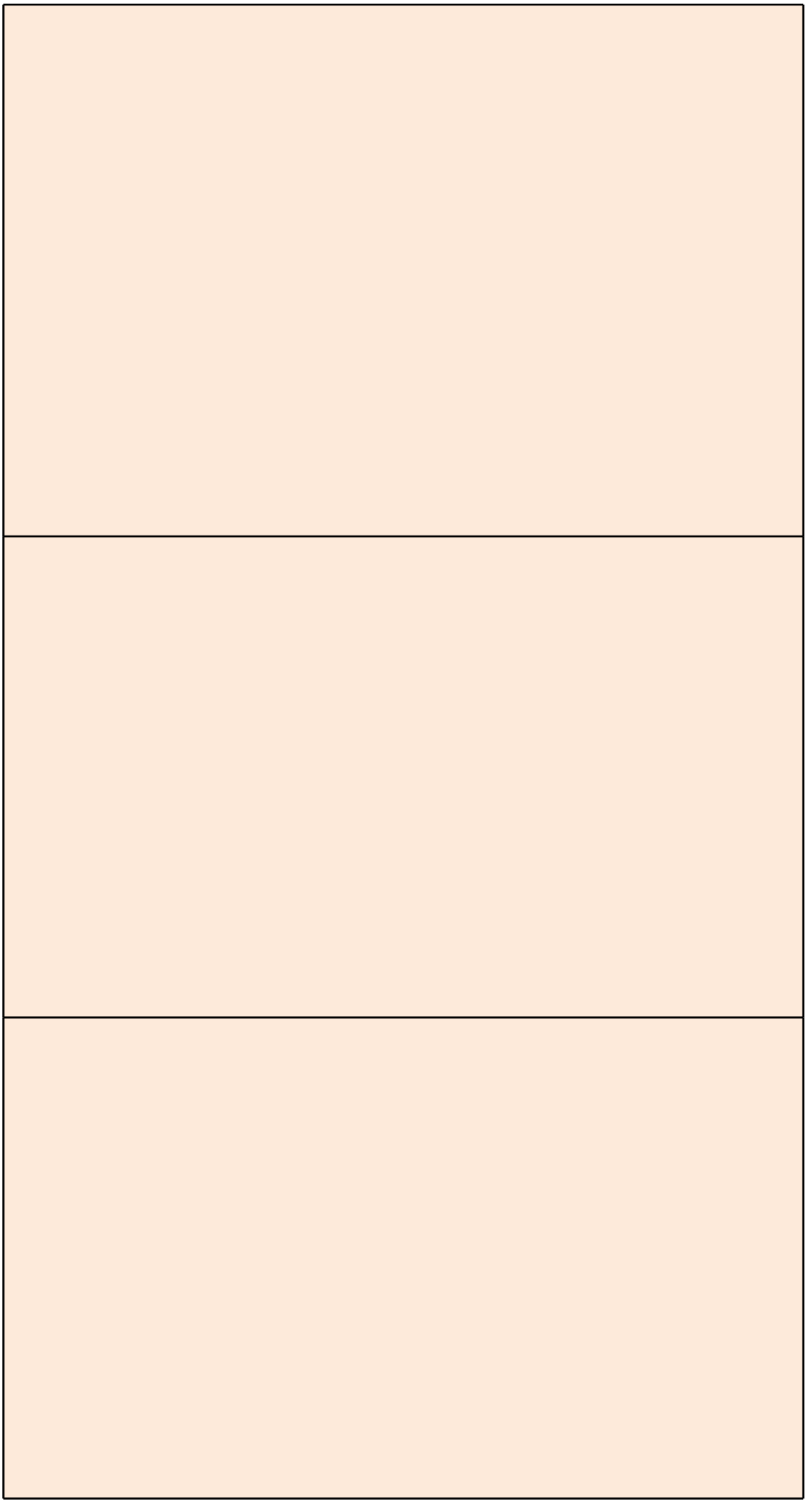


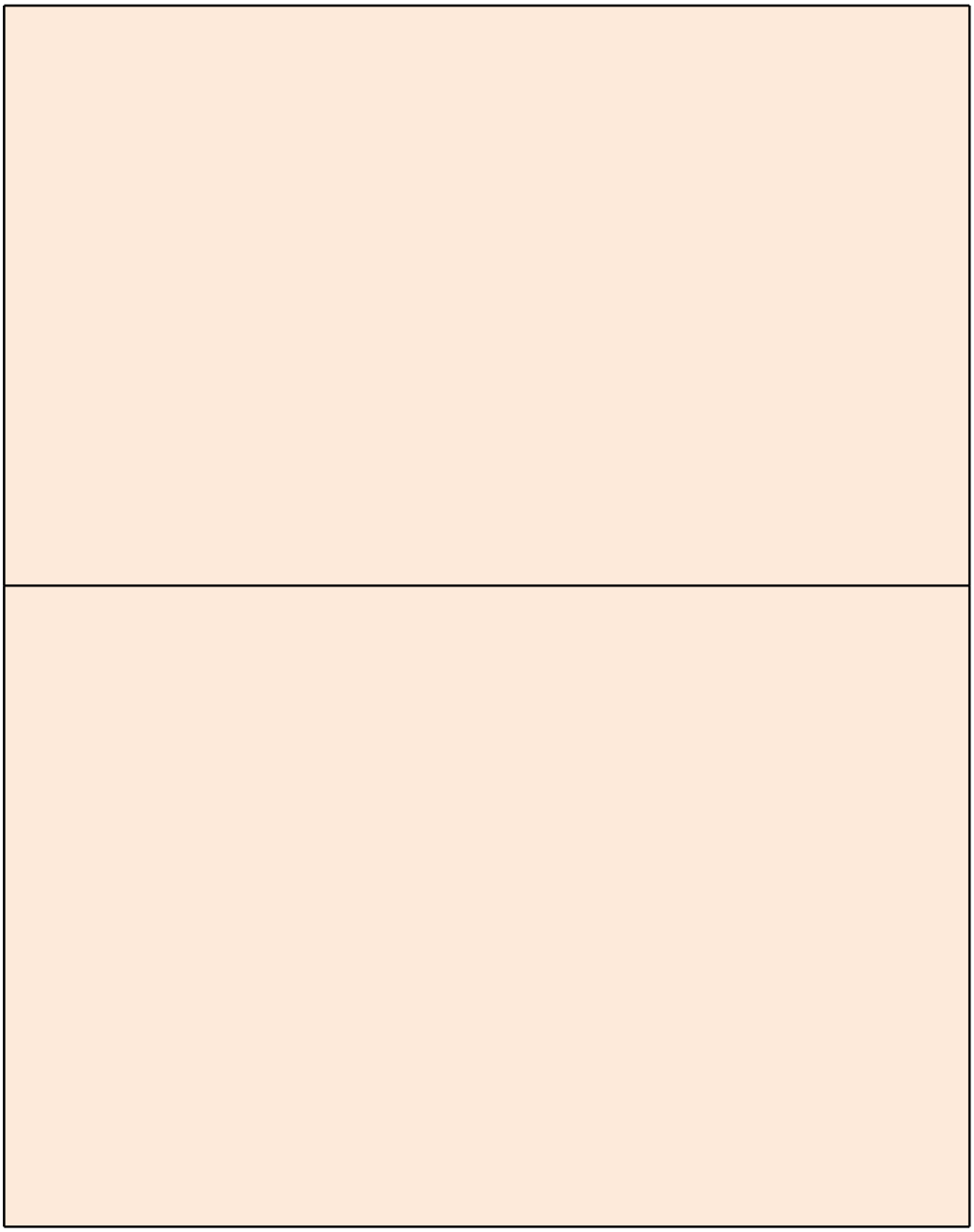


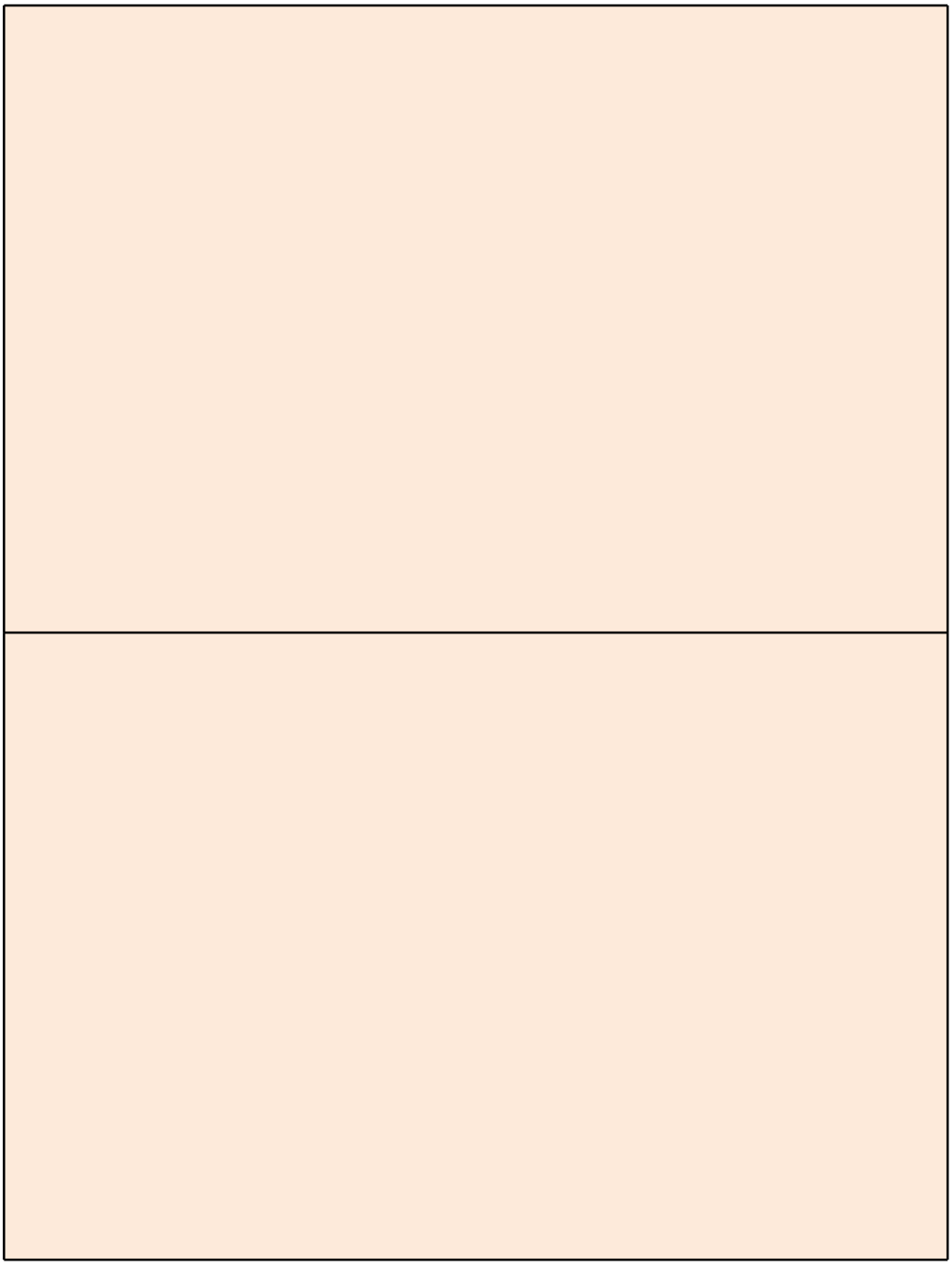




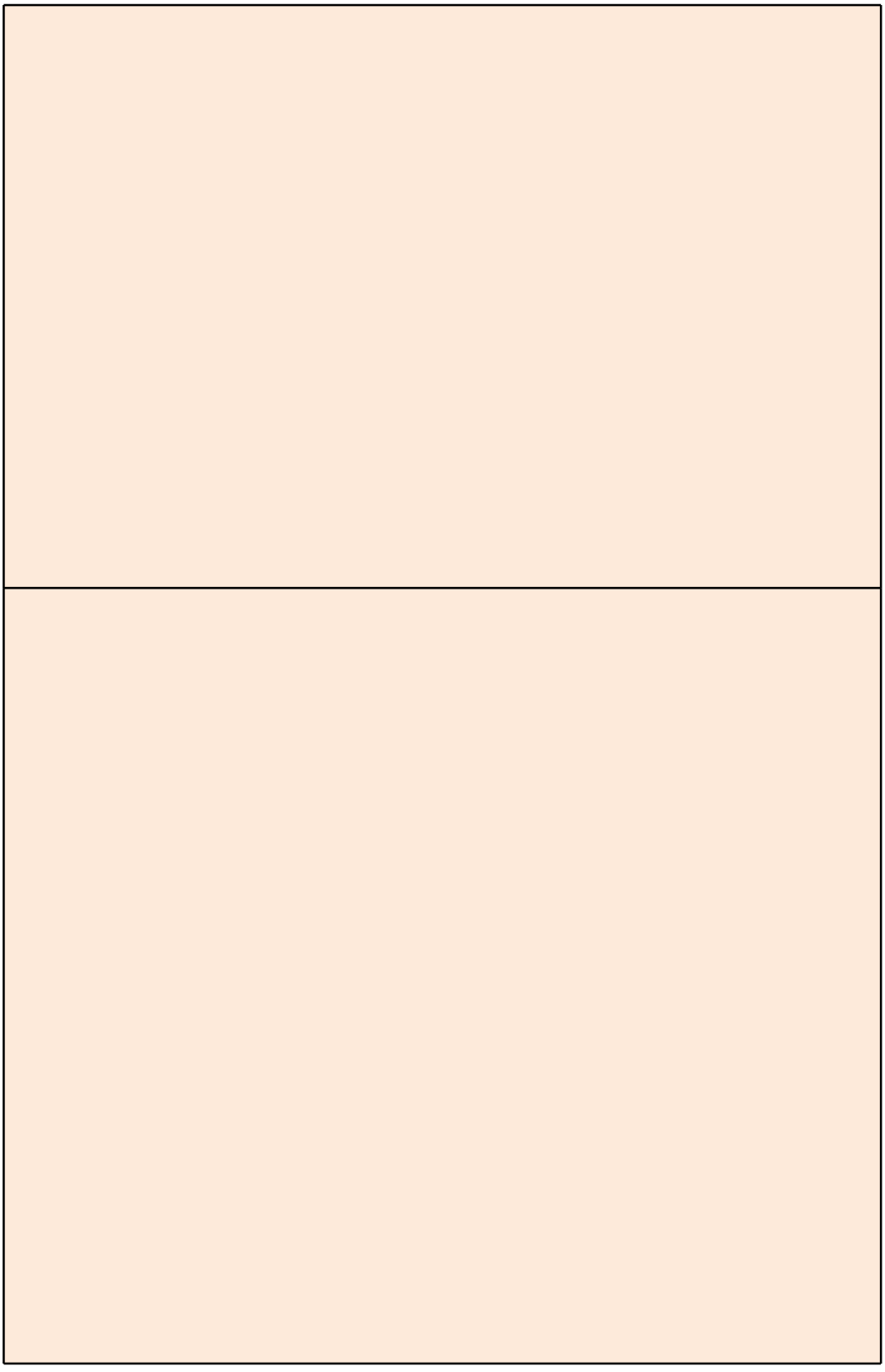


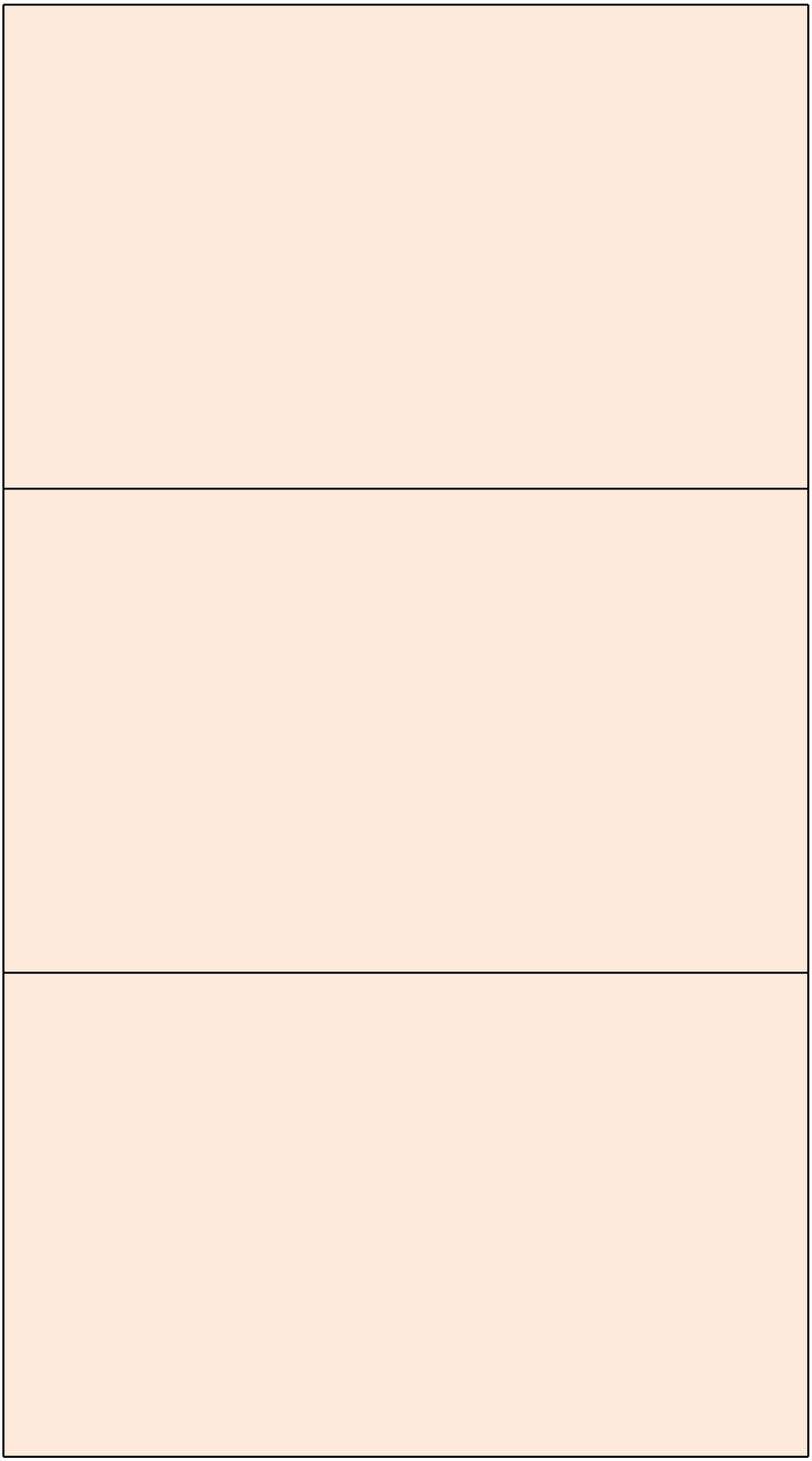




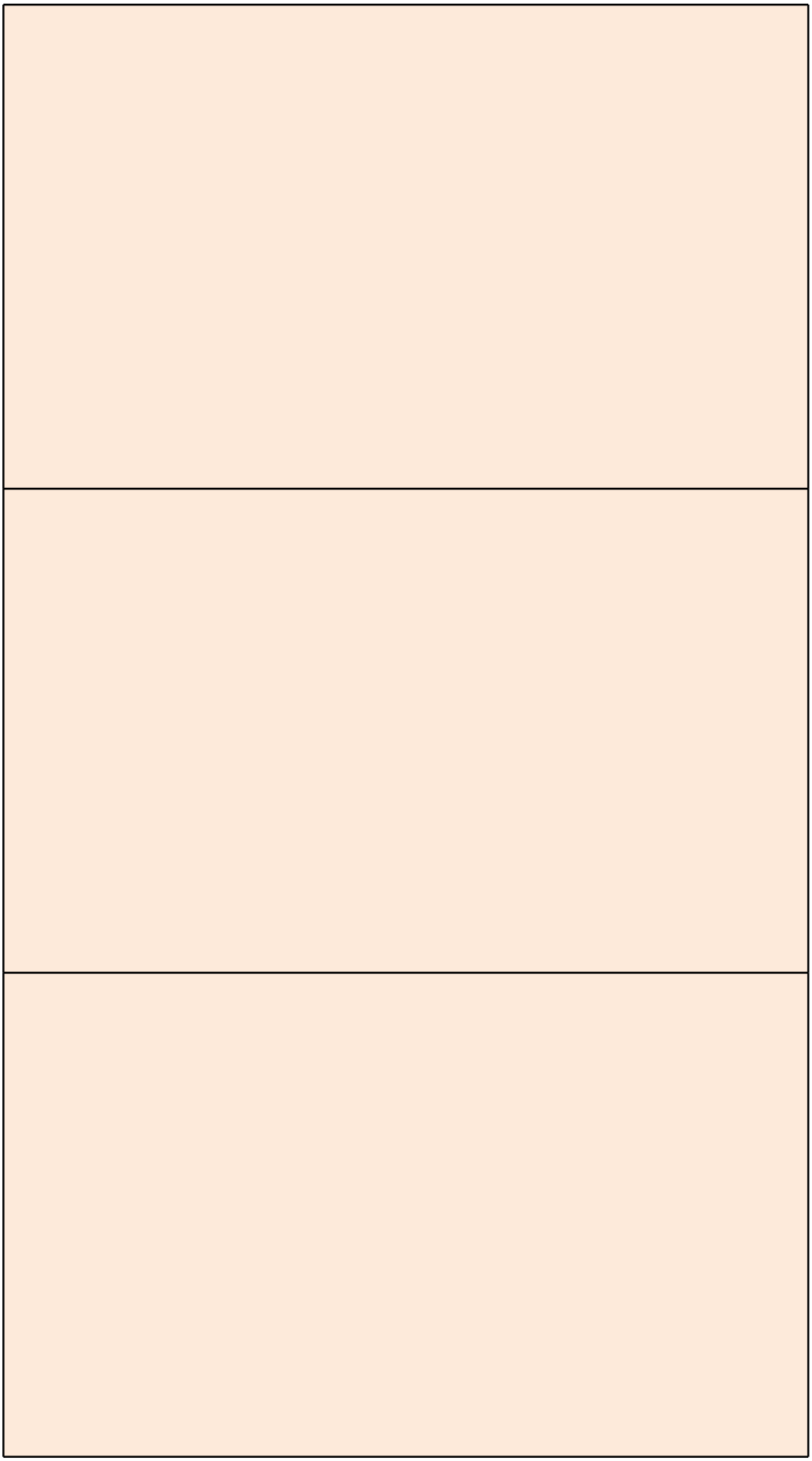


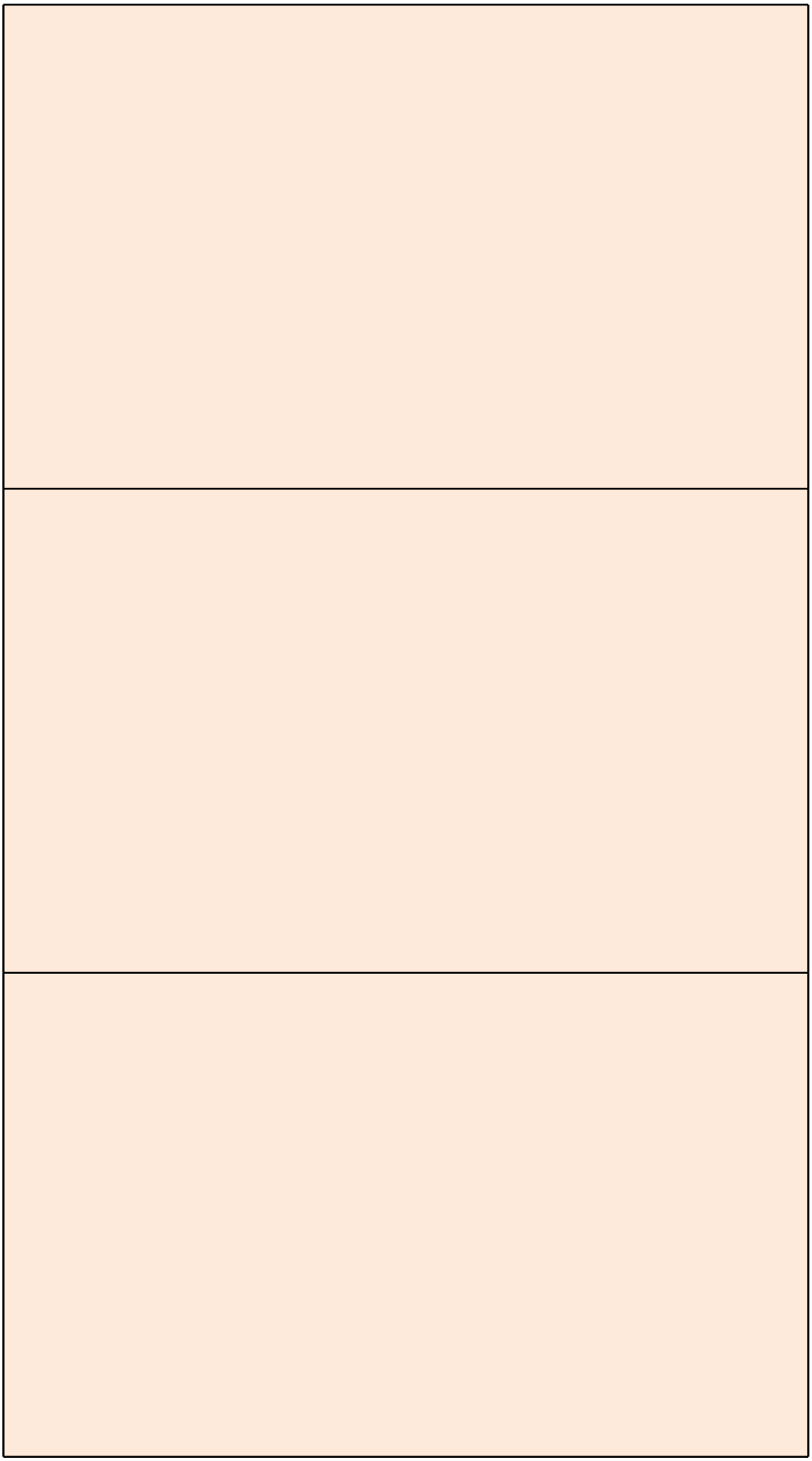
Muu mahdollinen kommentti

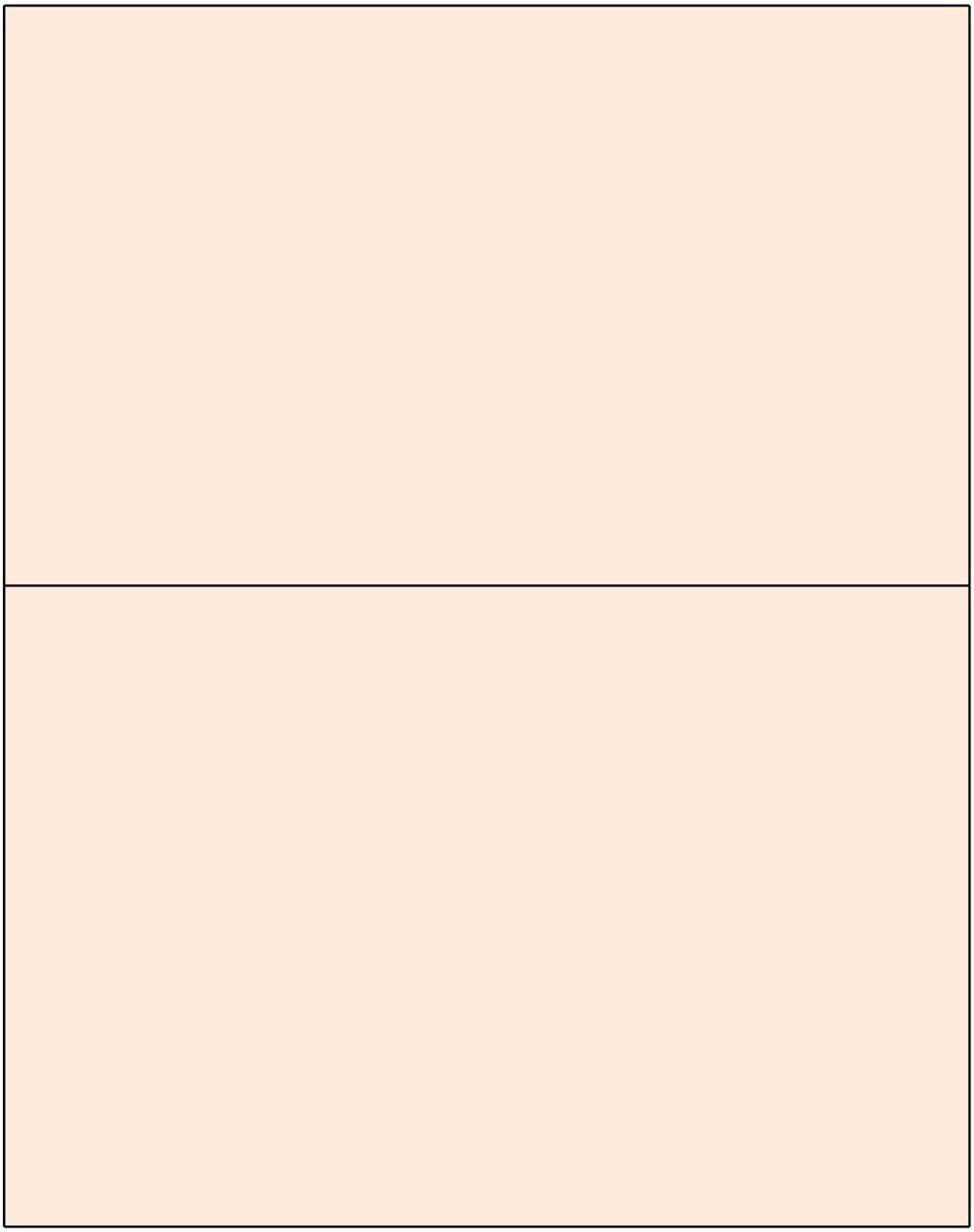


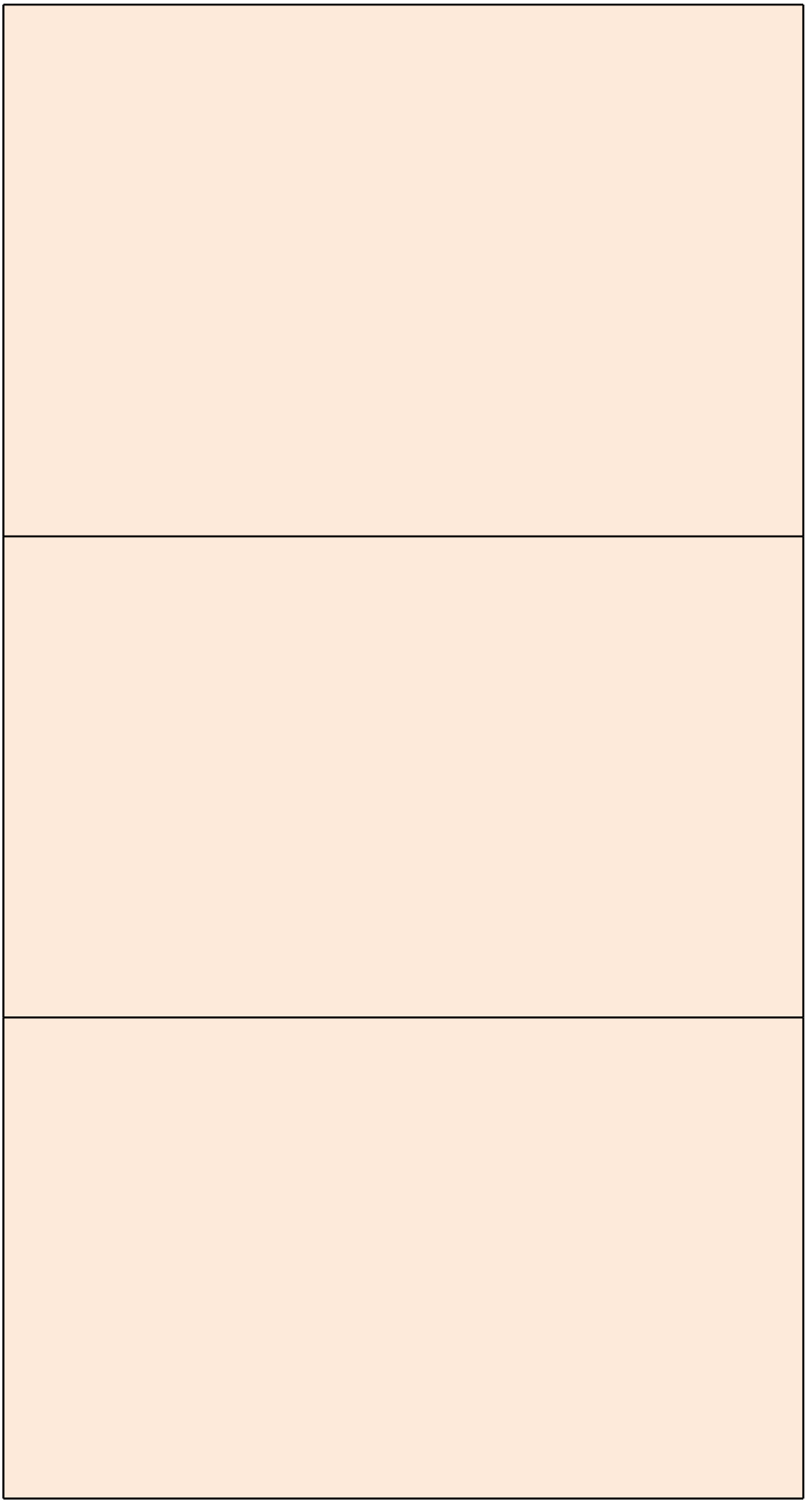


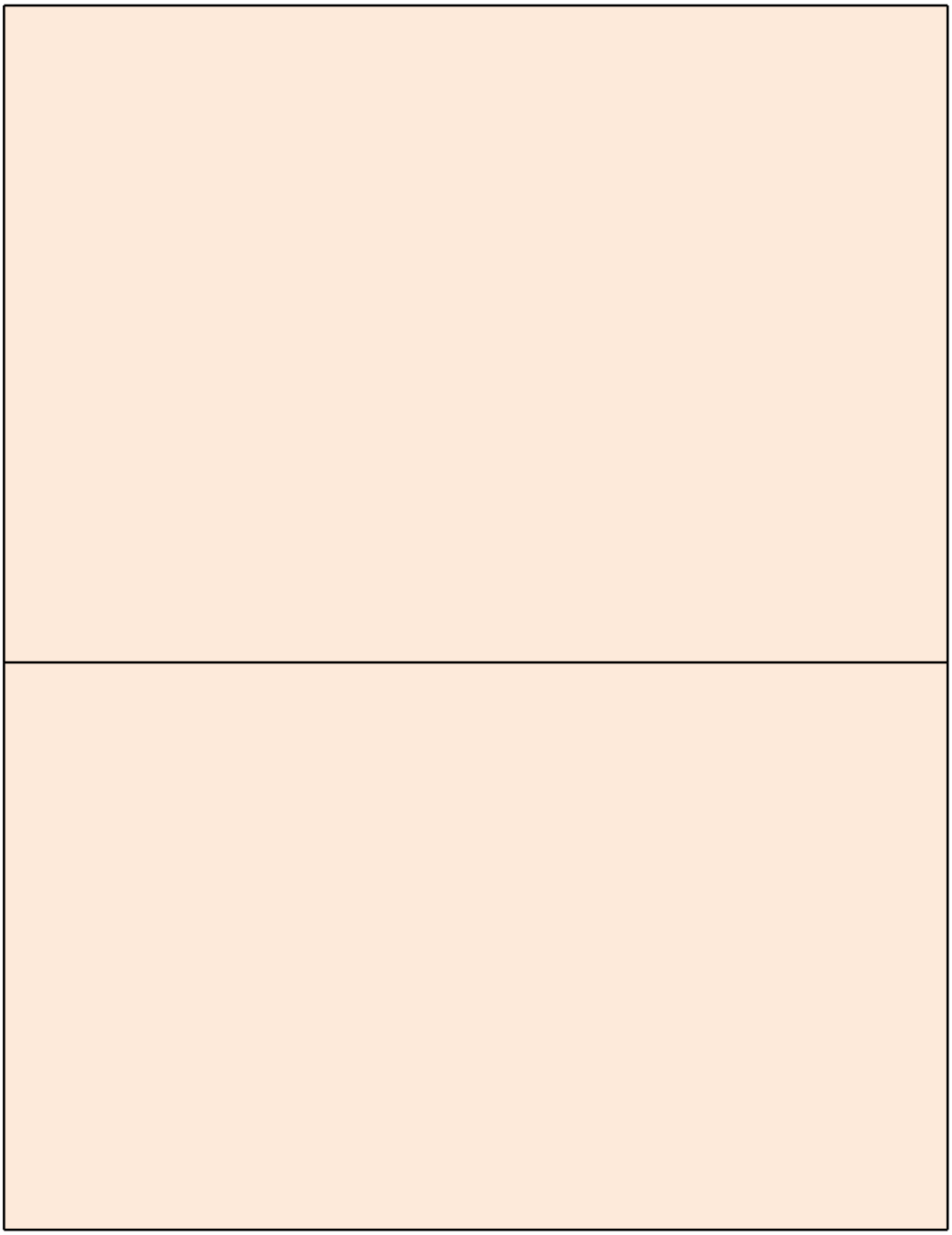
Kulkuneuvon määritelmä tulisi lisätä: Kulkuneuvo on paikasta toiseen kulkemiseen tarkoitettu laite, joka voi kuljettaa matkustajia, tavaroita tai molempia maalla, vedessä tai ilmassa. (5 §, perustelumuistion teksti)

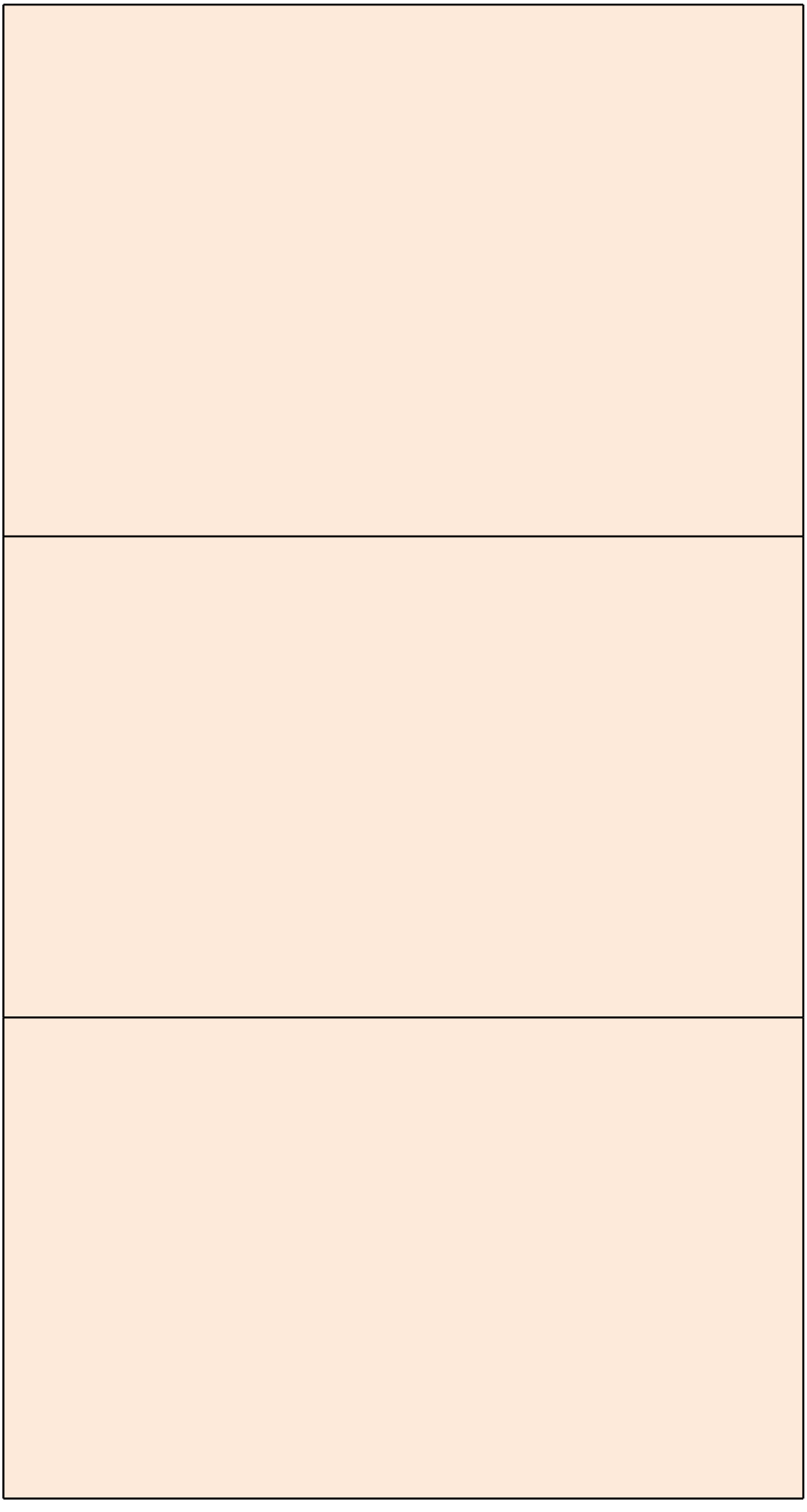




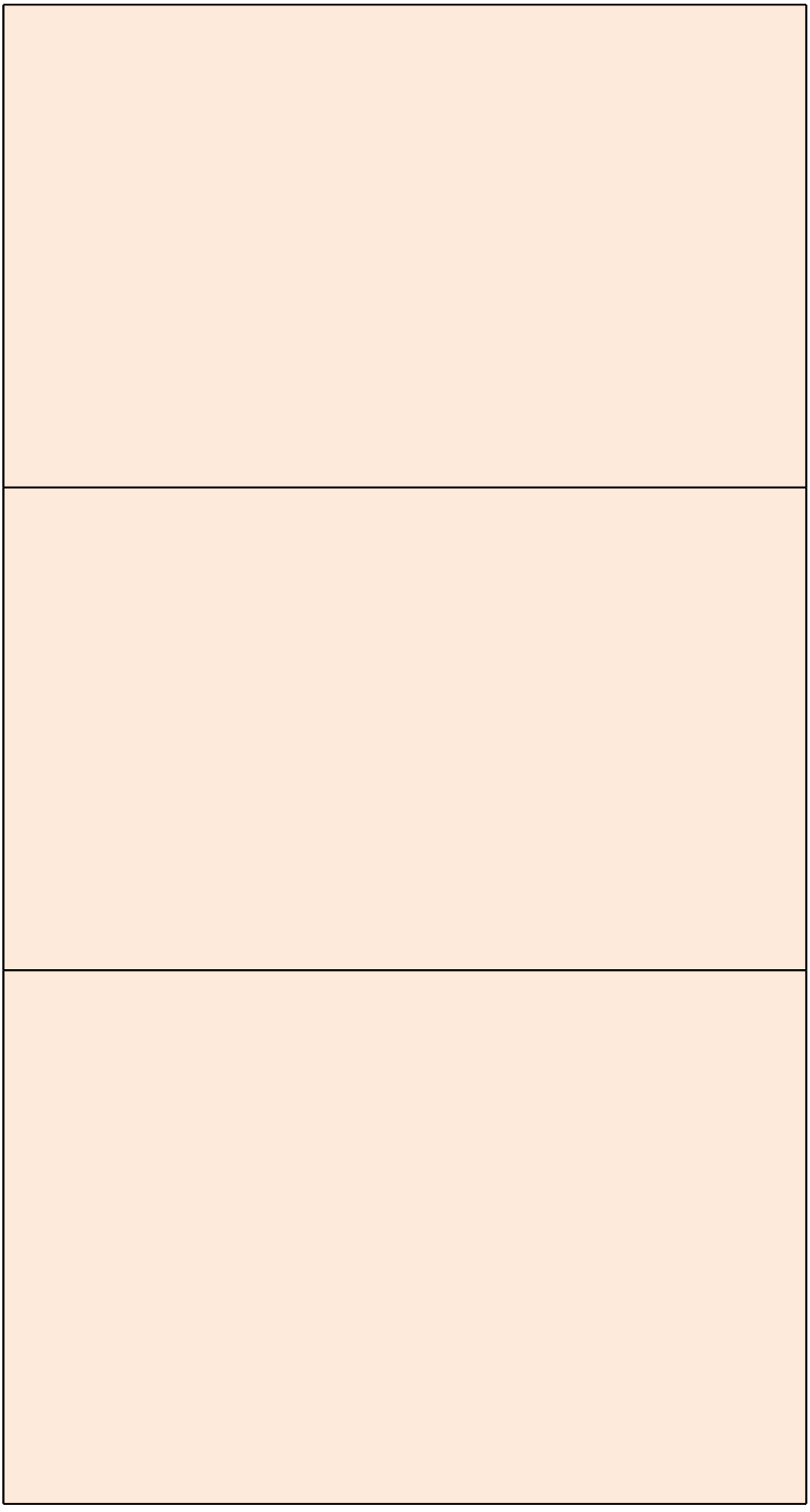


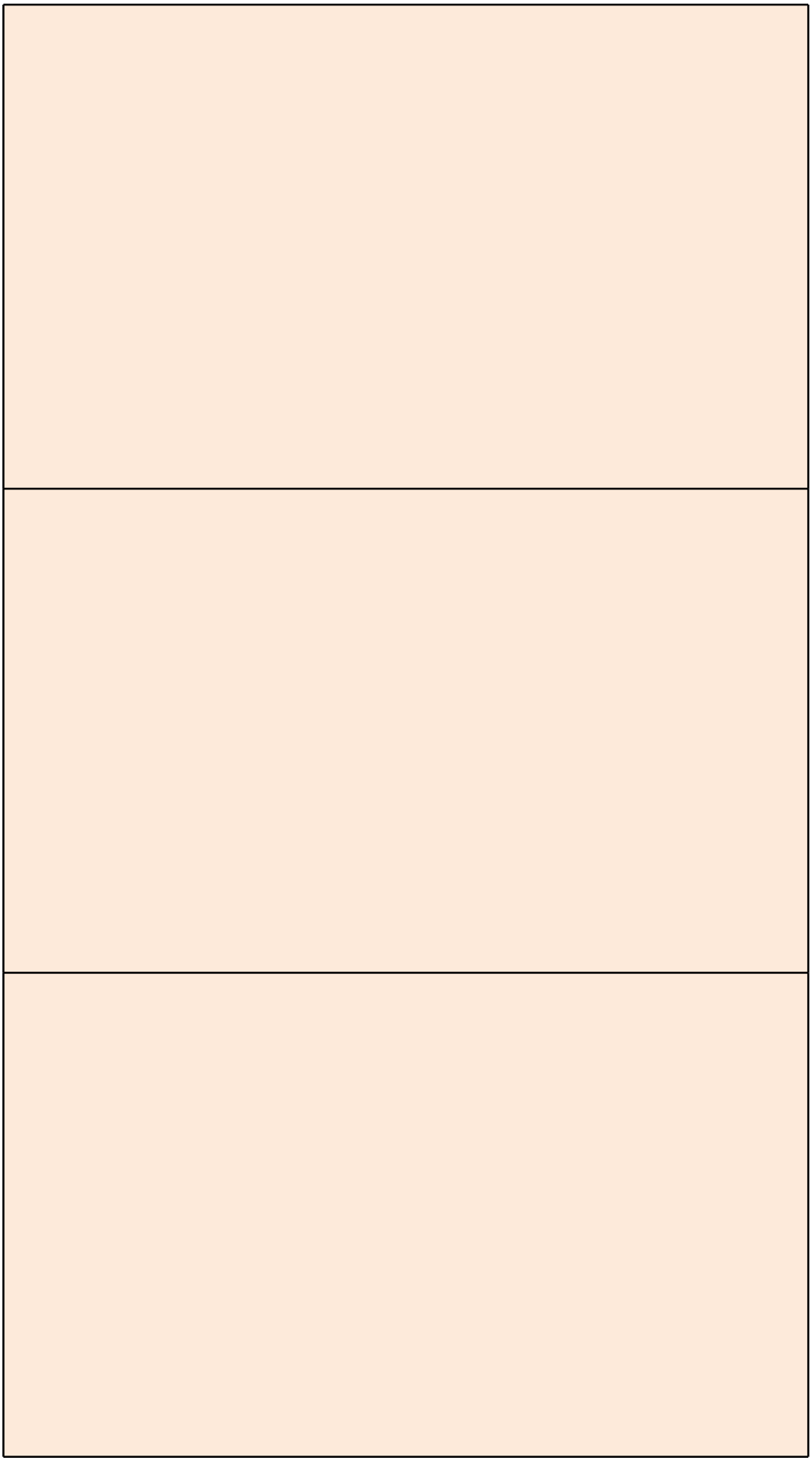


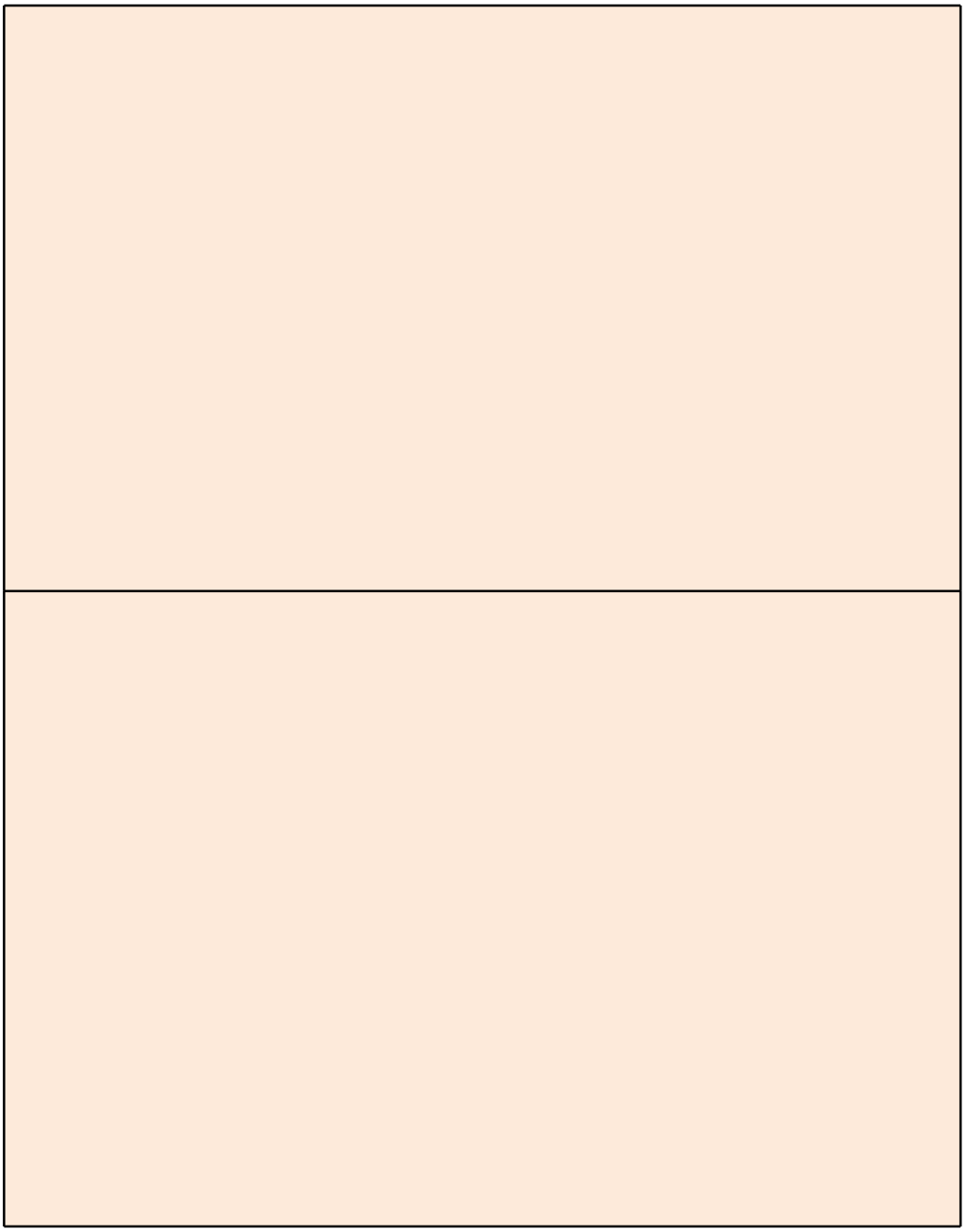


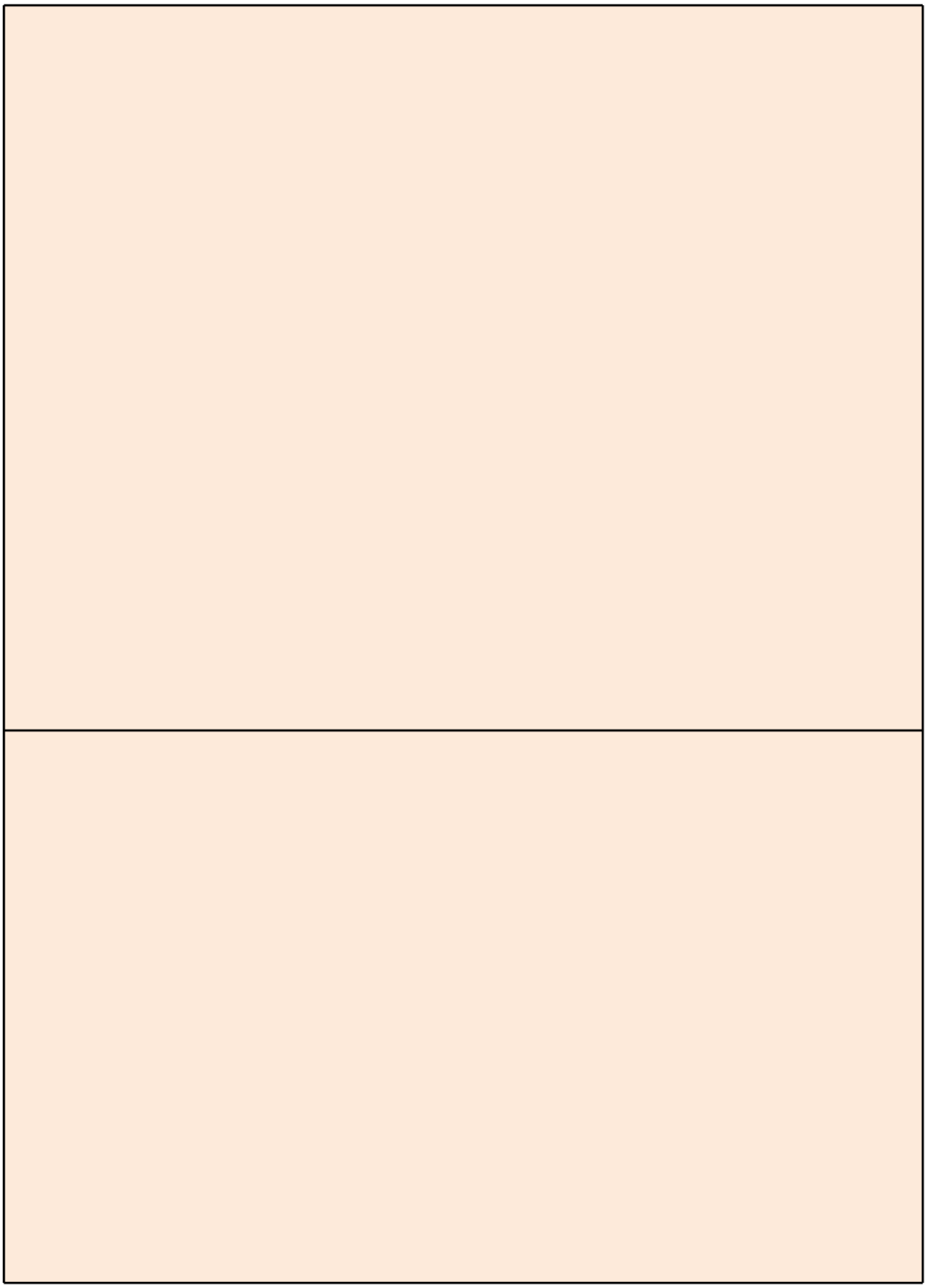


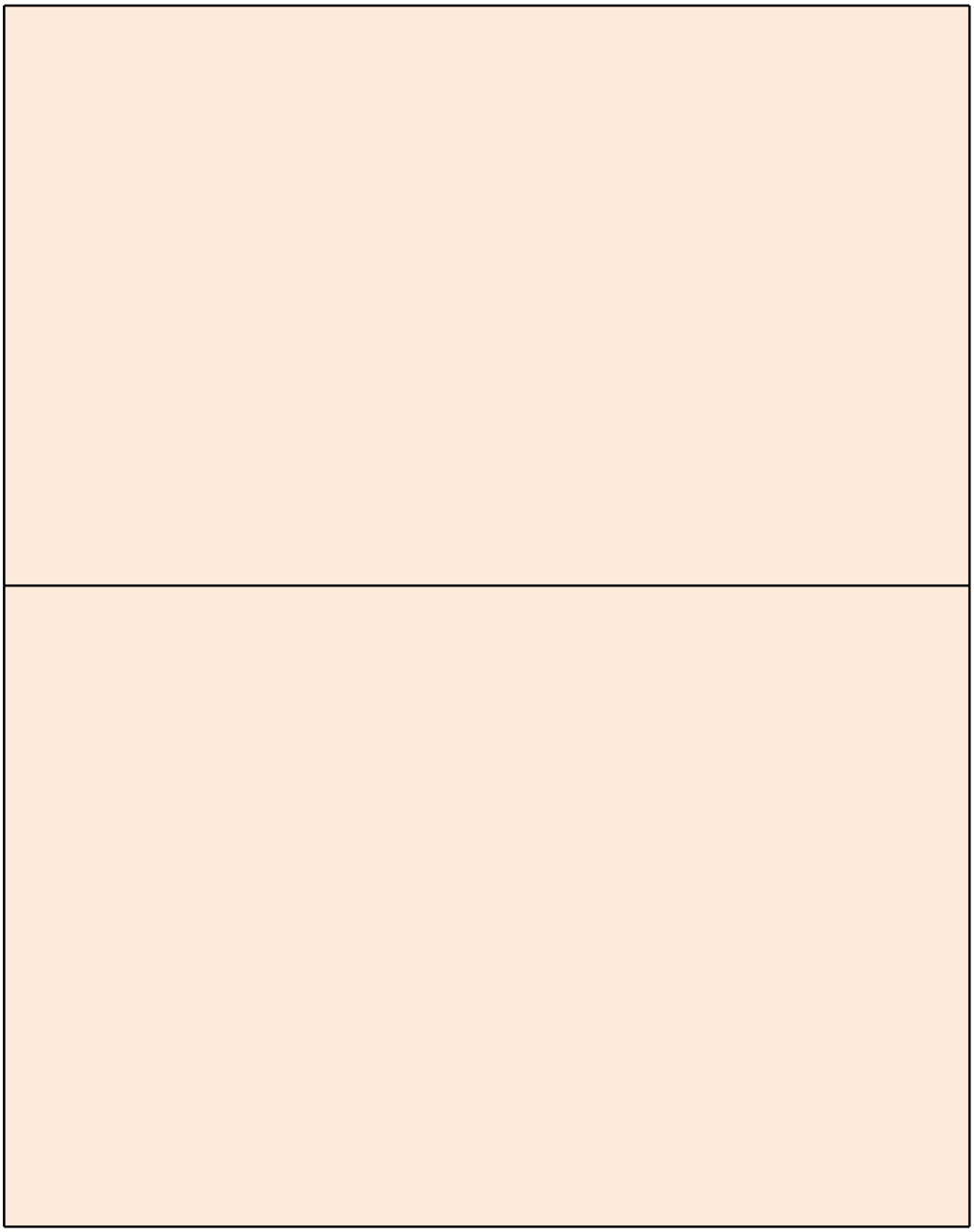
Kulkuneuvon määritelmä tulisi nostaa Luku 1 2 § "Määritelmät" Alle, eikä kirjoitettaa tässä kohtaa perustelumuistioon.

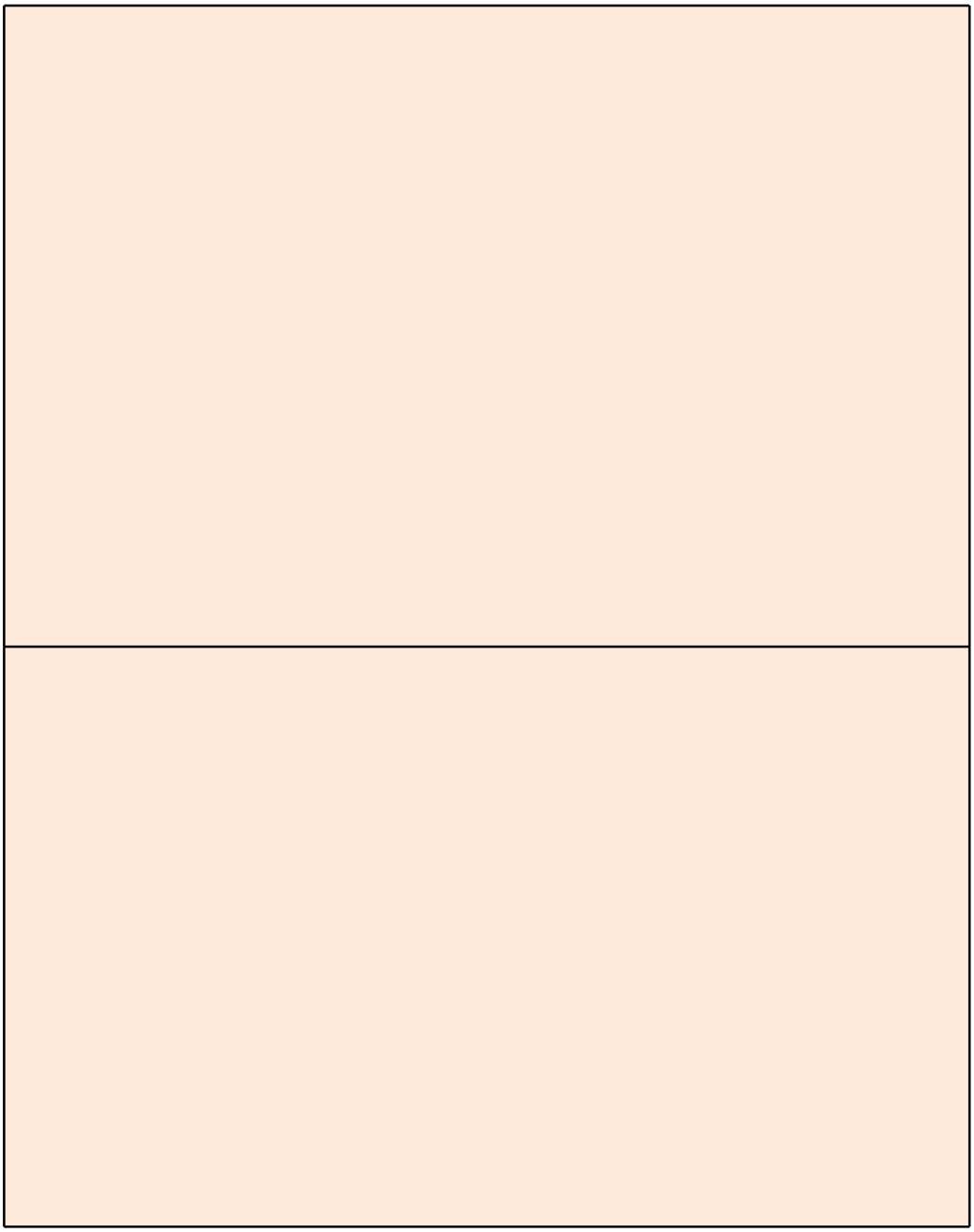


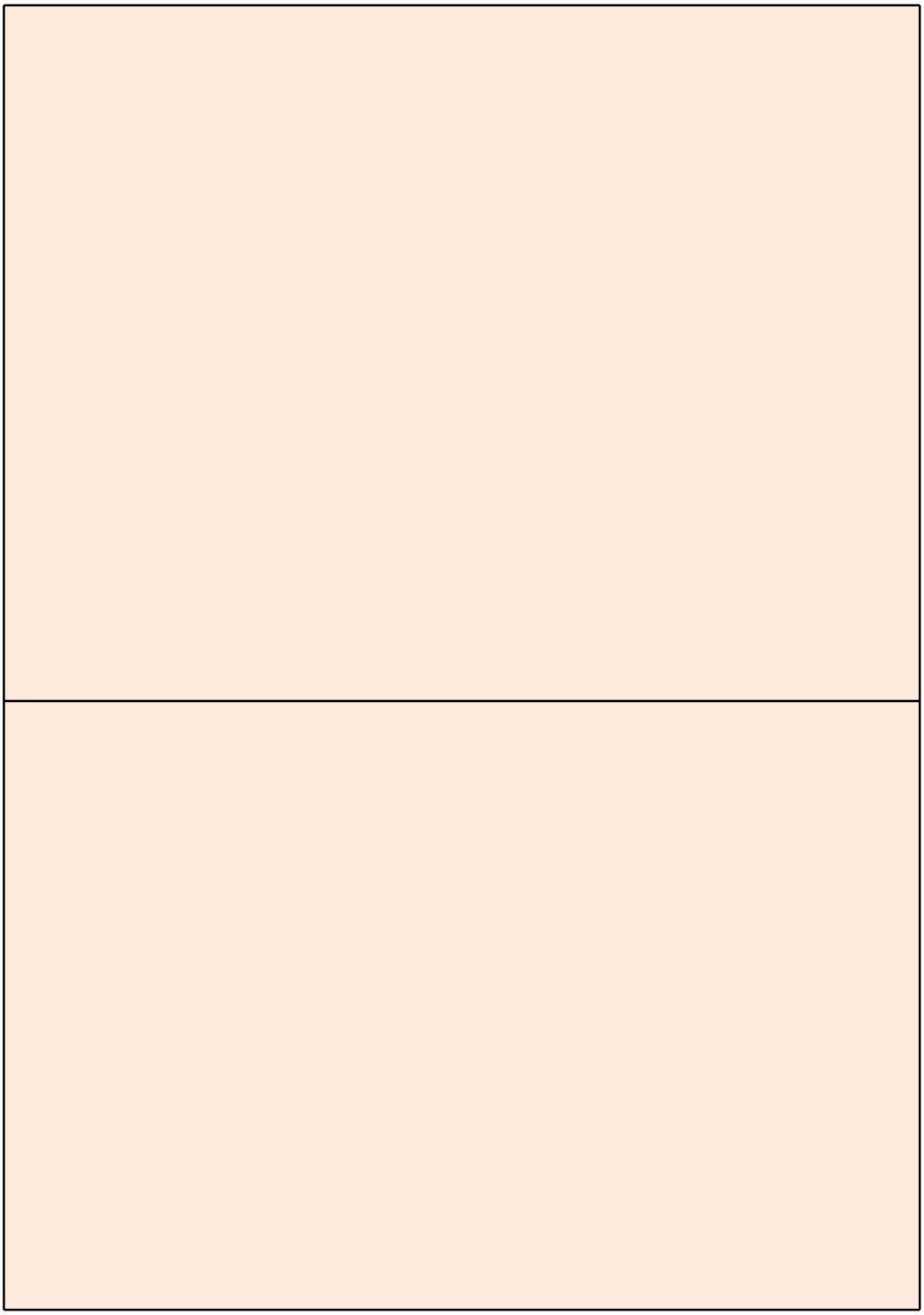


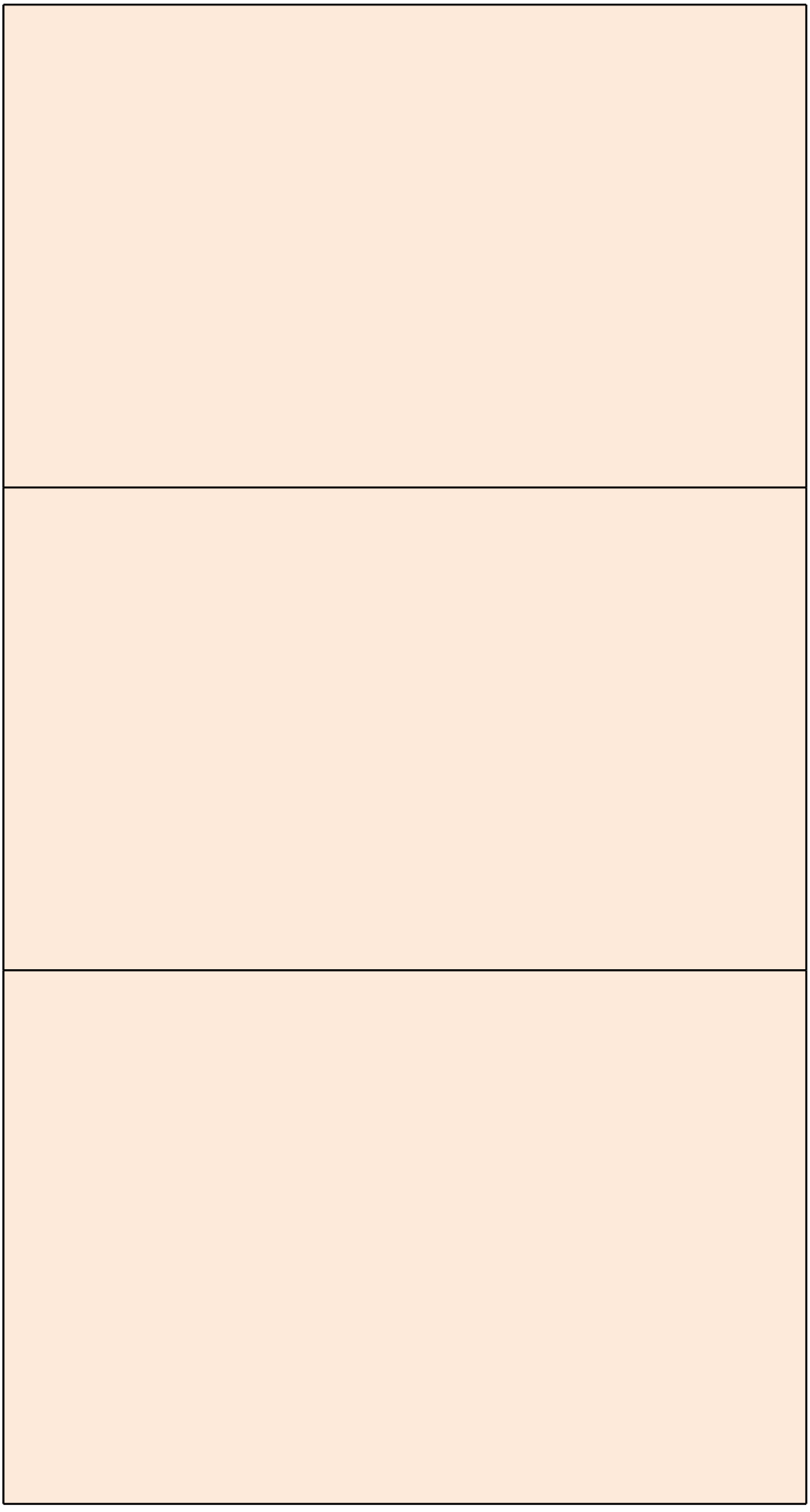


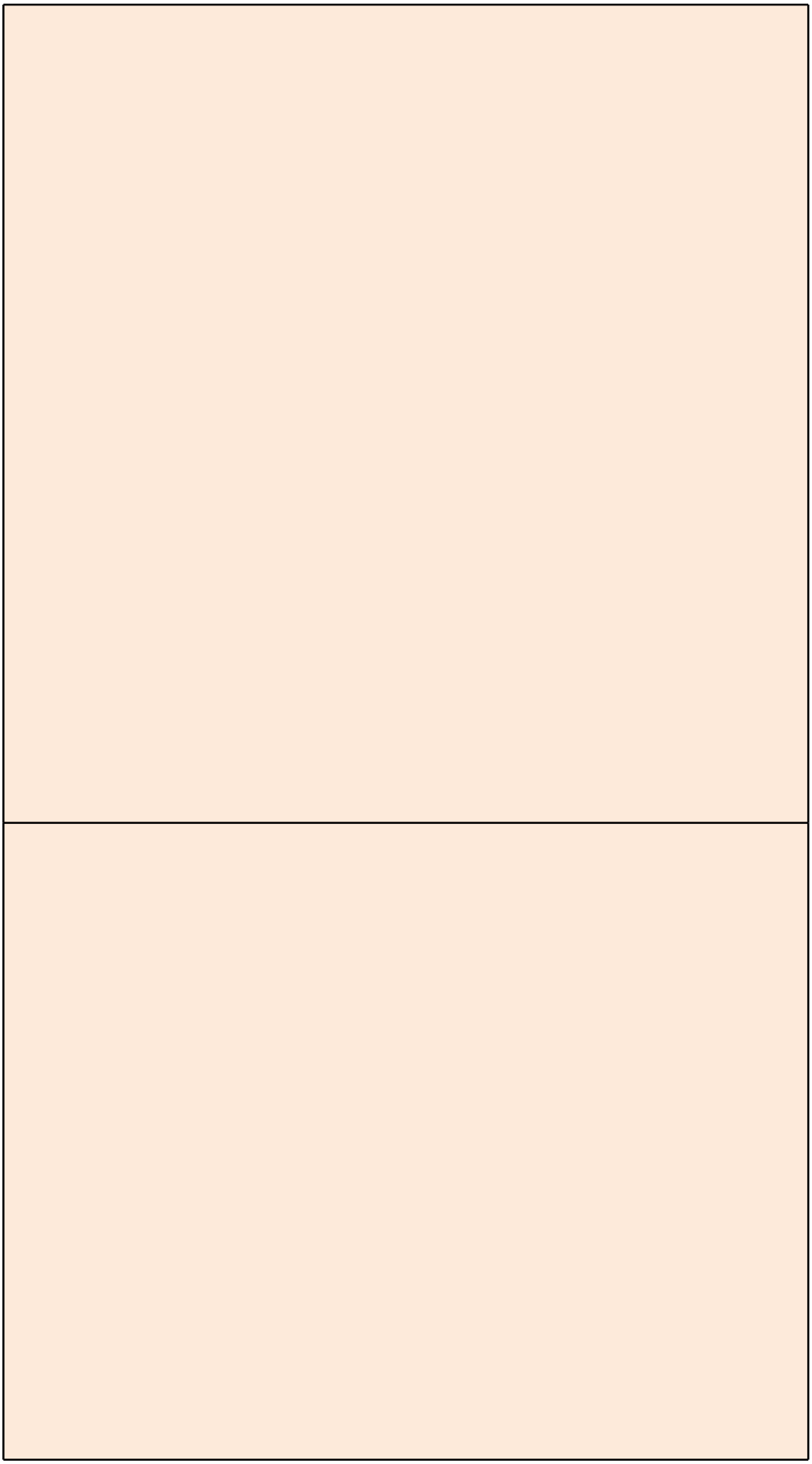


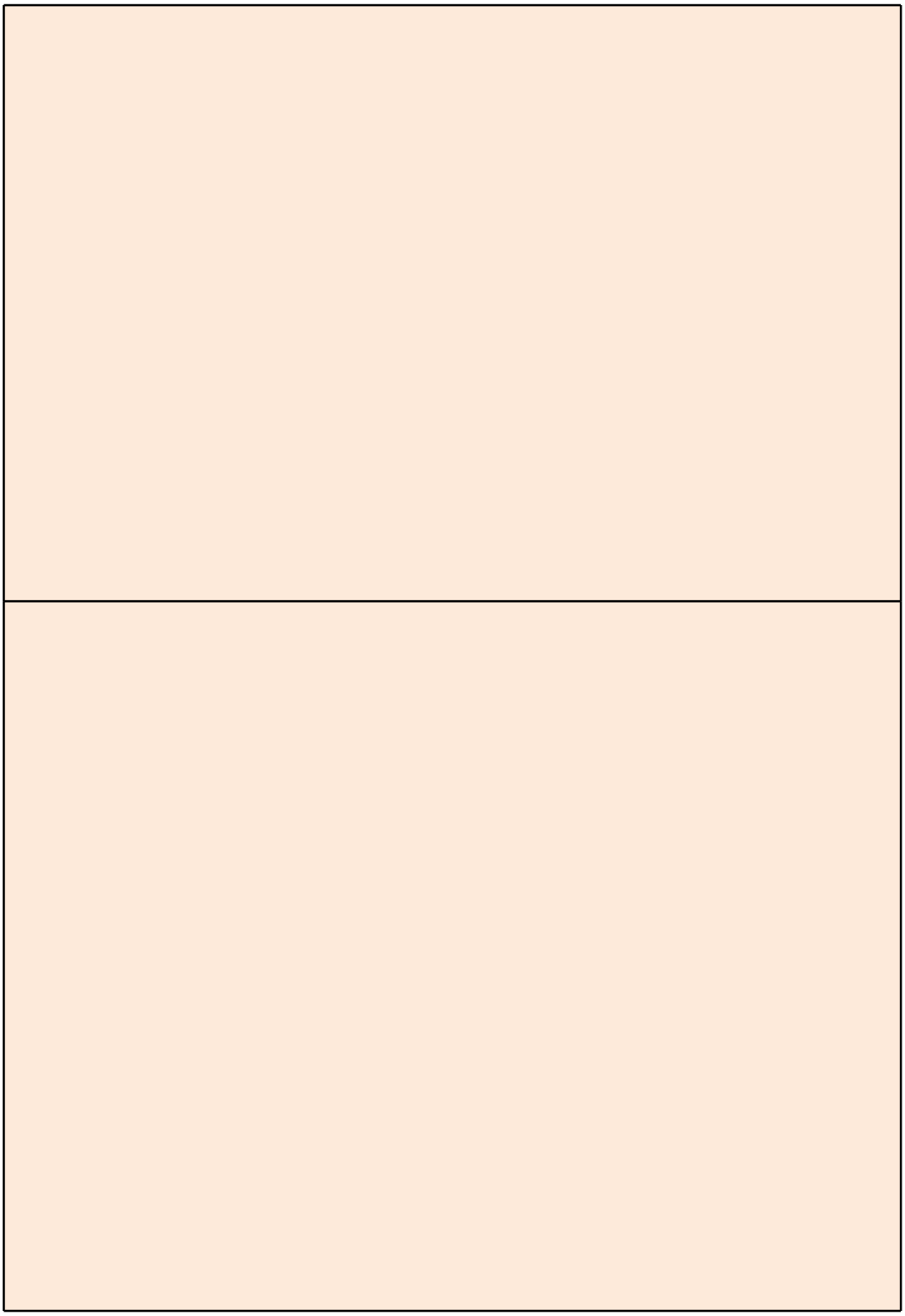


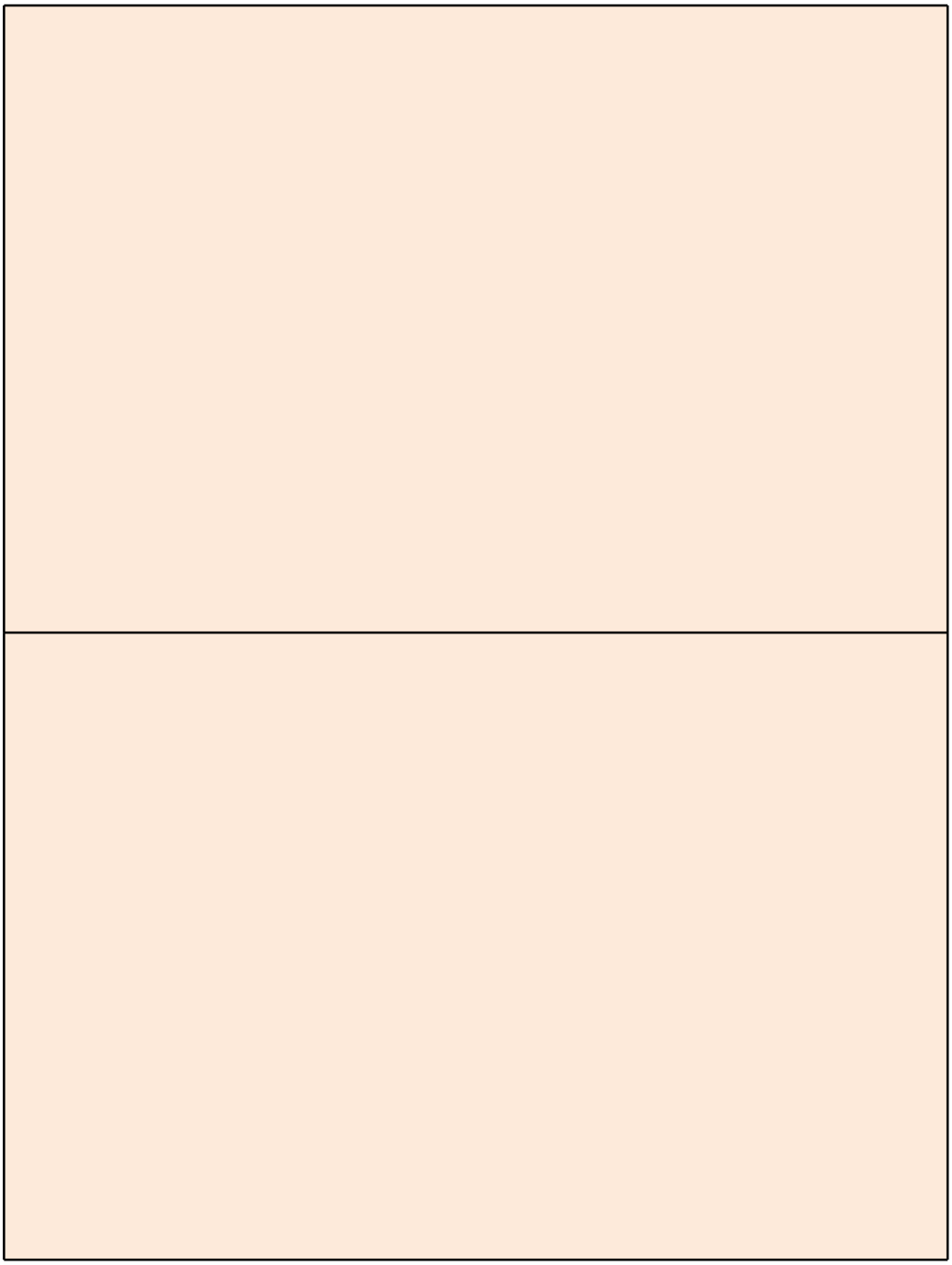


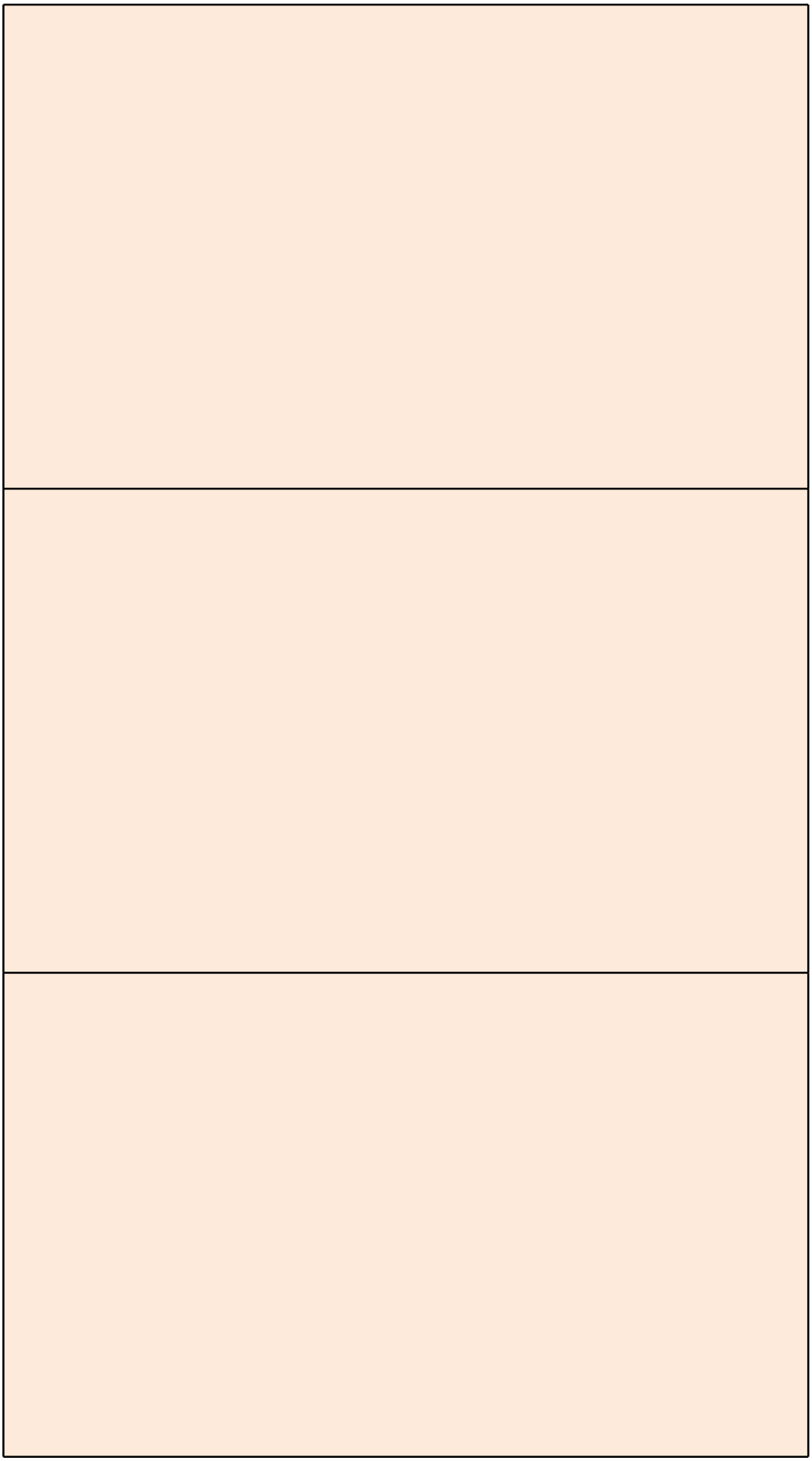


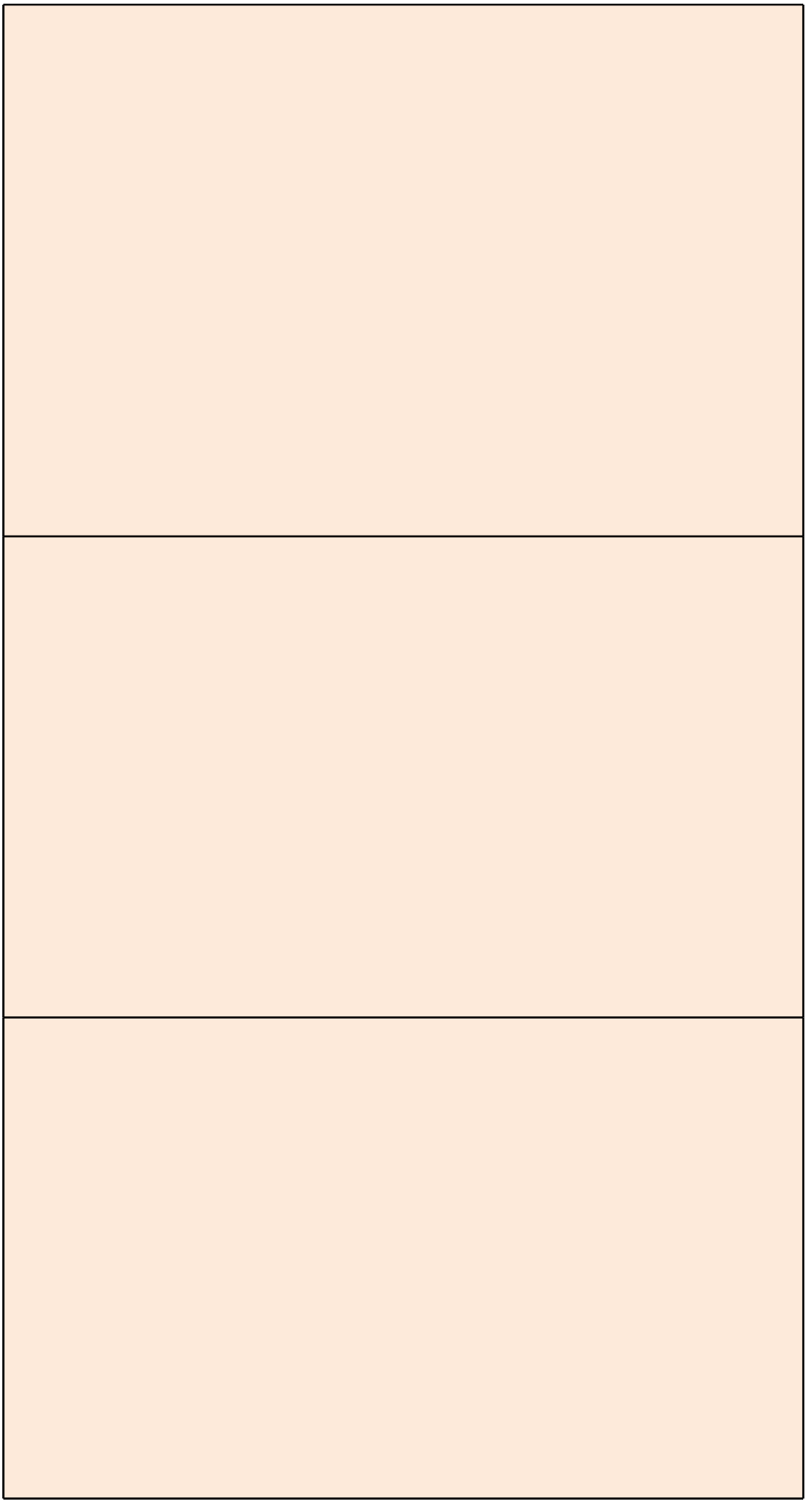


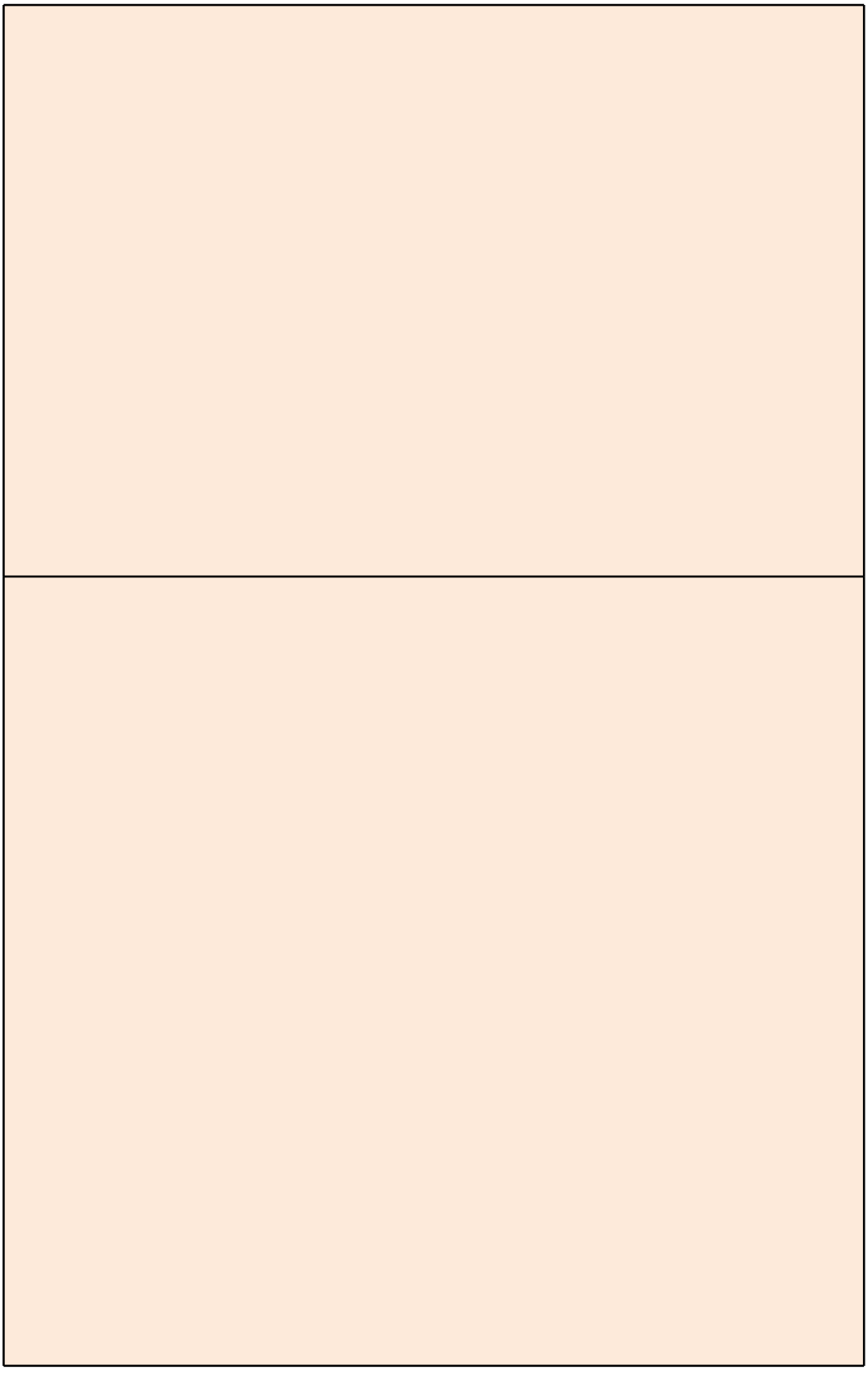


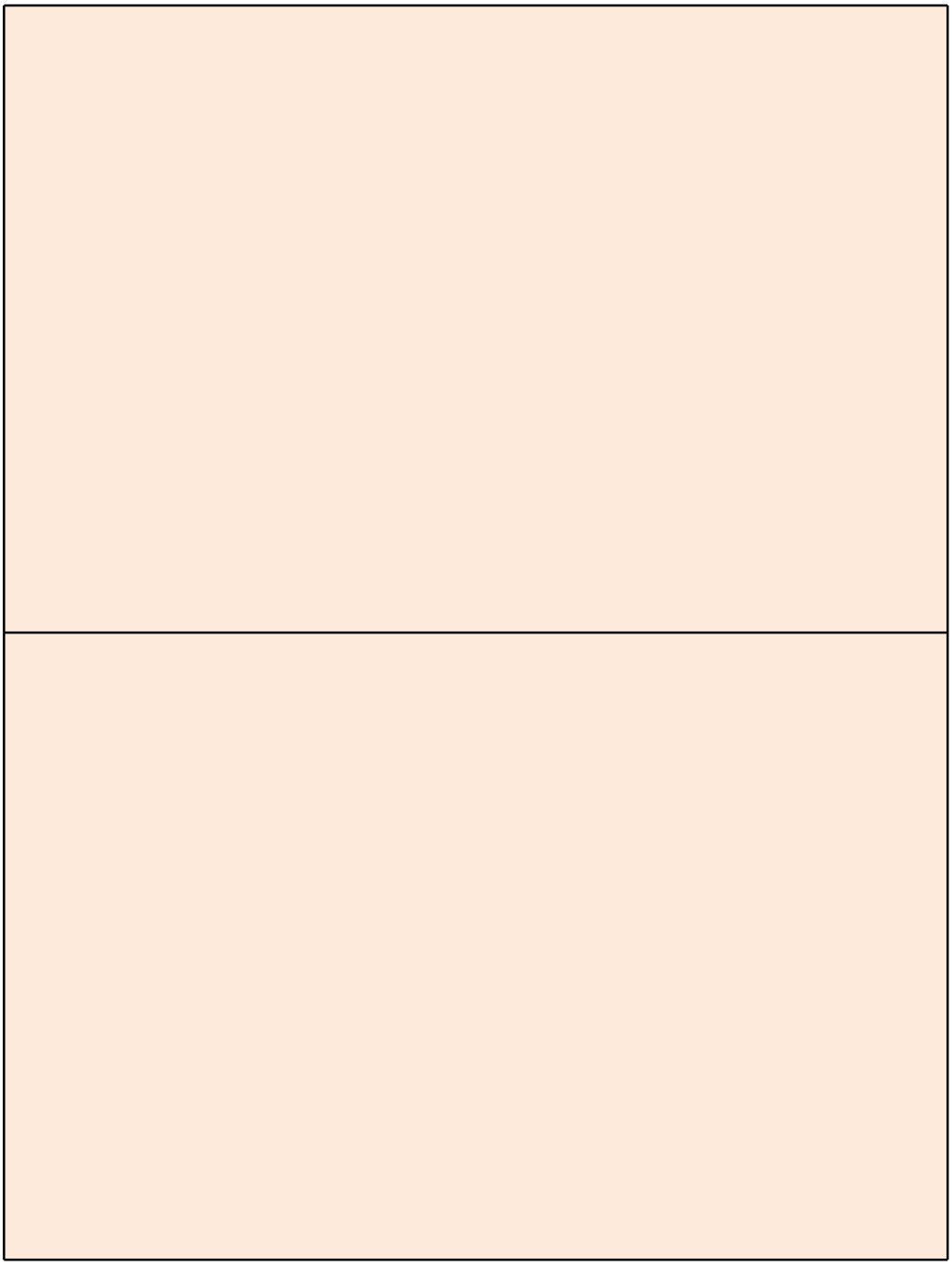


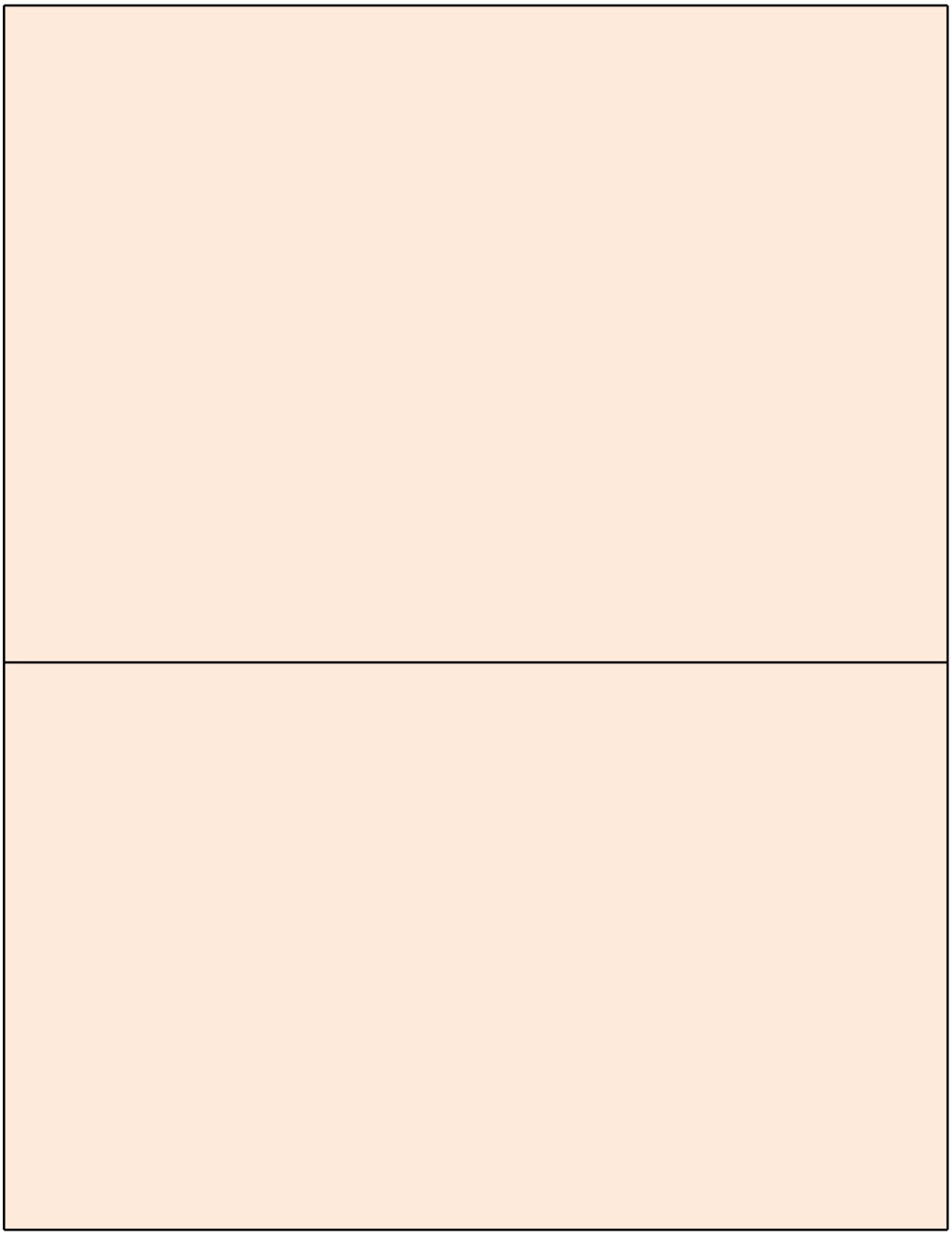


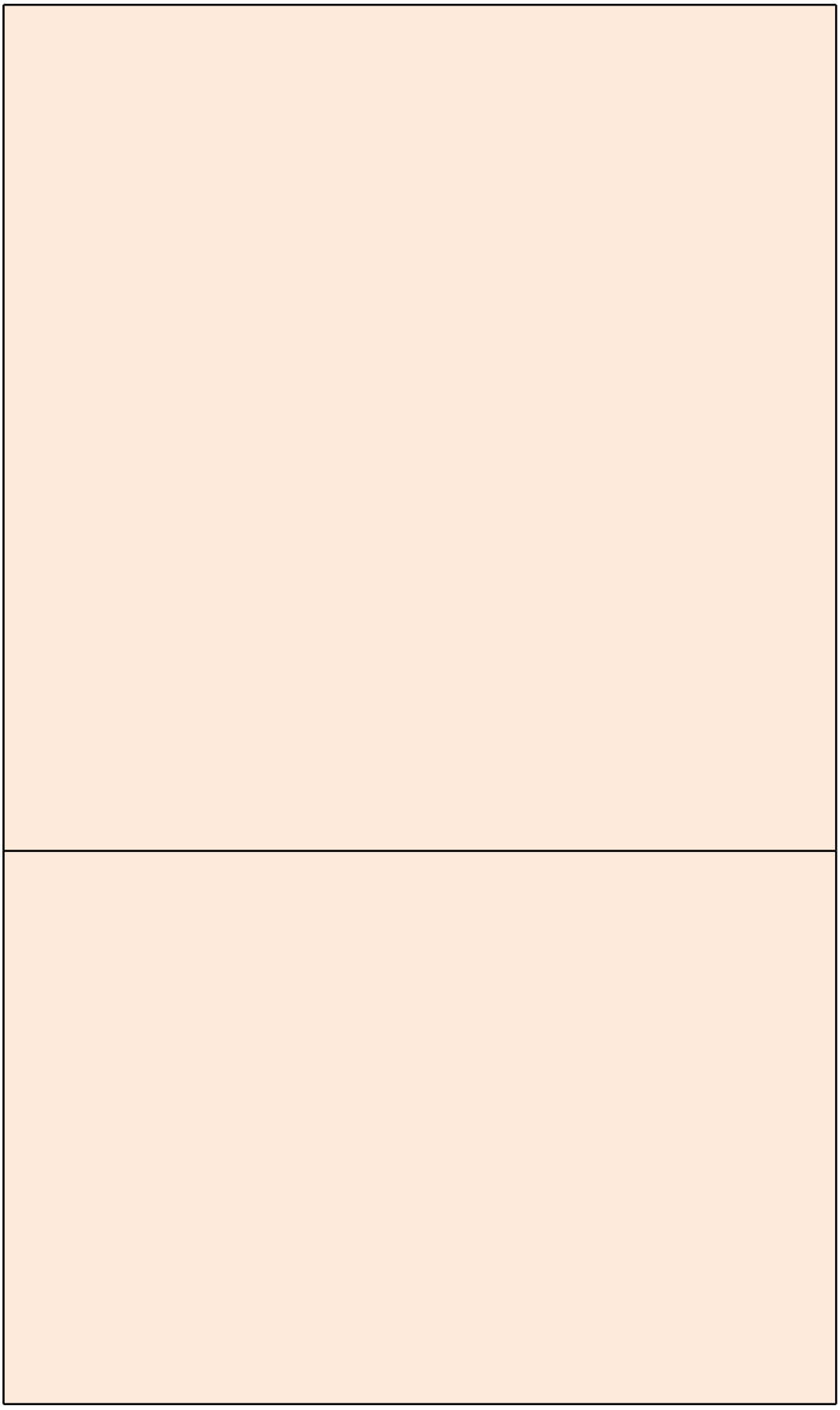


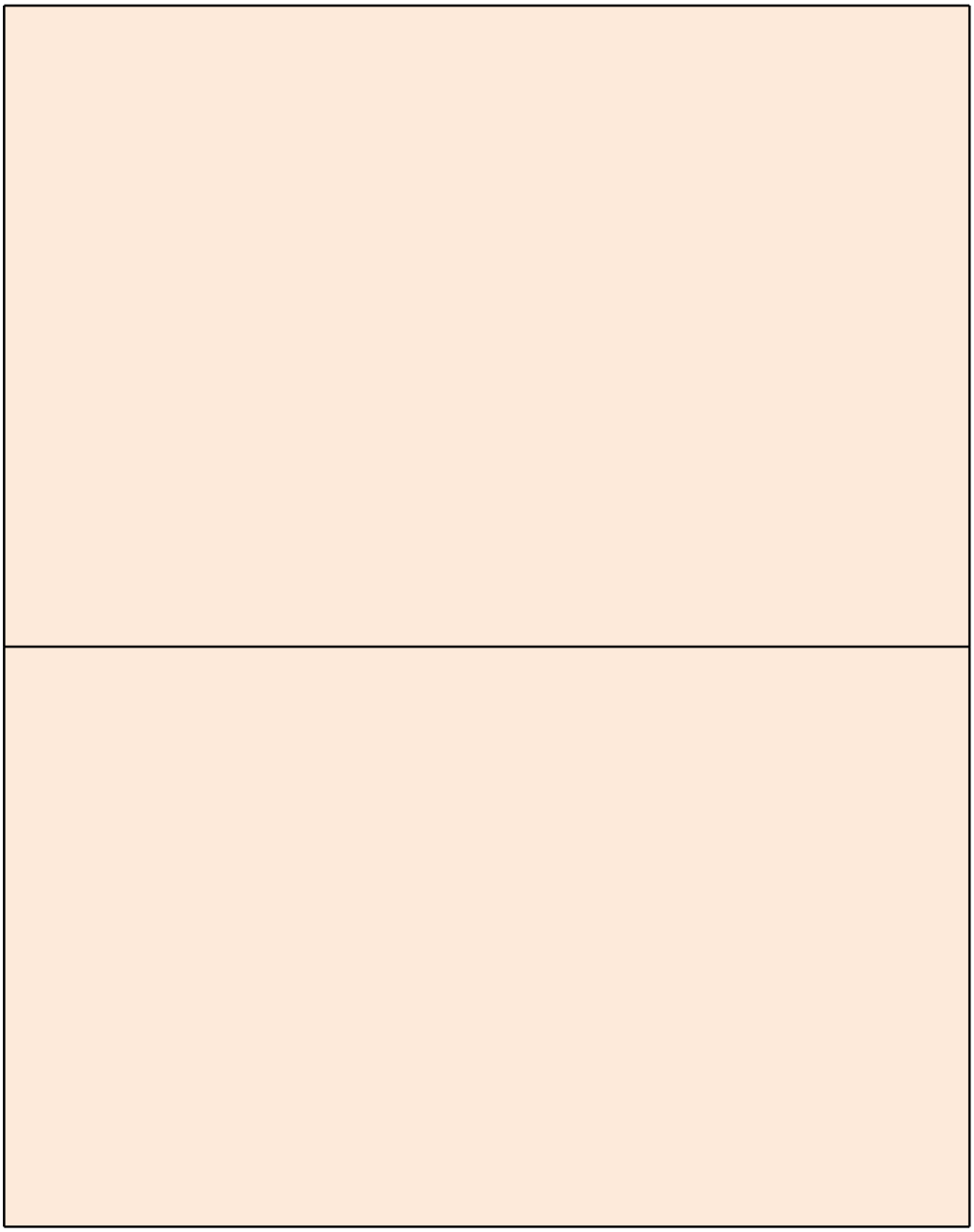


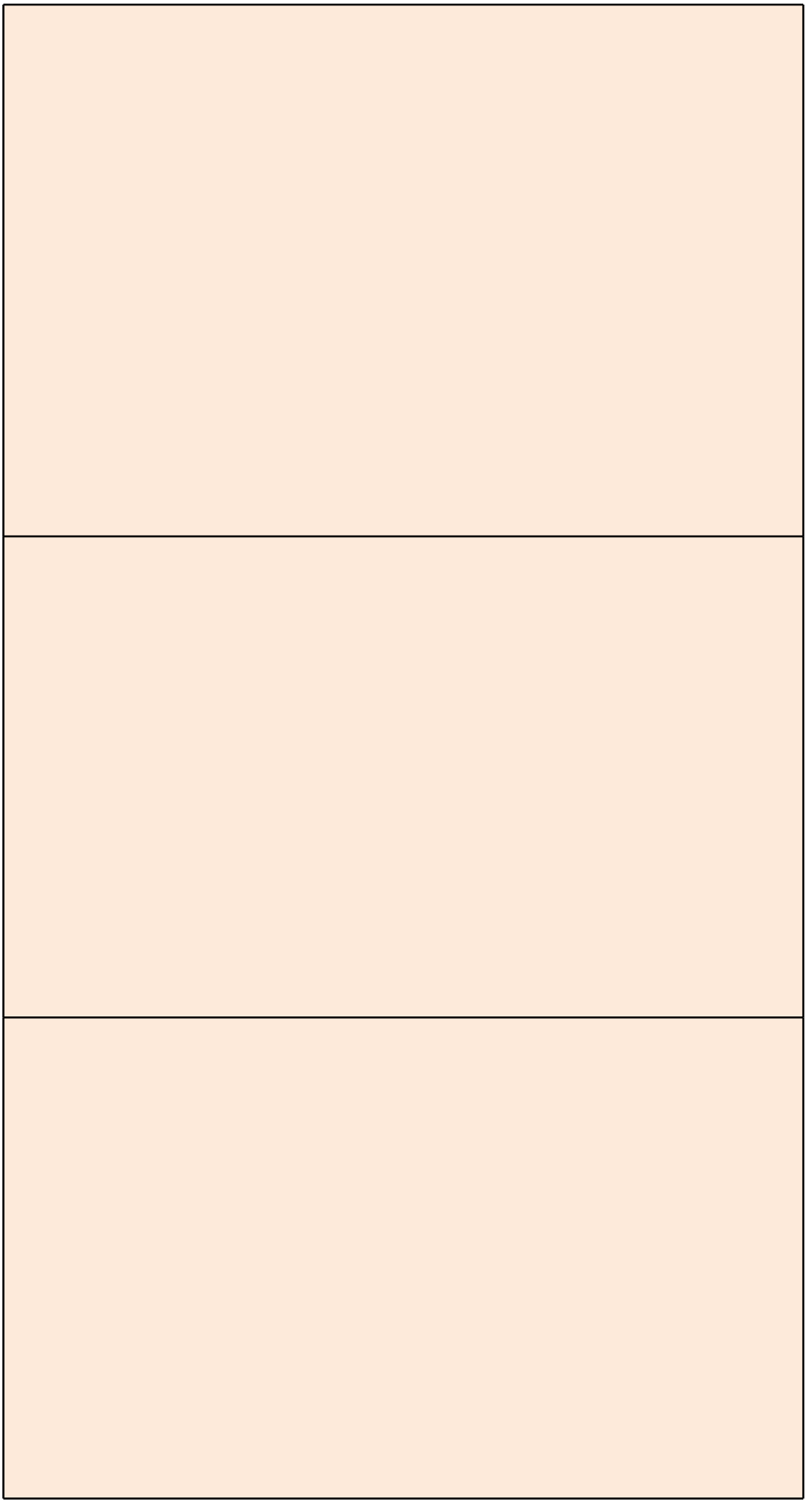


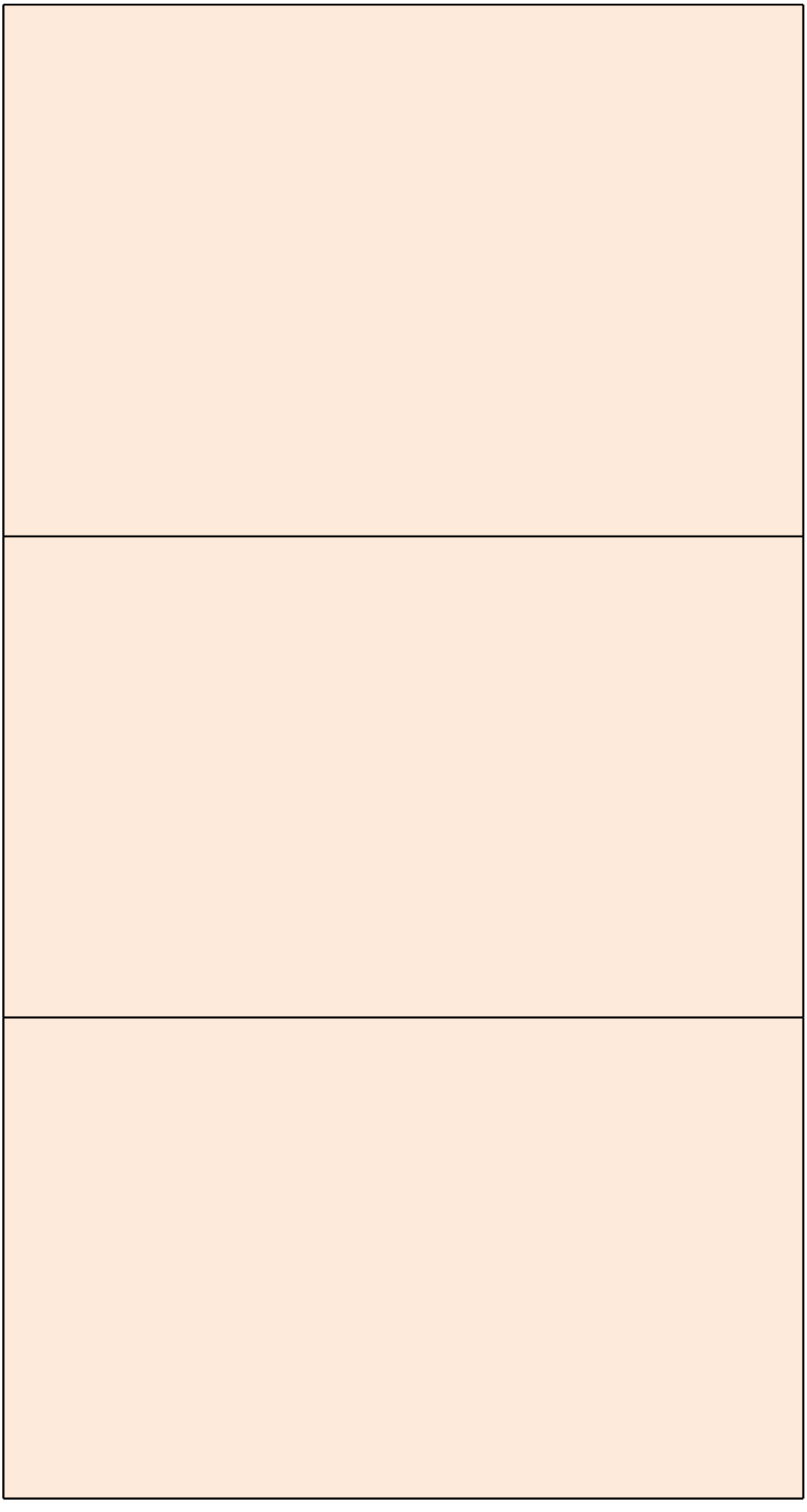


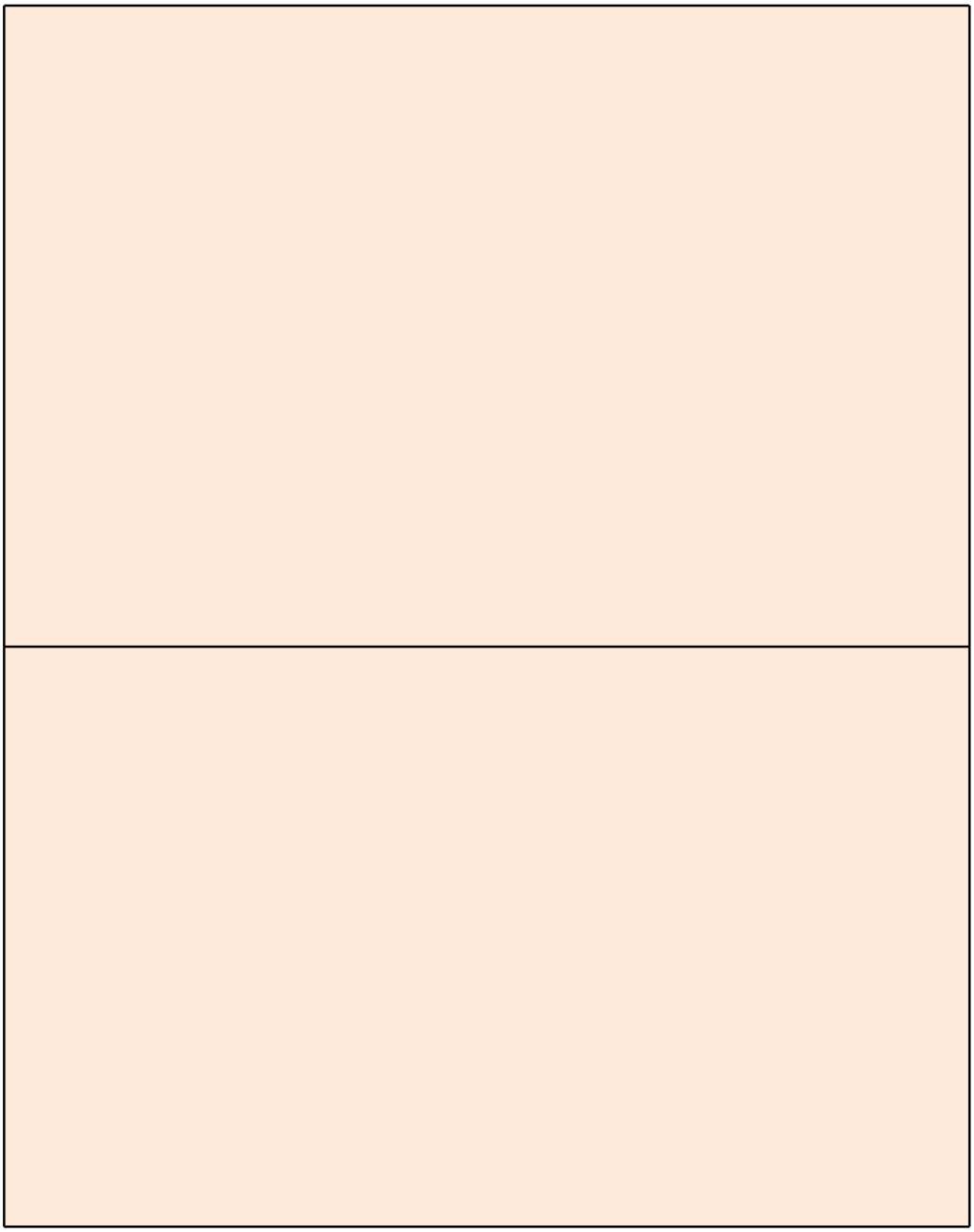


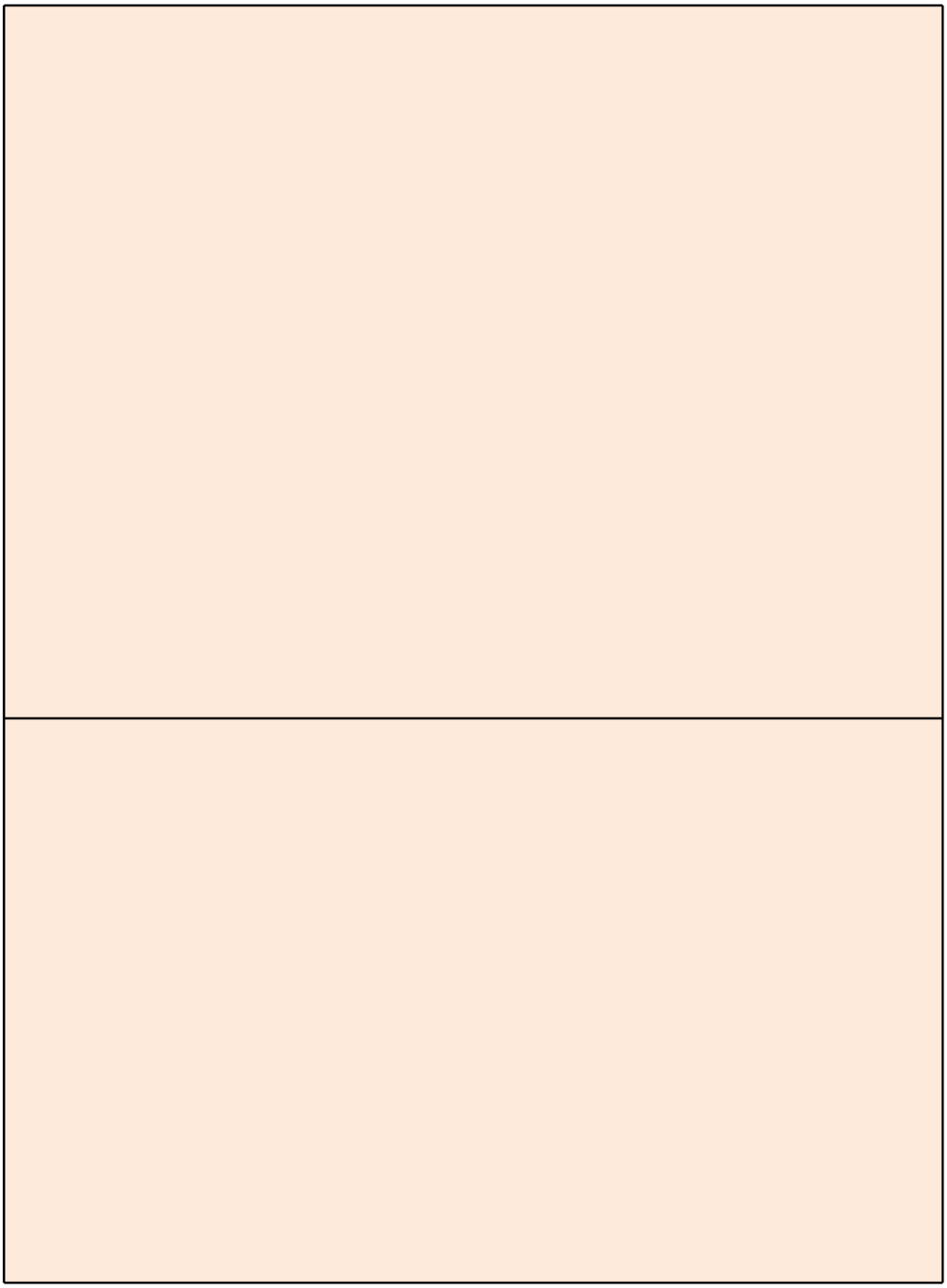


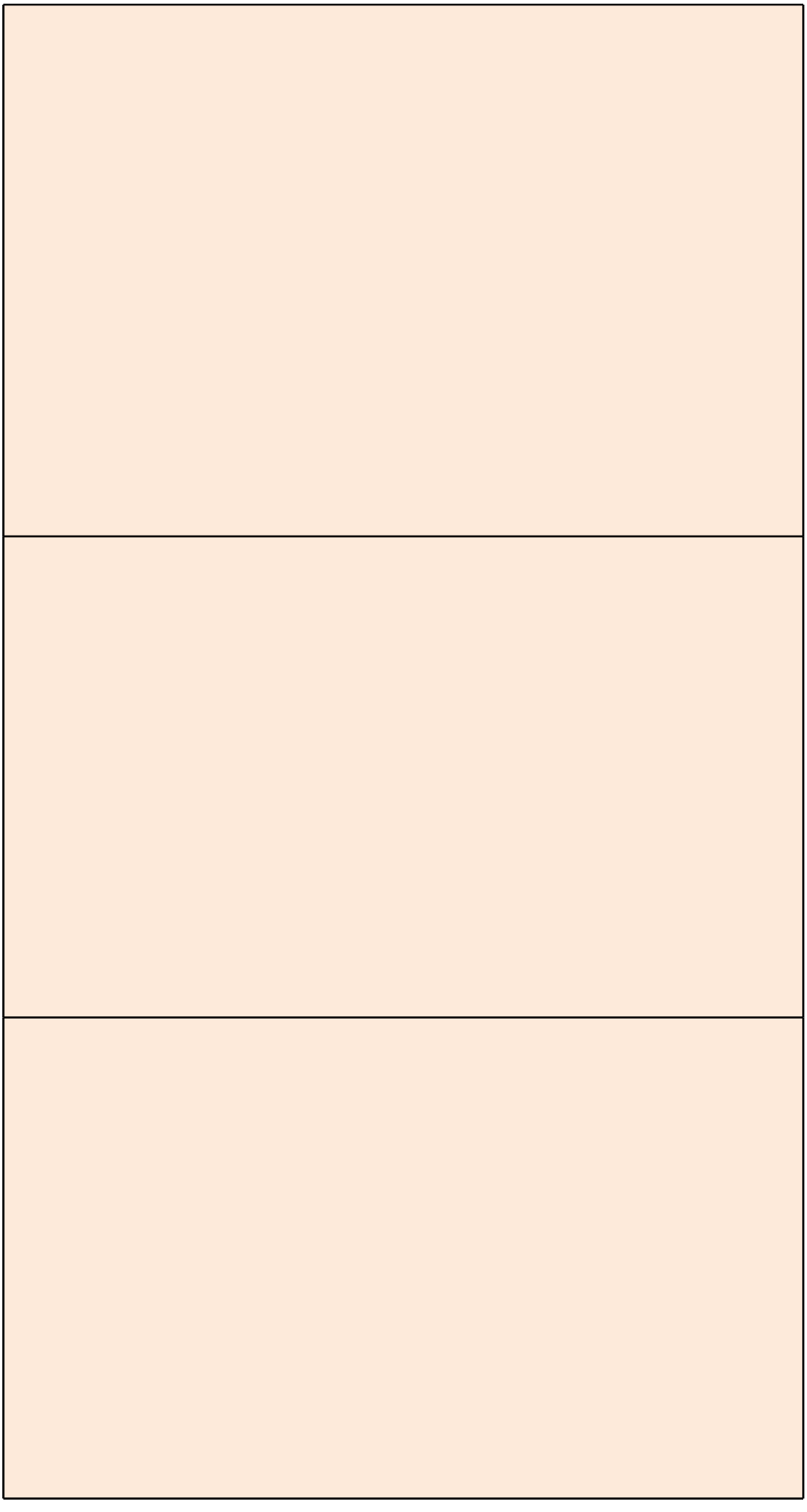


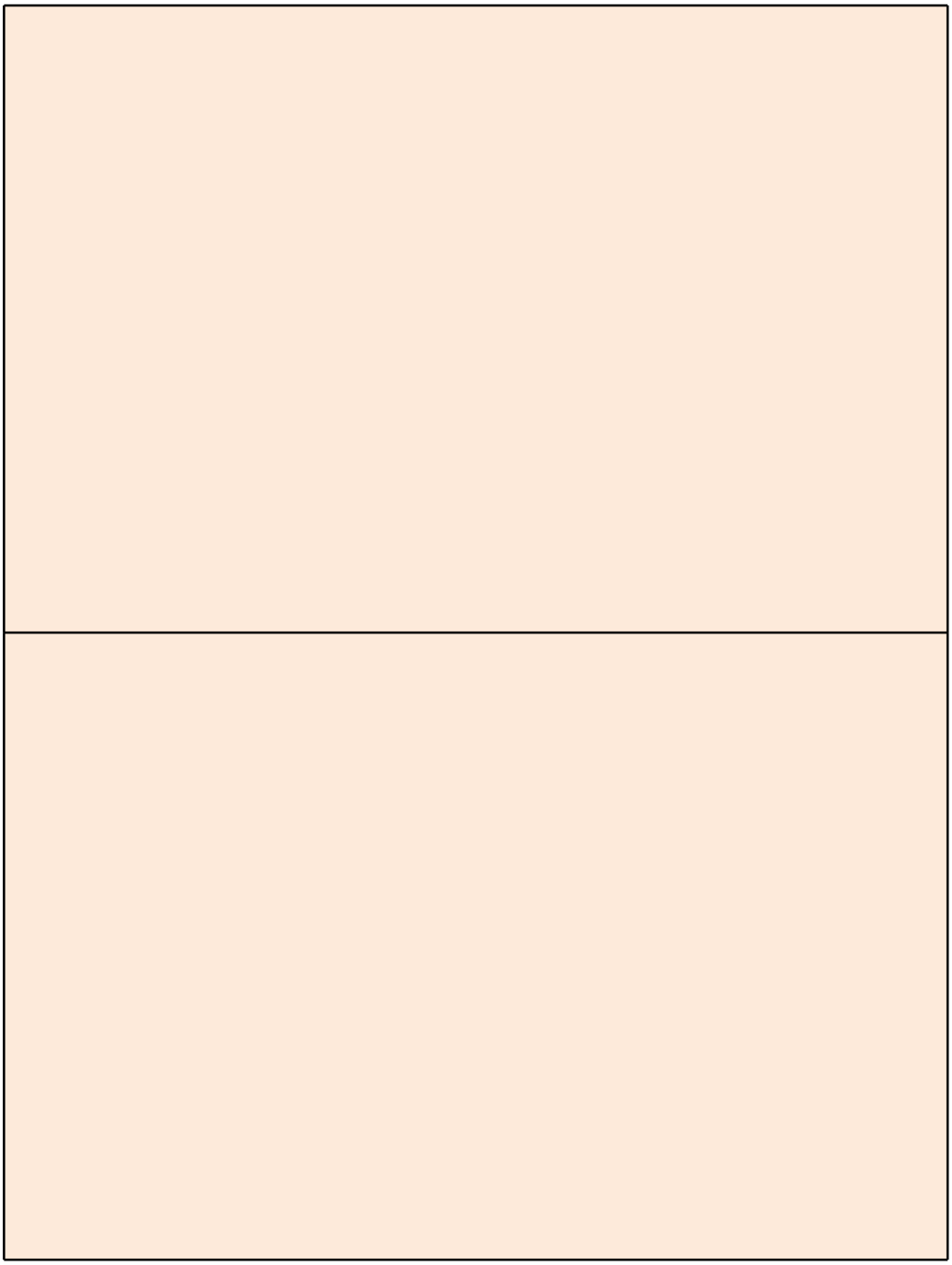


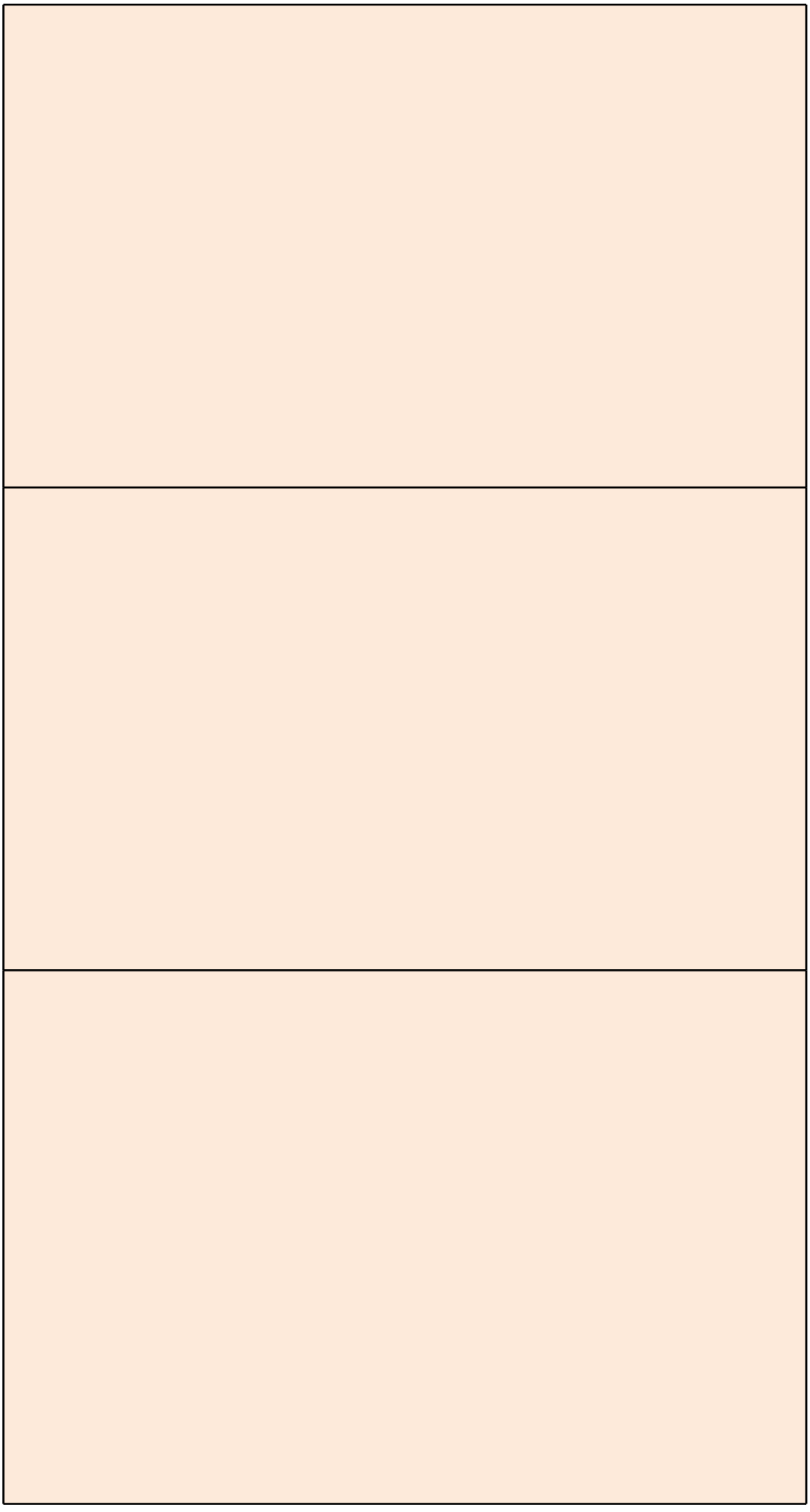


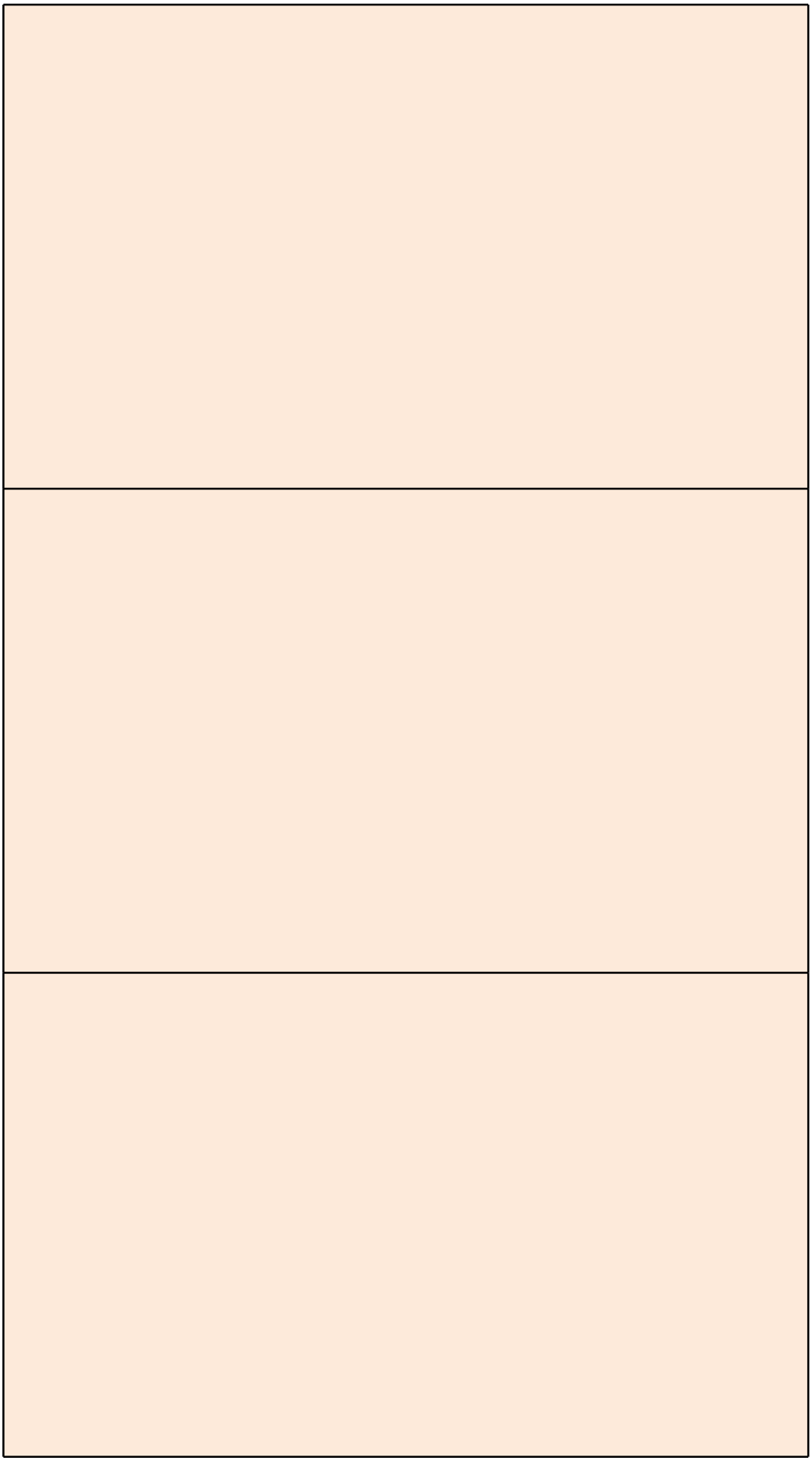


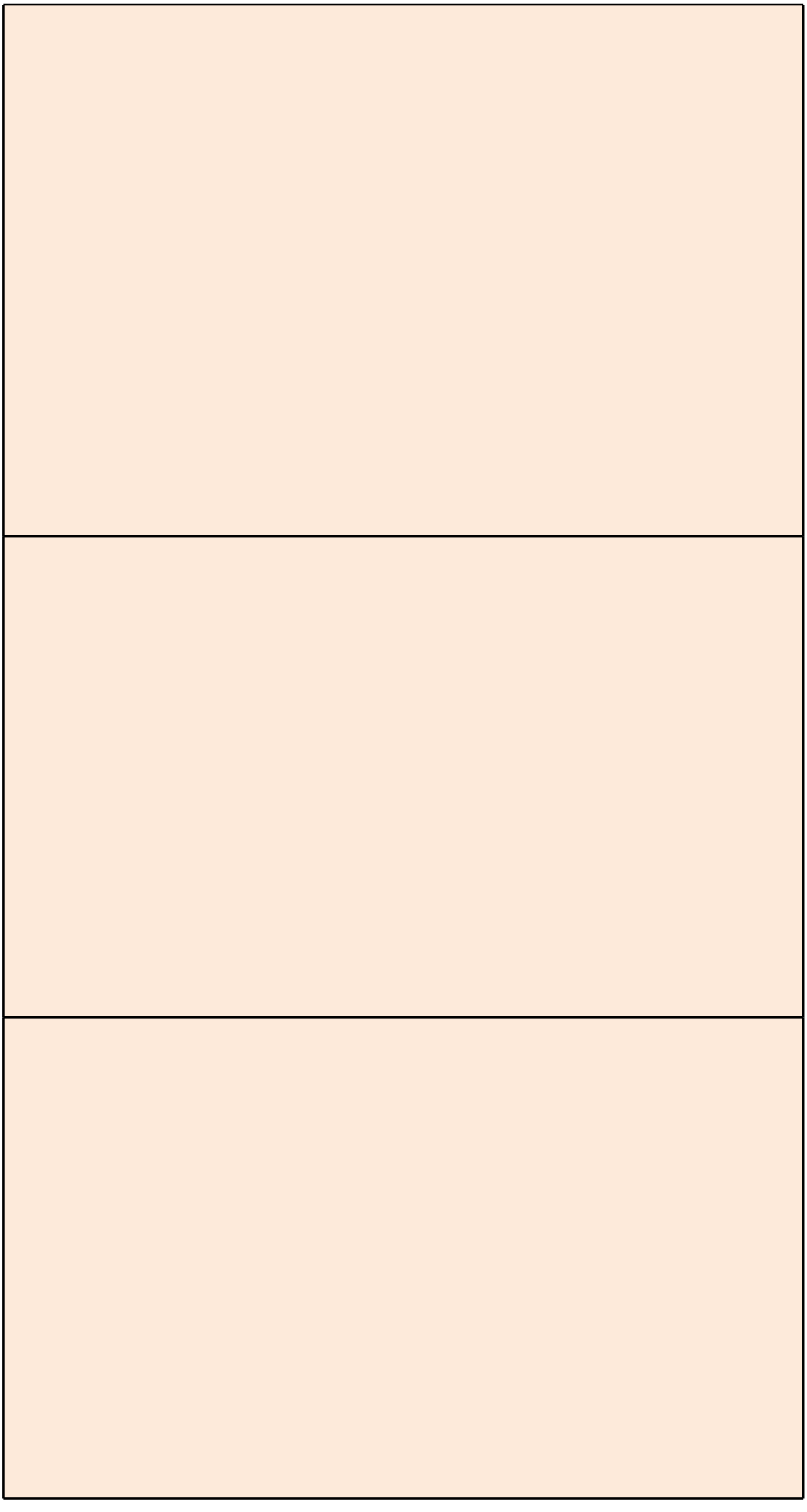


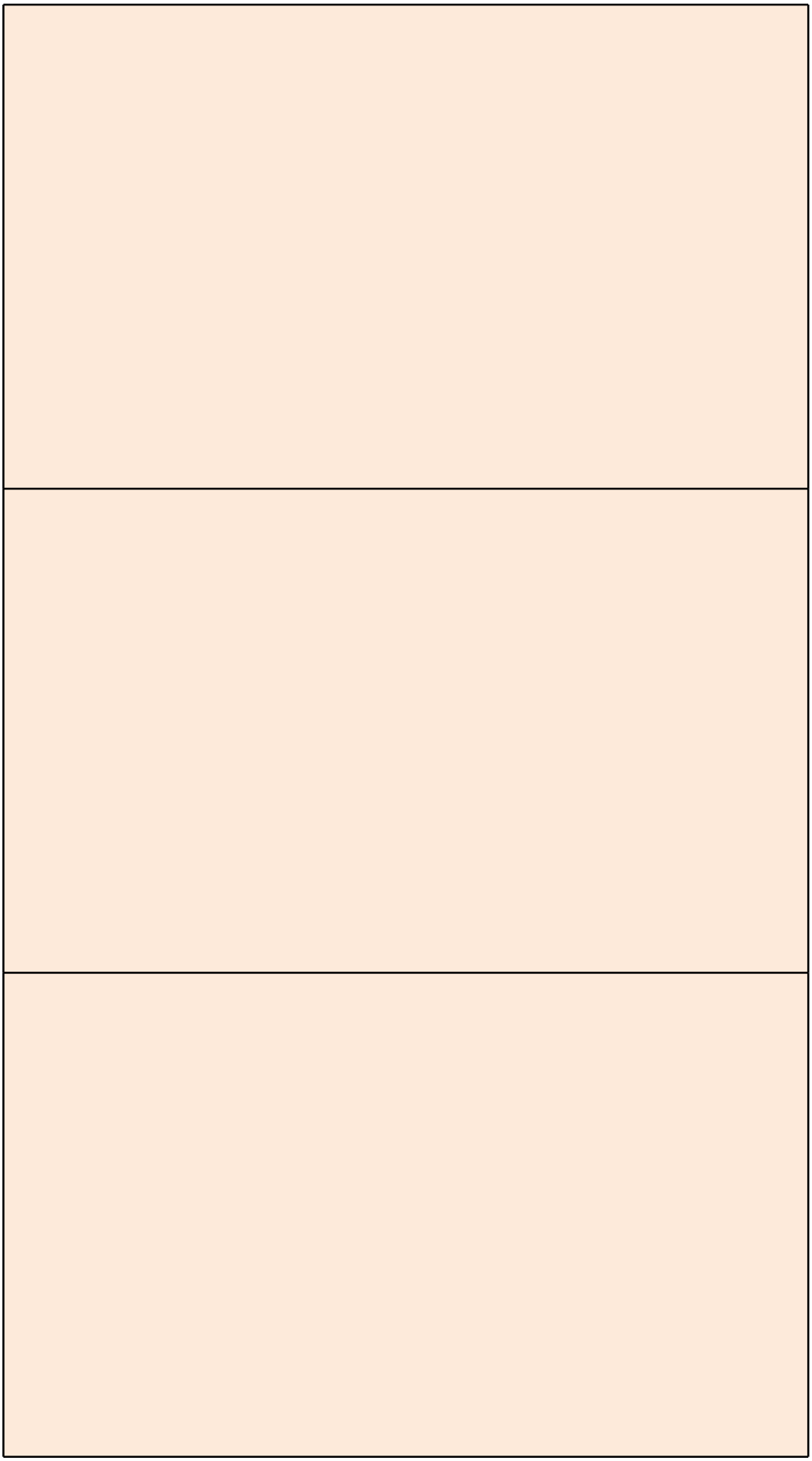


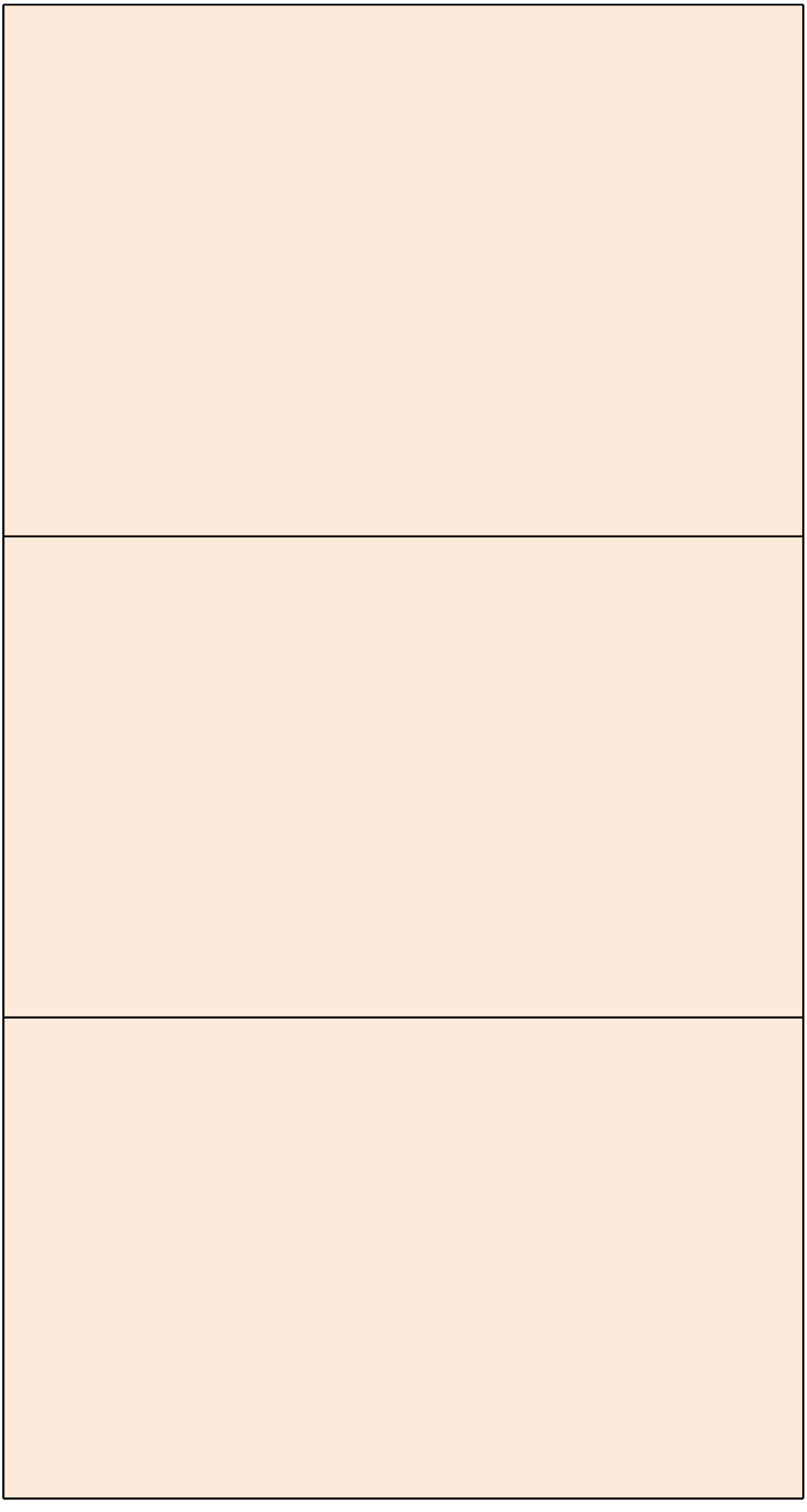


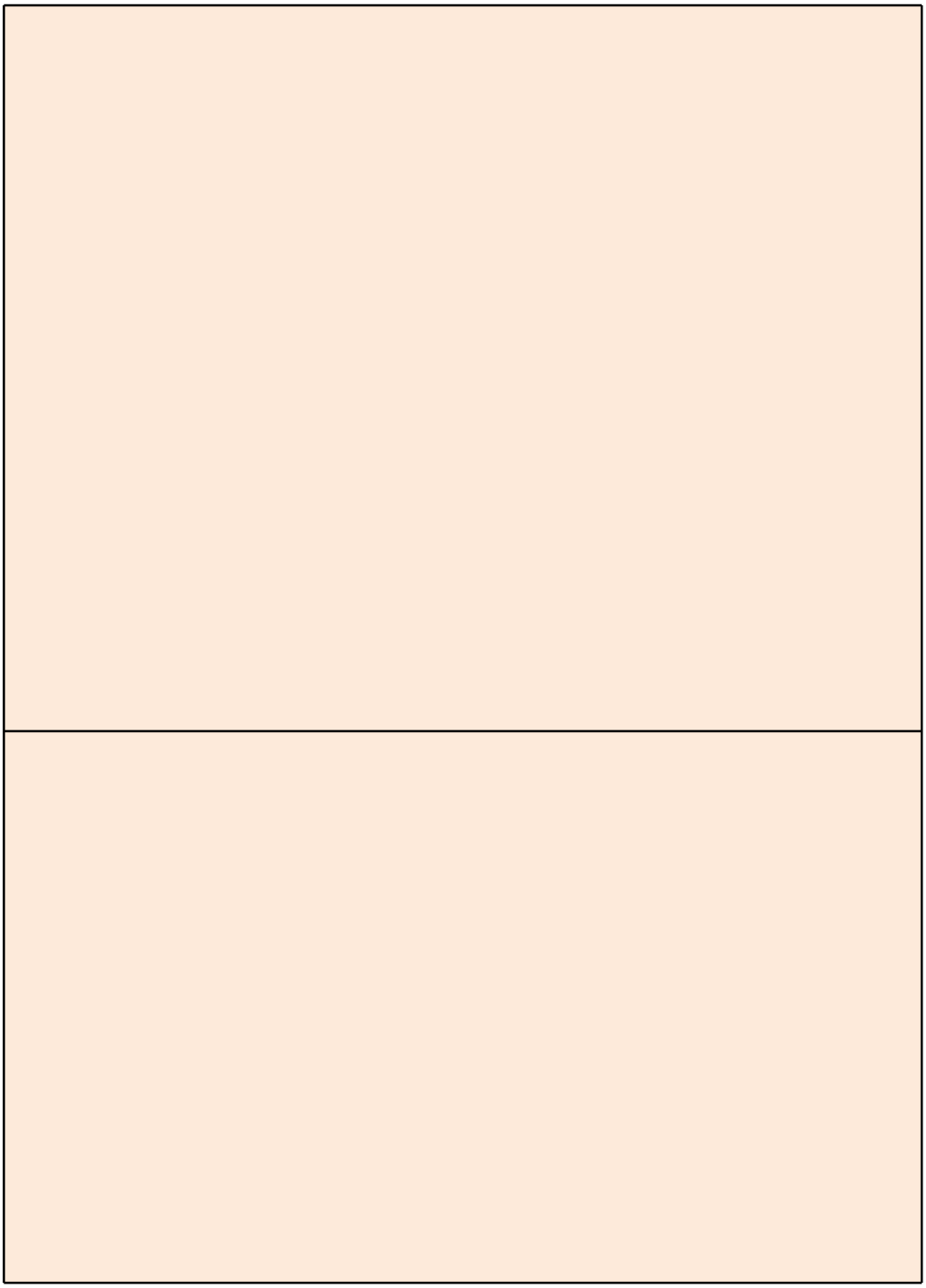


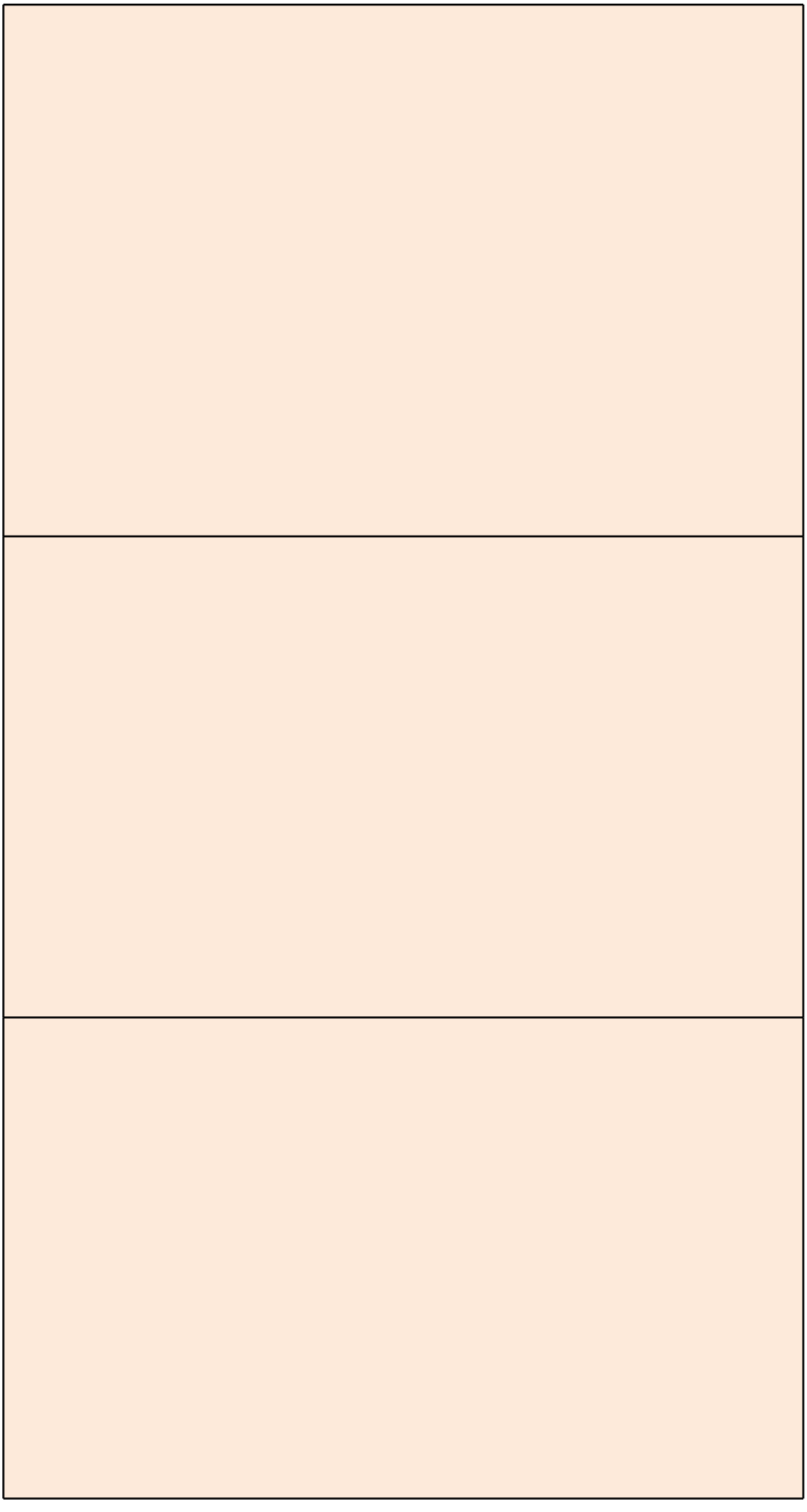


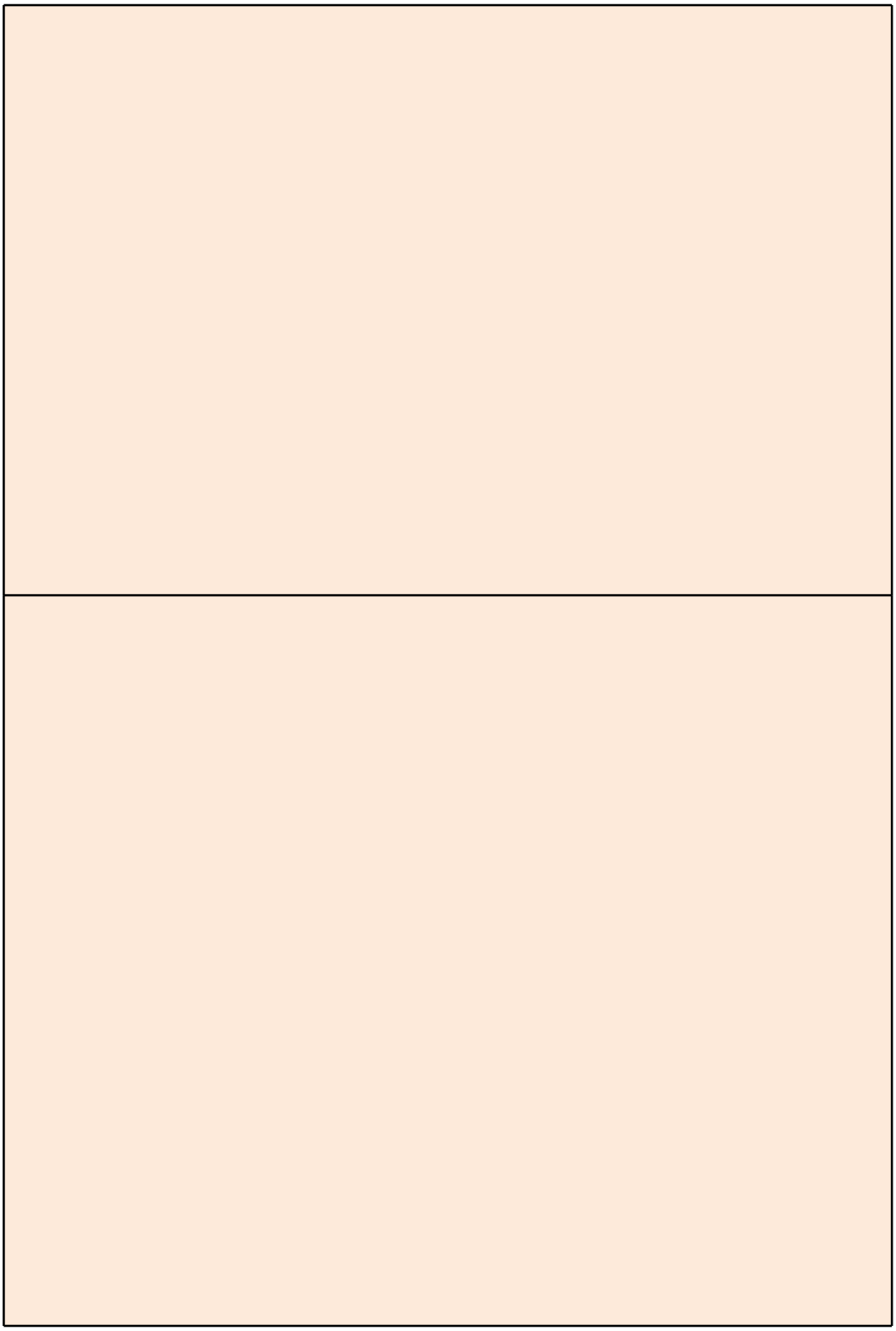


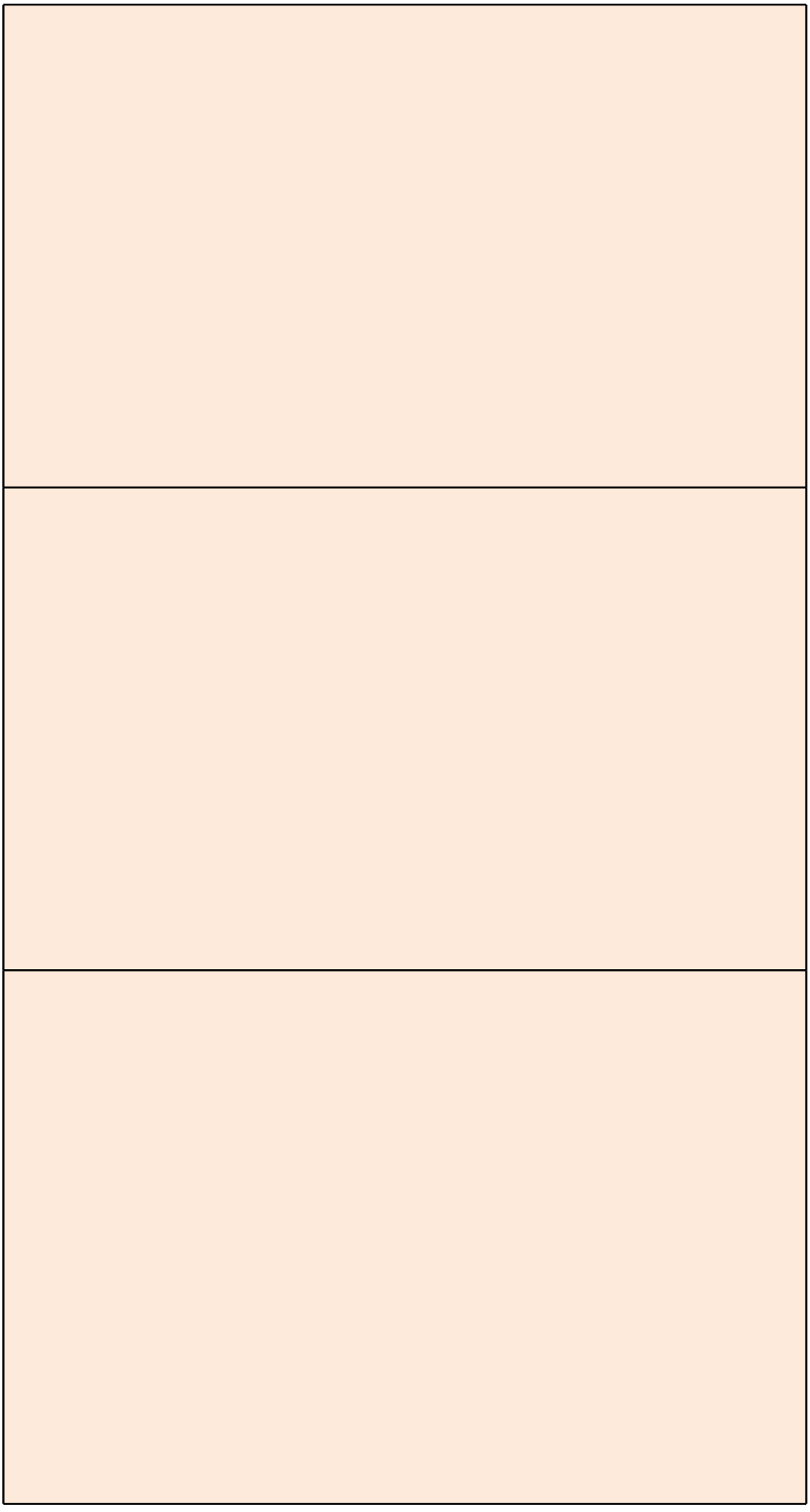


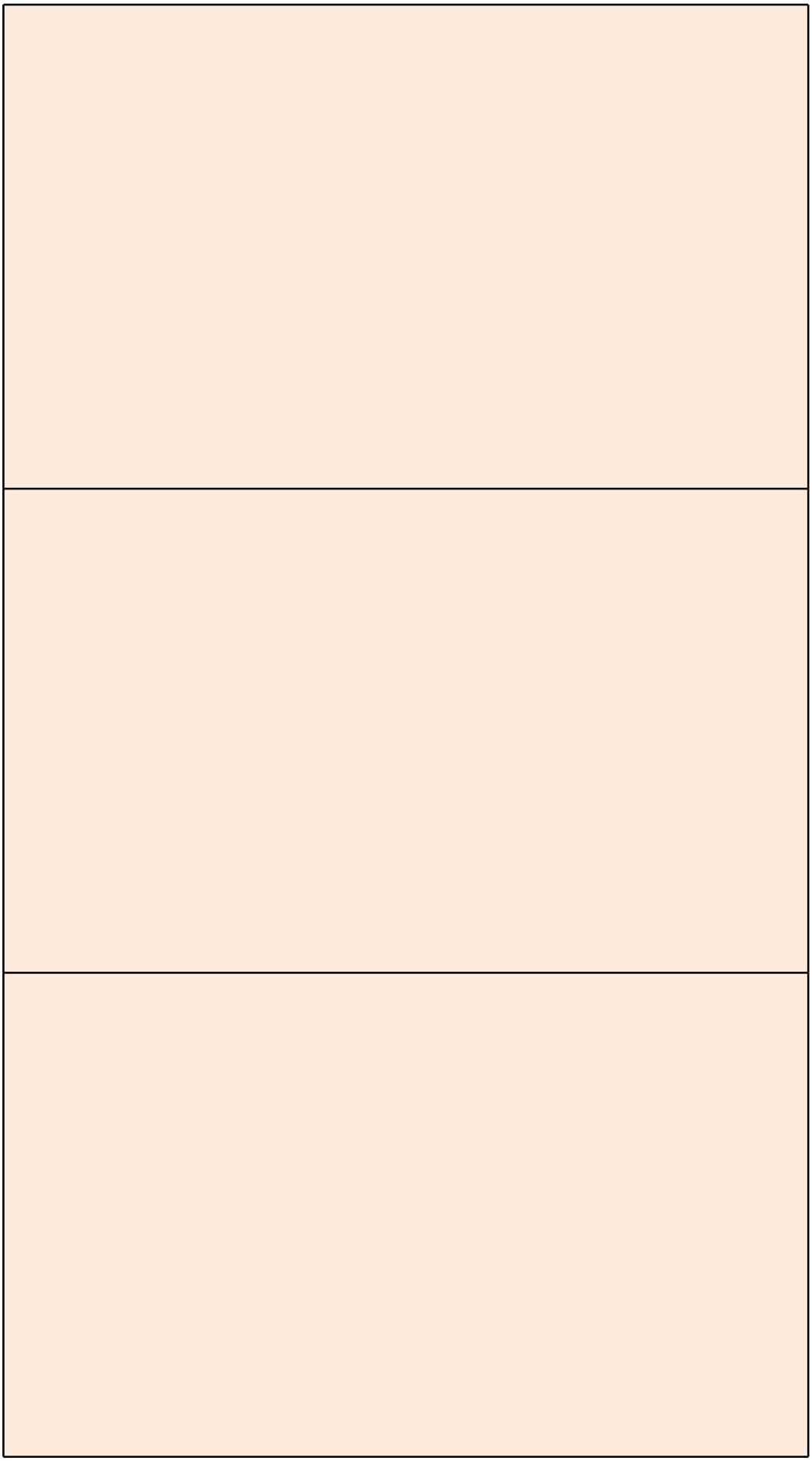


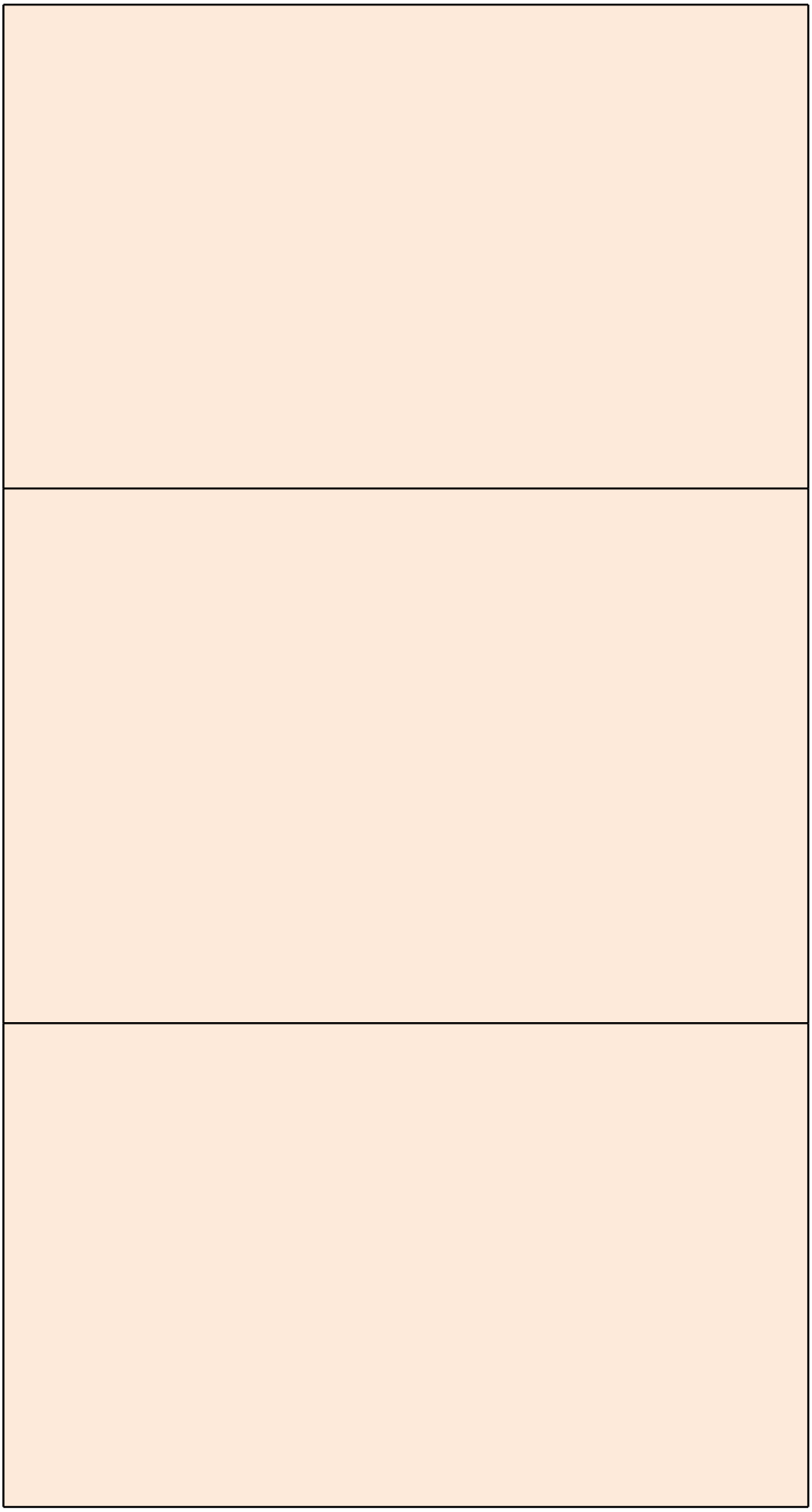


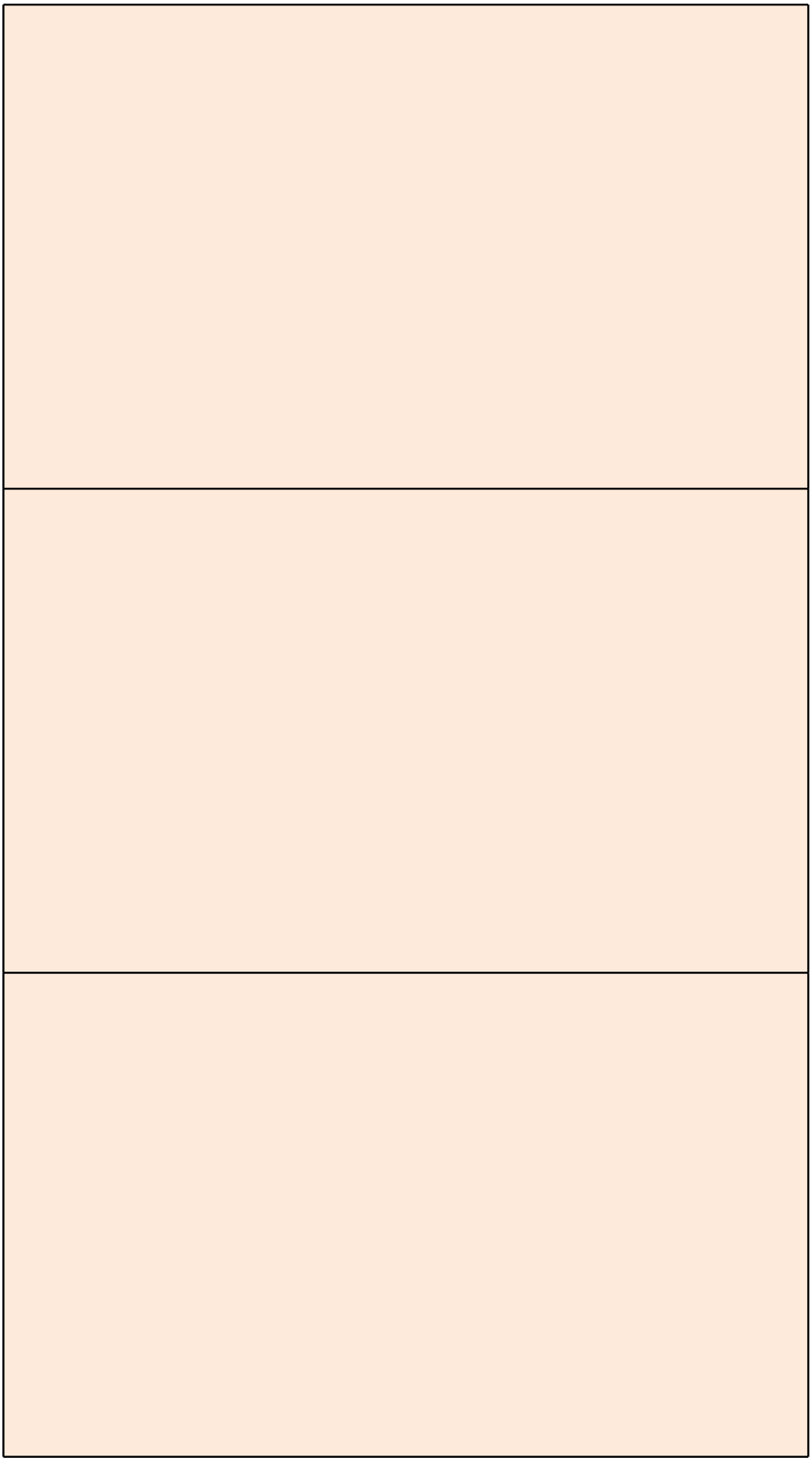


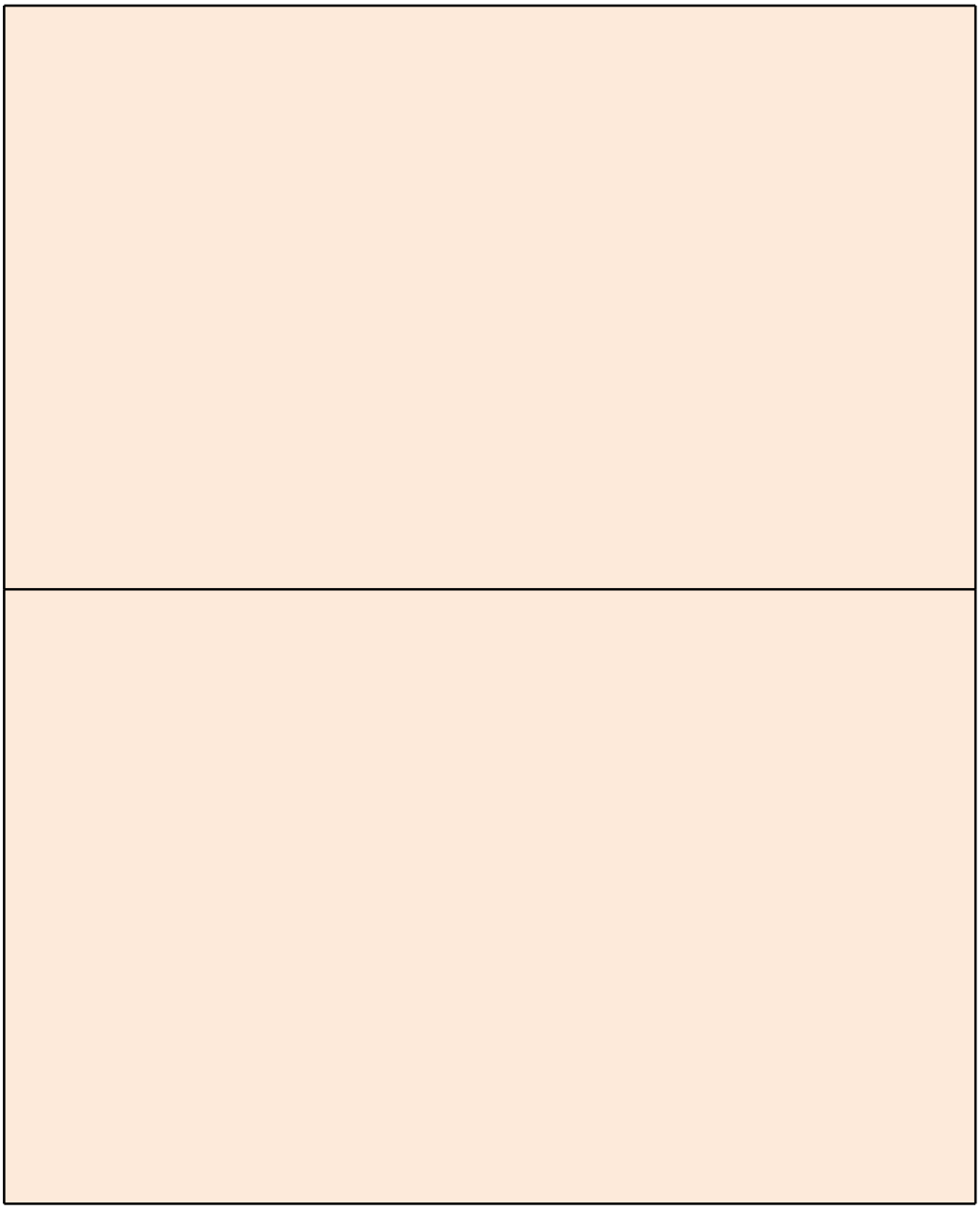


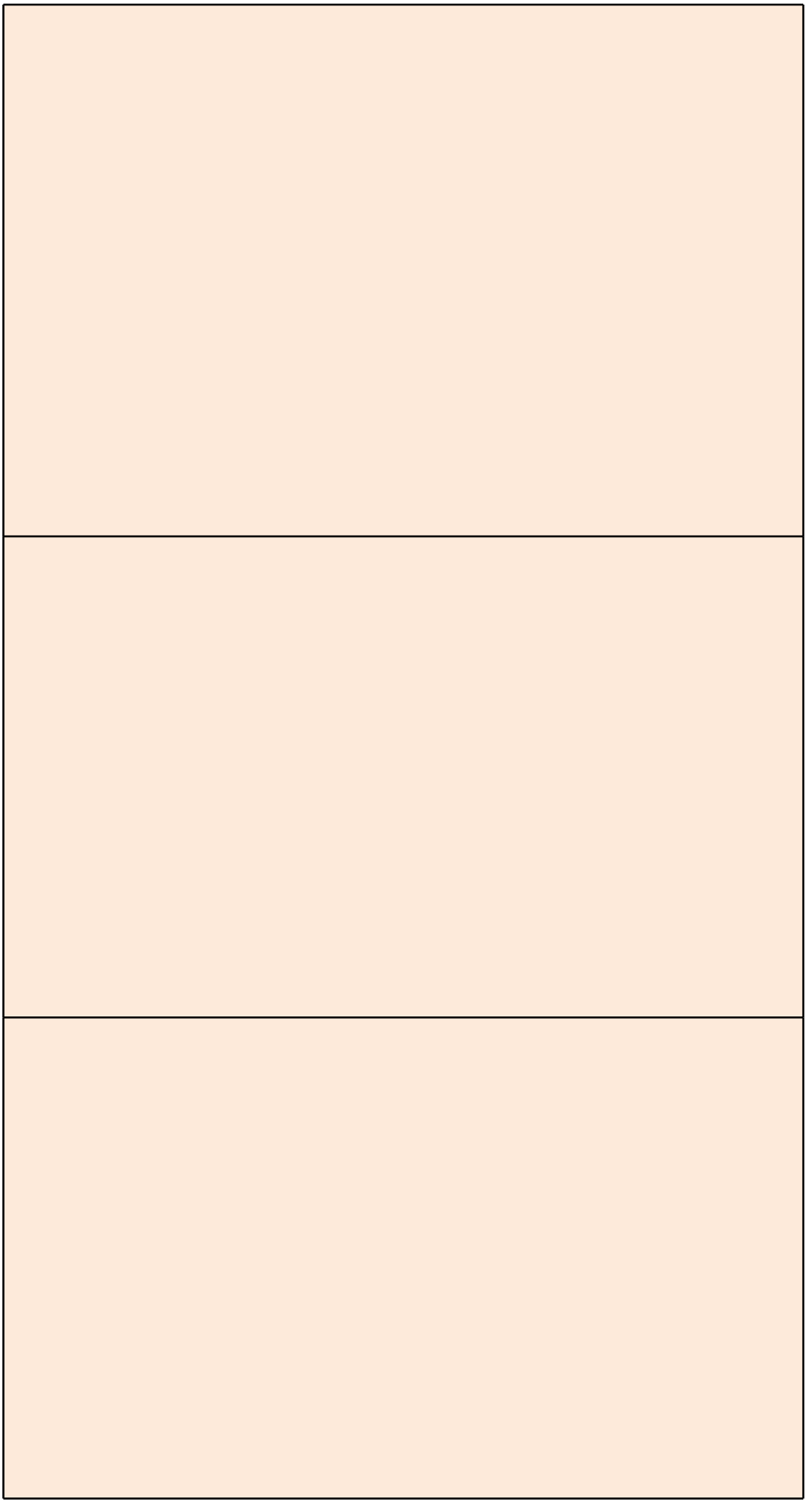


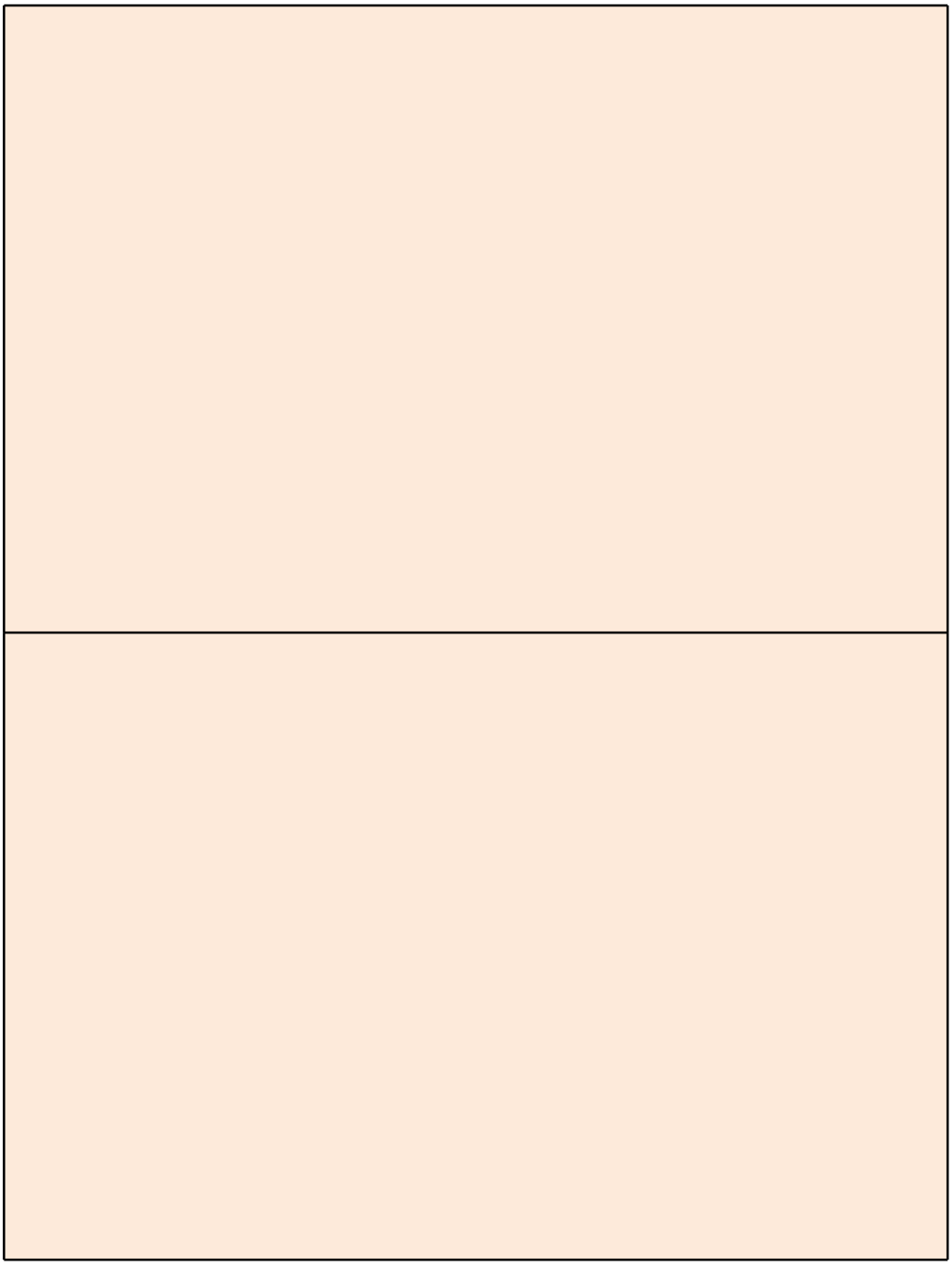


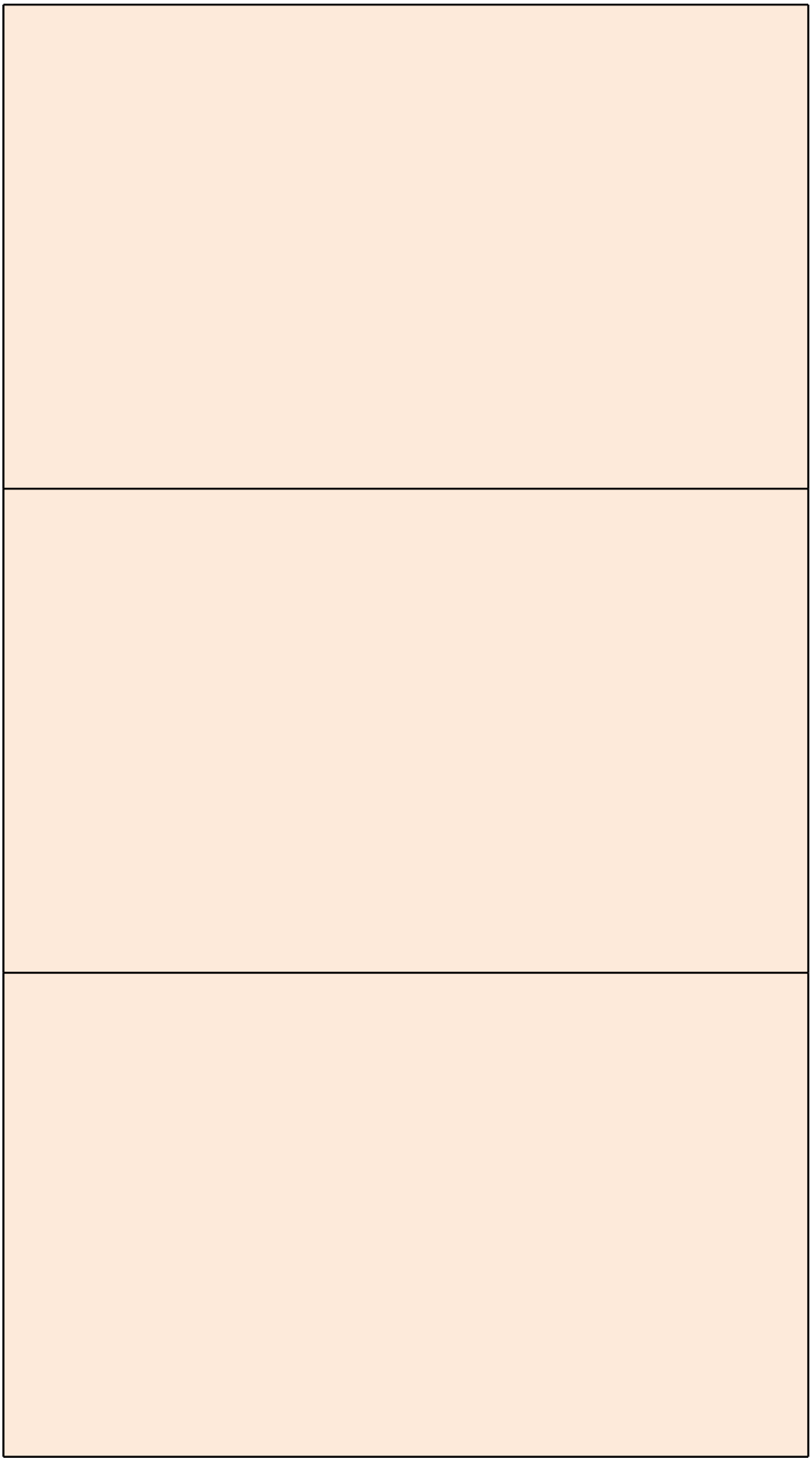


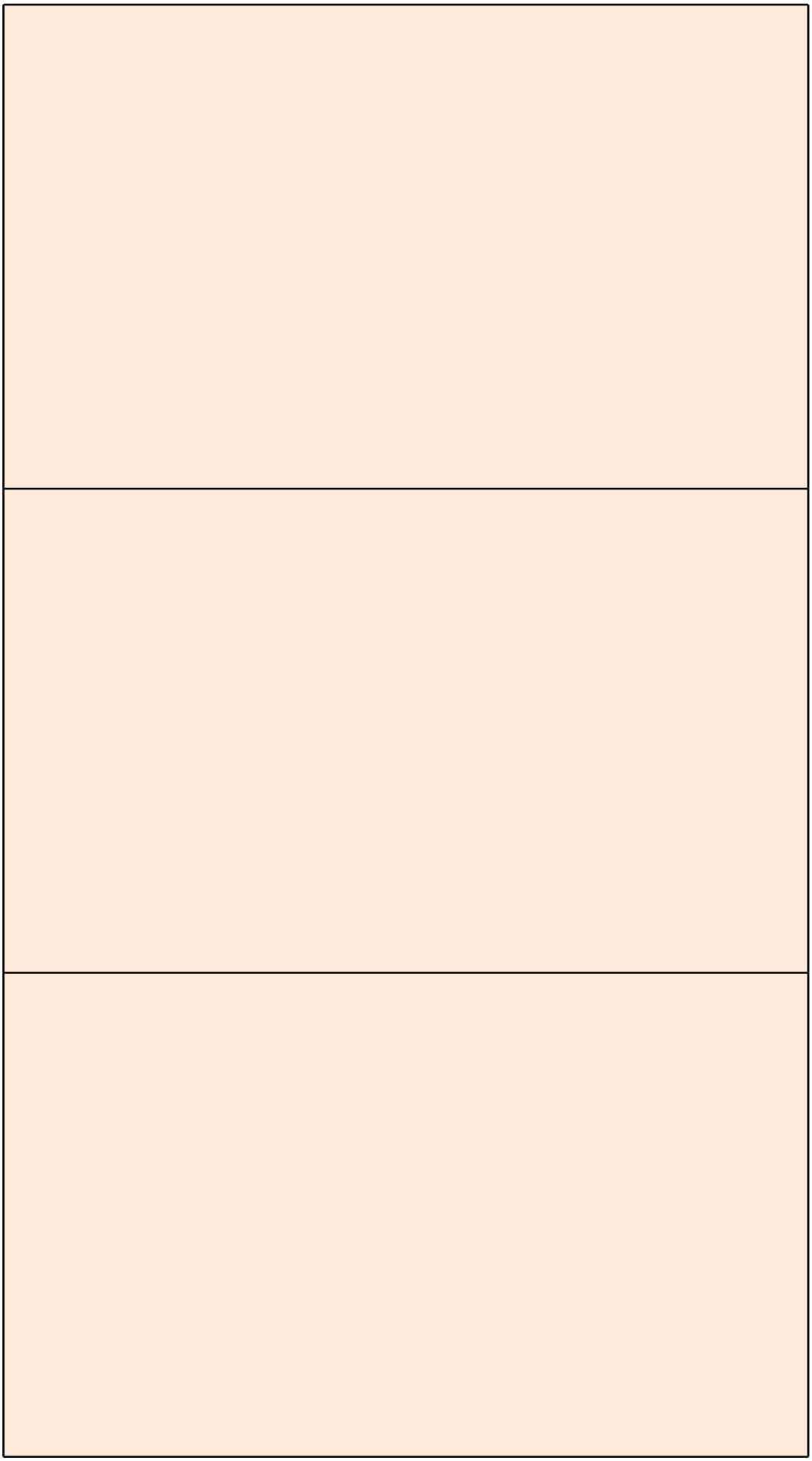


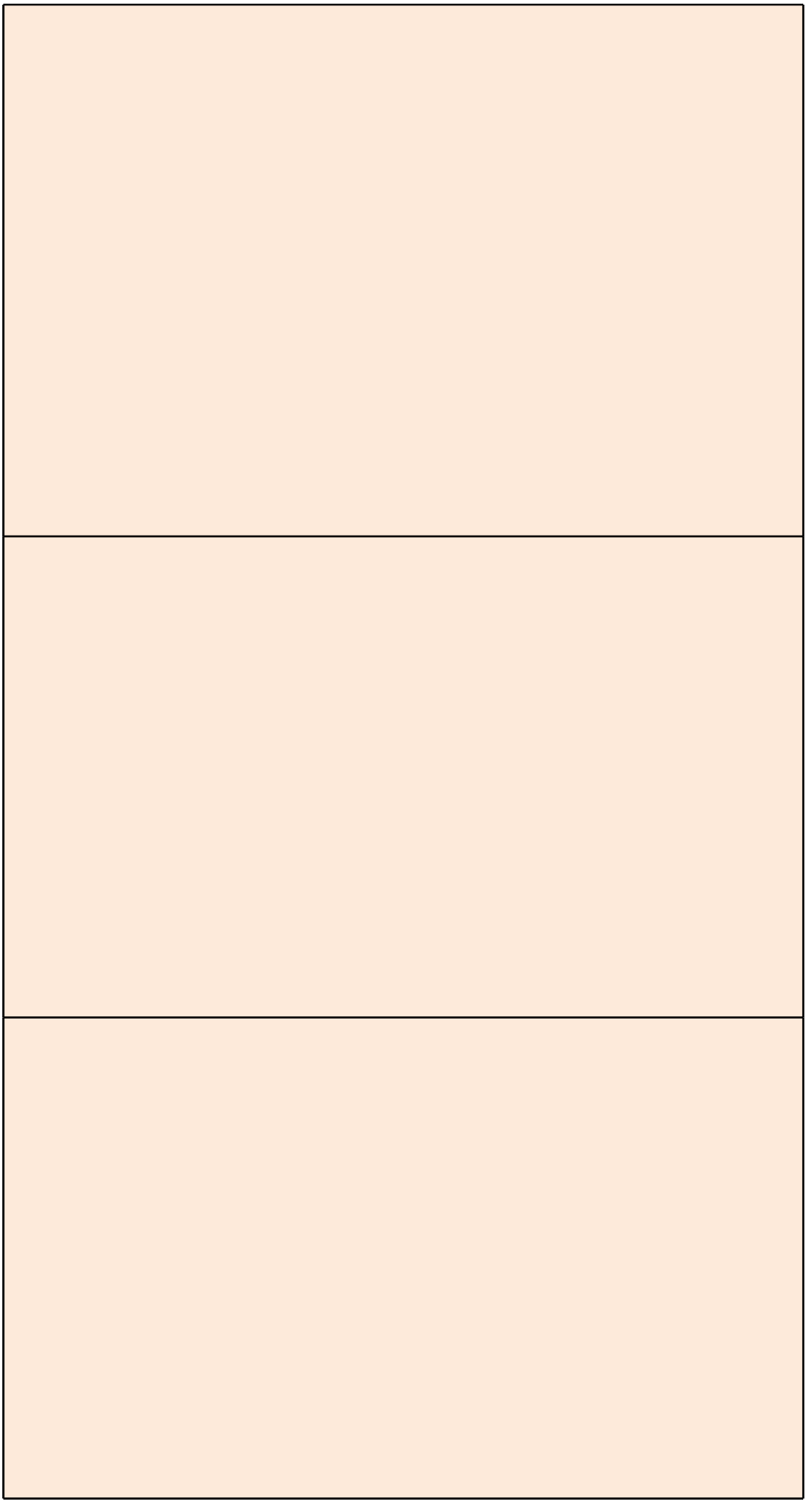


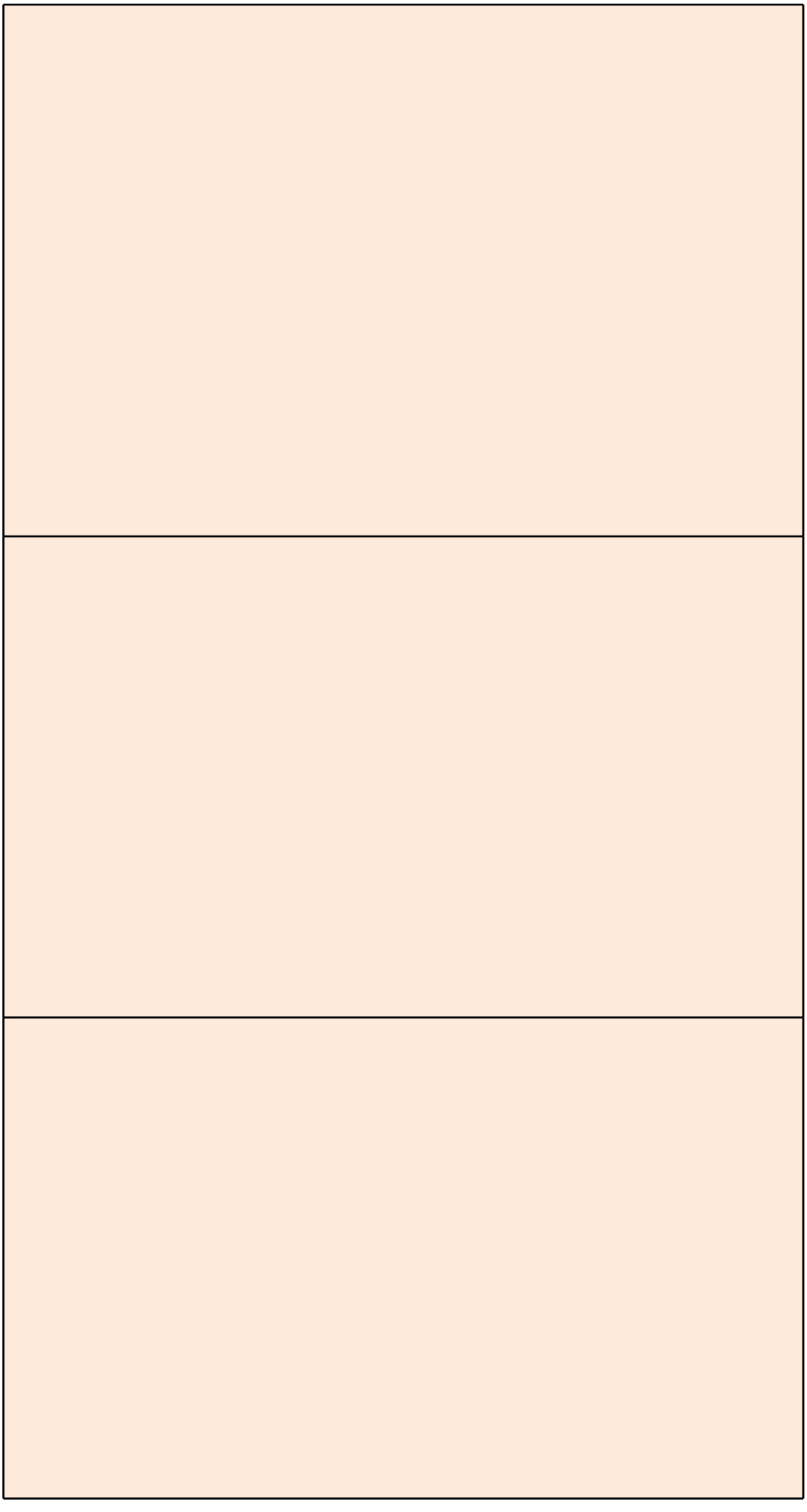


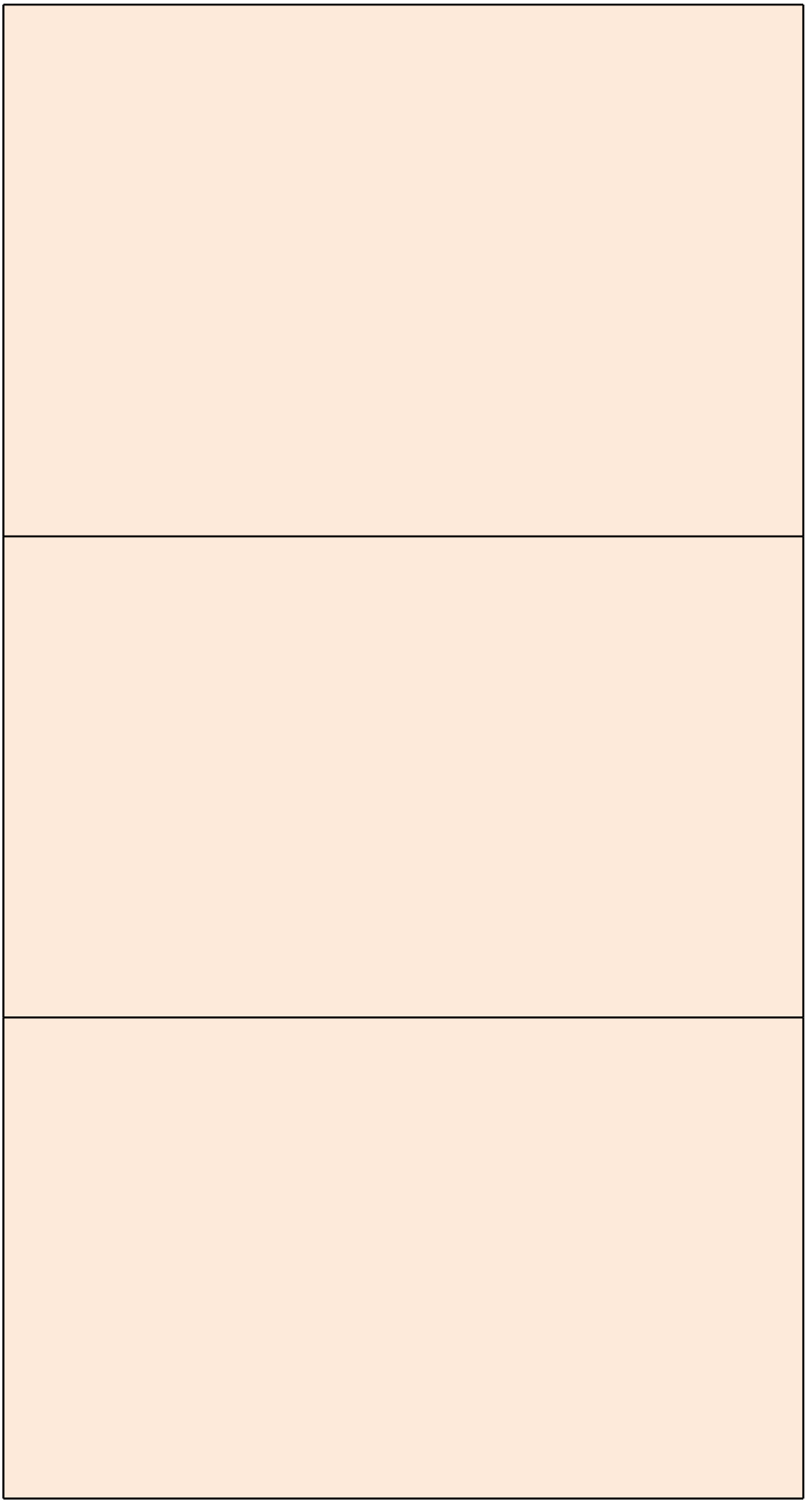




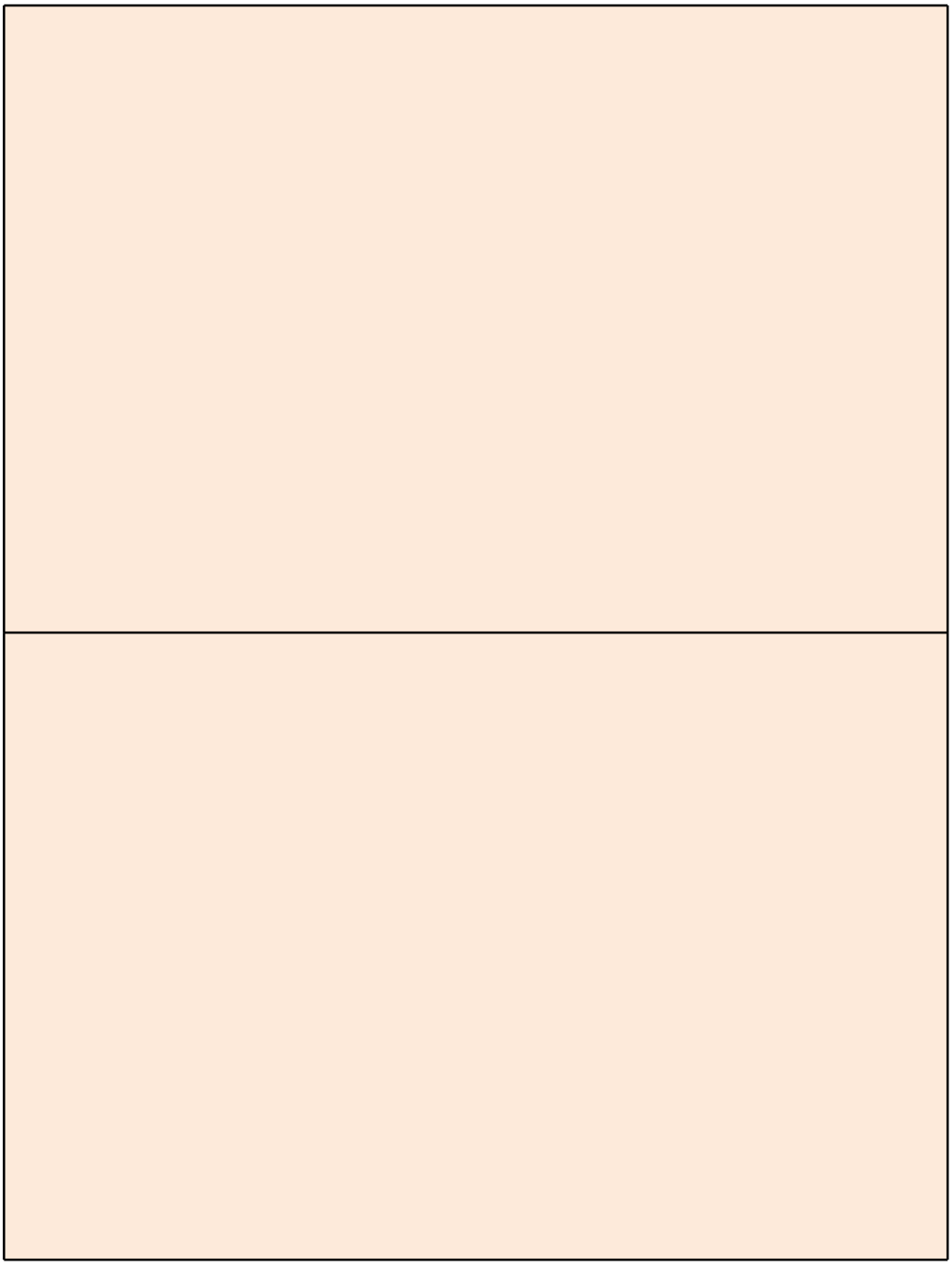


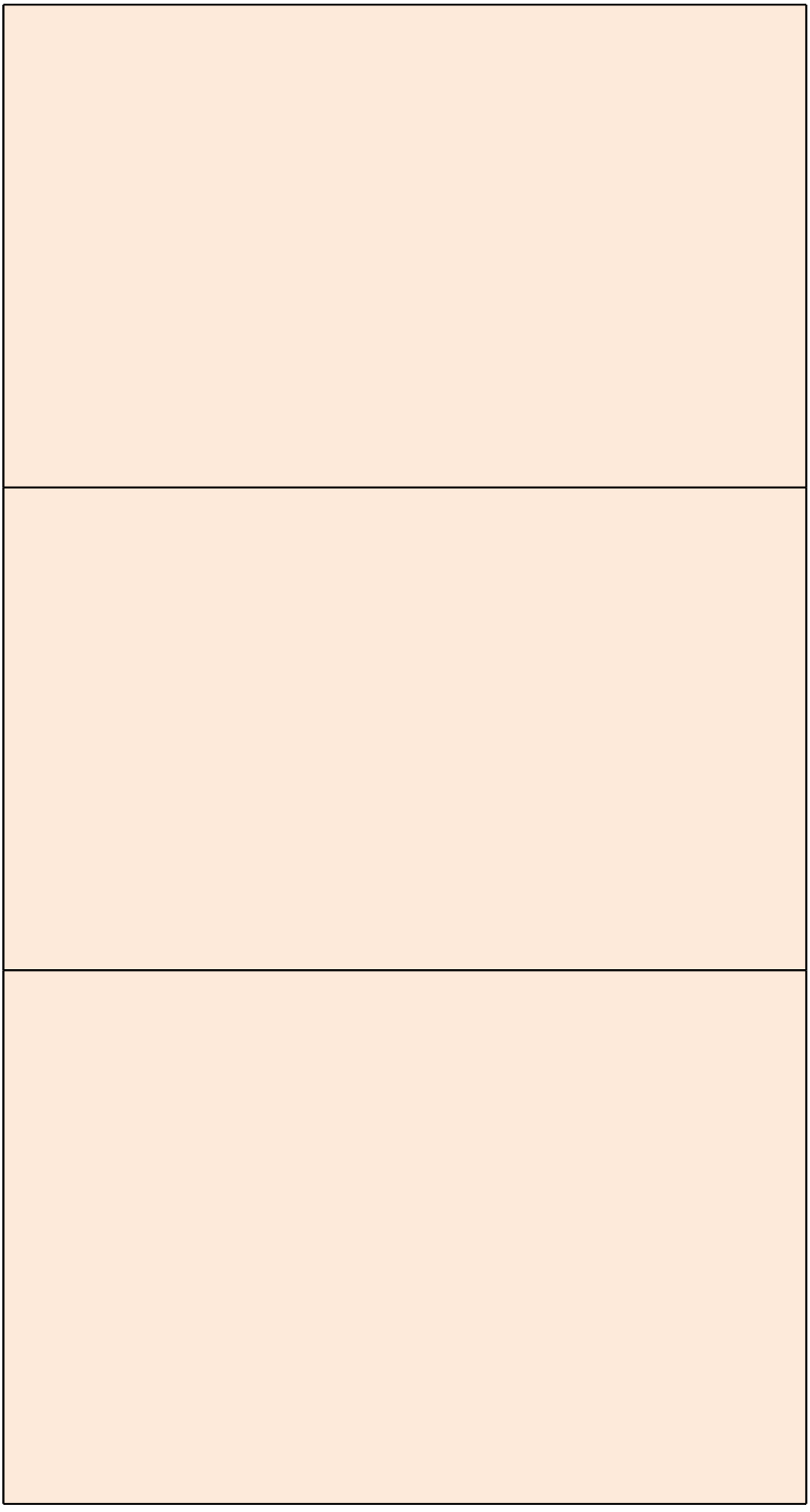


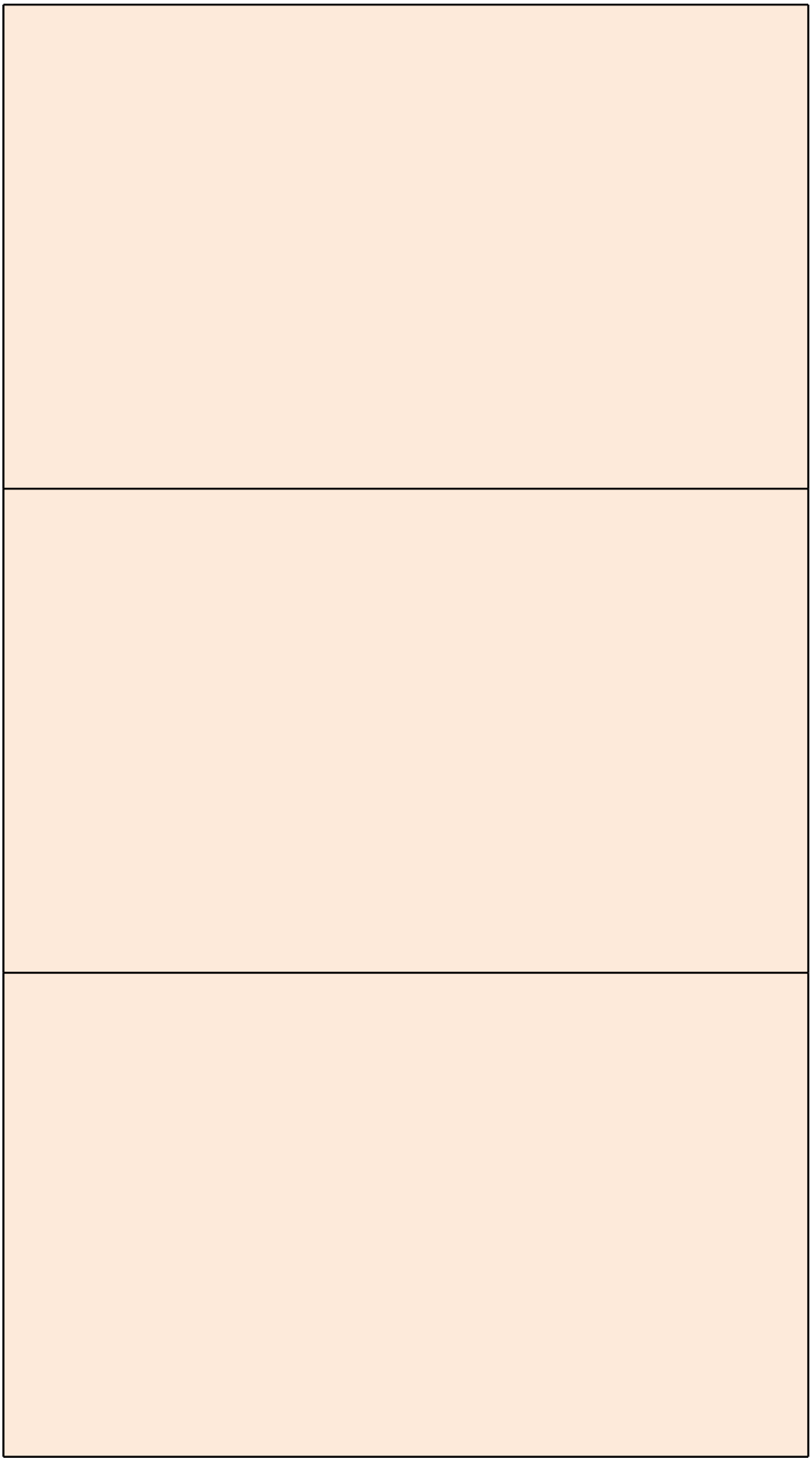




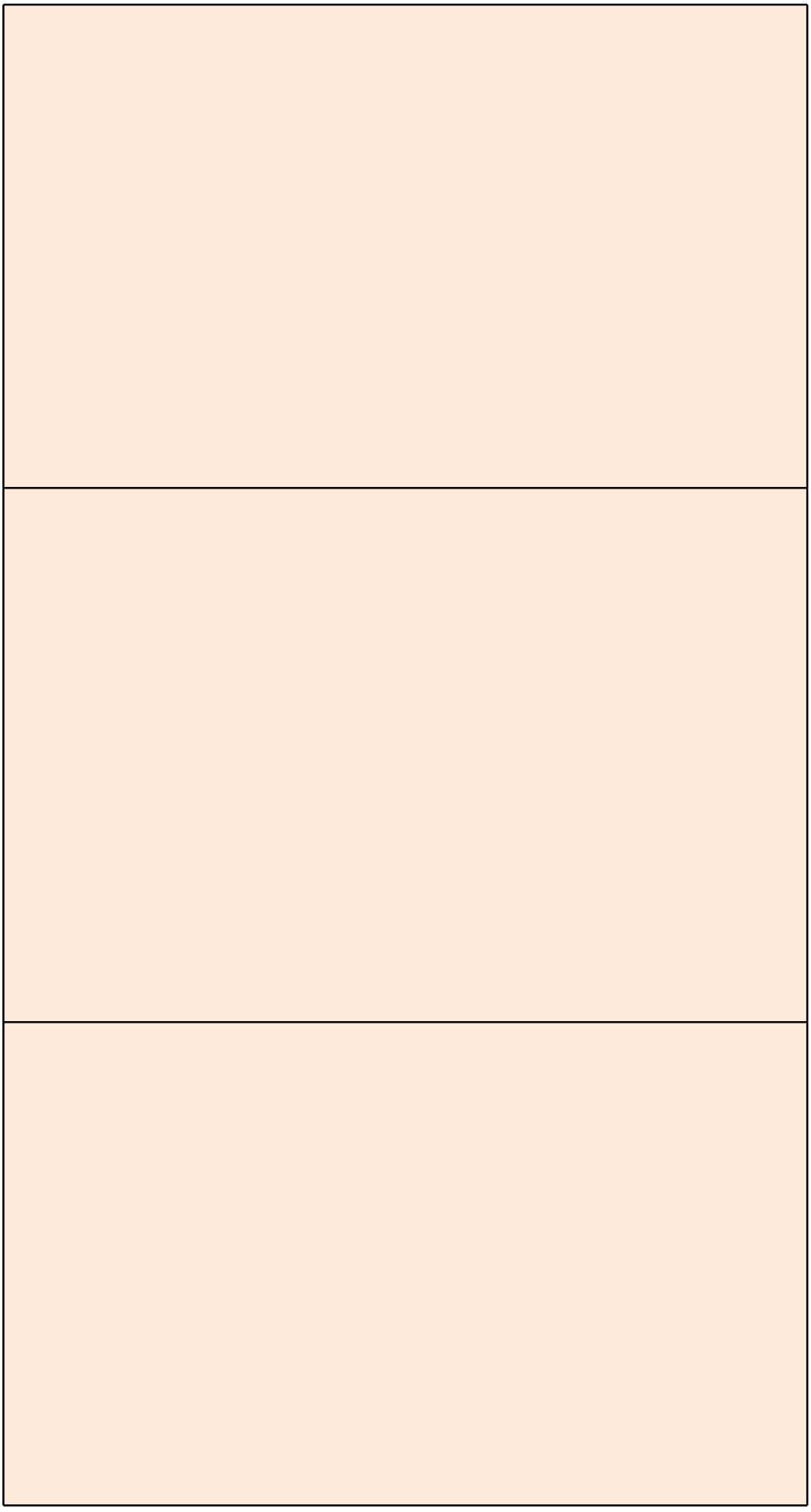
Olennaisena sidosryhmänä tulee huomioida myös sijaintipaikkakunta.

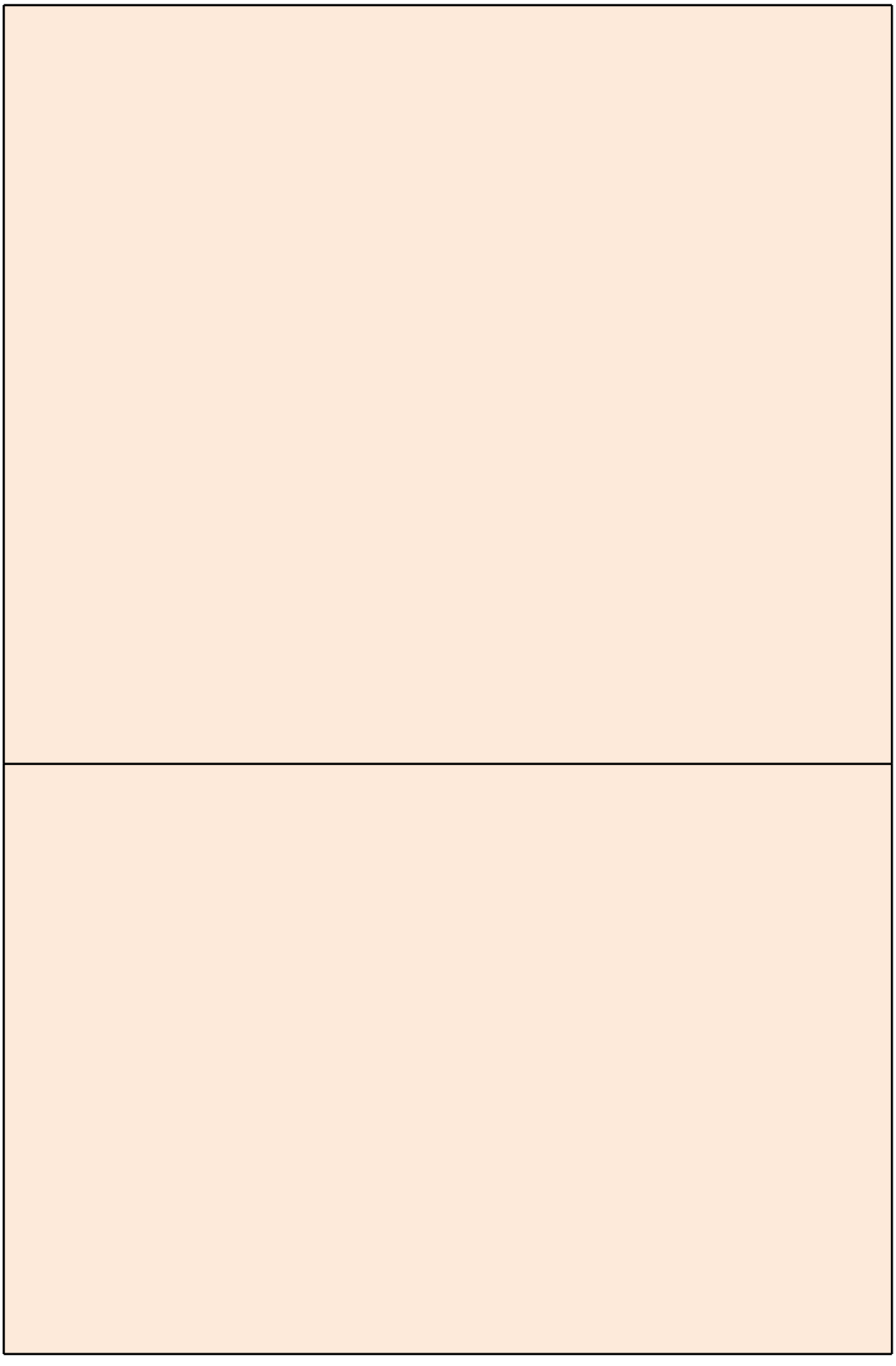


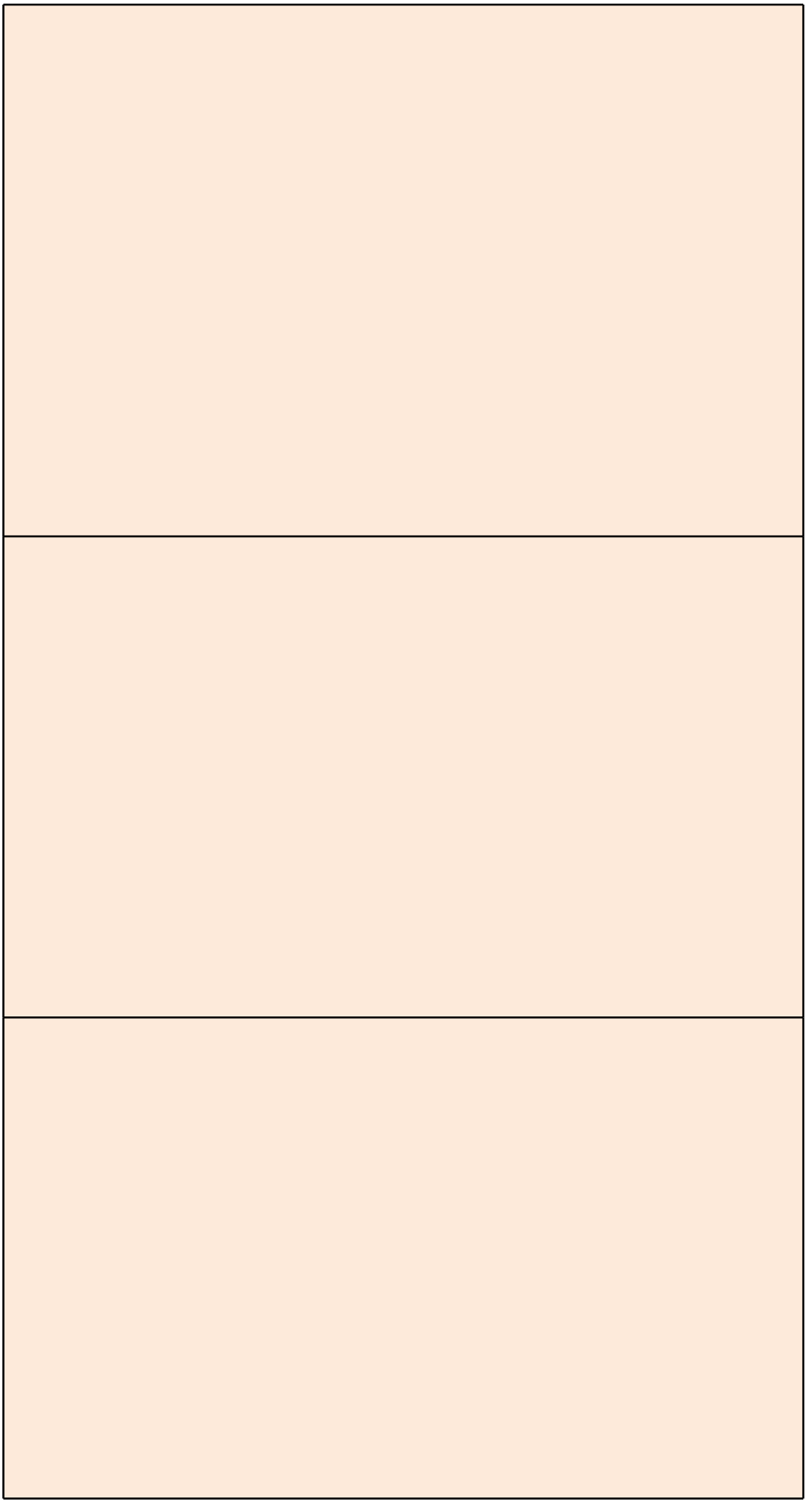


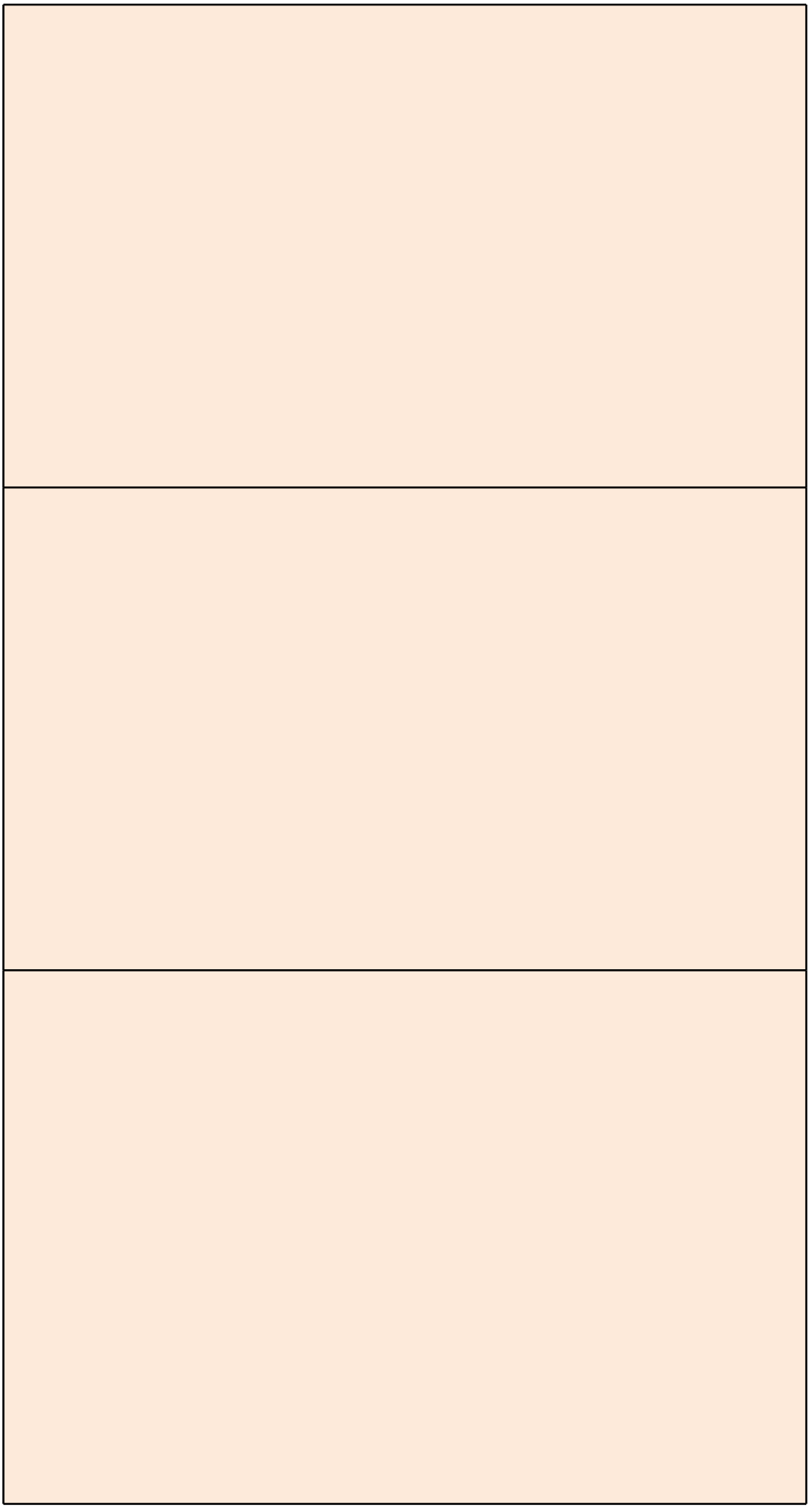


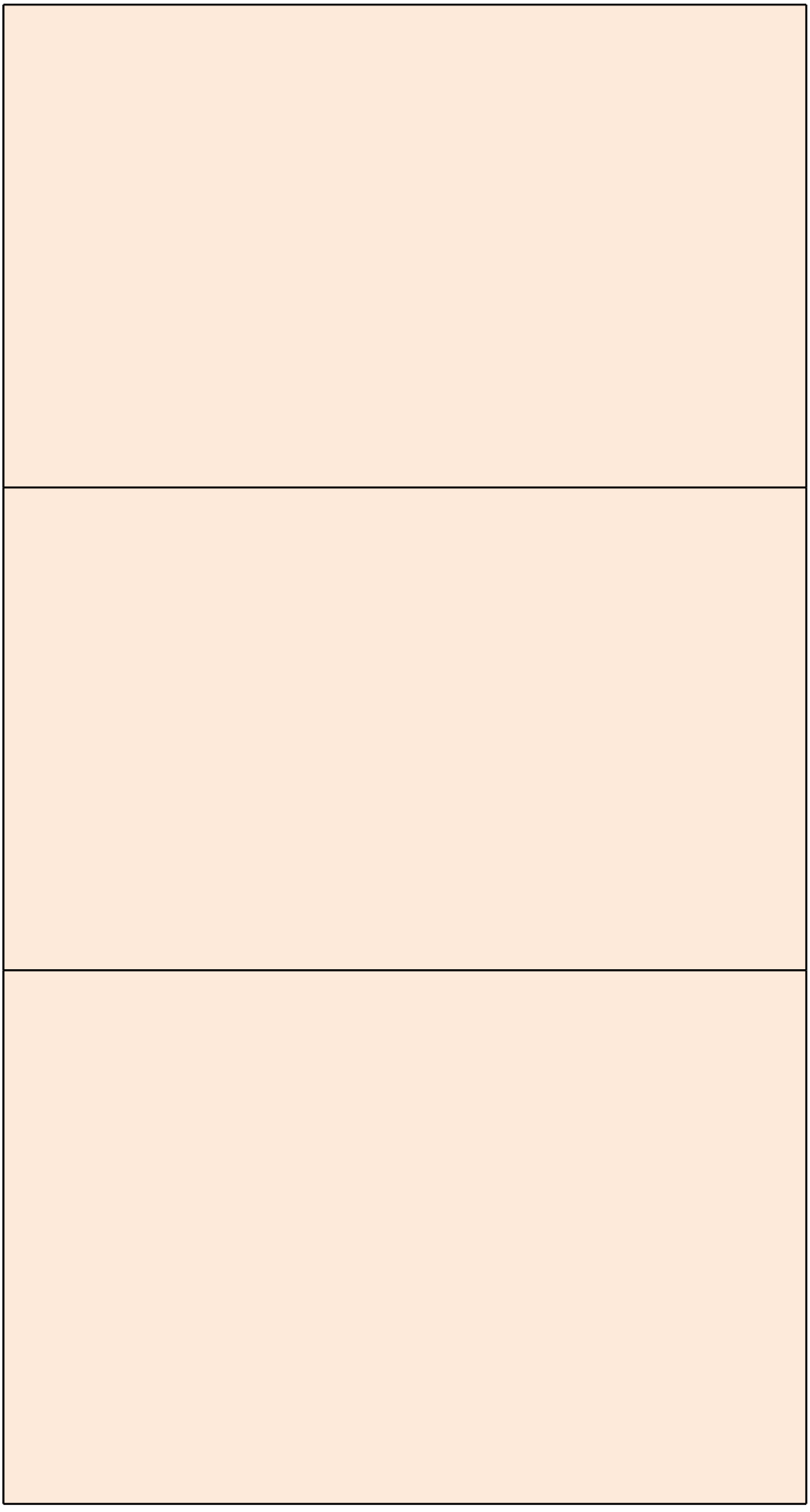
Ydinlaitoksen sijaintipaikkakunnan tulee saada välittömästi tiedot
- Mahdollisista poikkeamatilanteista sekä häiriö- ja onnettomuustilanteista, valmius- ja säteilyvaaratilanteista, epänormaaleista käyttötapahtumista, tilanteiden ja tapahtumien vaikutuksesta turvallisuuteen sekä viivytyksettä merkittävimmät havainnot ydinlaitosten valvonnassa, ympäristön säteilytarkkailun tulosten yhteenveto sekä mahdolliset ympäristön säteilyrajojen ylitykset ja niiden mahdolliset vaikutukset ja asettamat rajoitukset.
- Turvajärjestelyistä, siltä osin kuin se on tarkoituksenmukaista kunnan oman toiminnan ja varautumisen suunnittelun näkökulmasta.
Ydinlaitospaikkakuntien täytyy olla tietoisia yllä mainituista asioista, jotta ne voivat omissa suunnitelmissaan ja toimissaan ottaa nämä asiat huomioon ja siten edesauttaa omalta osaltaan ydin- ja säteilyturvallisuuden säilymisen ja vahvistamisen esimerkiksi turhien päällekkäisten tapahtumien estämisenä tai muiden turvallisuuteen vaikuttavien päätösten oikeellisuuden ja tarkoituksenmukaisuuden varmistamisessa (esim. tiestön tai muun infran kuten vesijohto- ja viemäriverkkojen peruskorjaukset tmv.). Lisäksi tämänkaltaisella riittävällä viestinnällä voidaan tukea ydinvoiman käytön yleistä hyväksyttävyyttä Suomessa ja laitospaikkakunnalla.

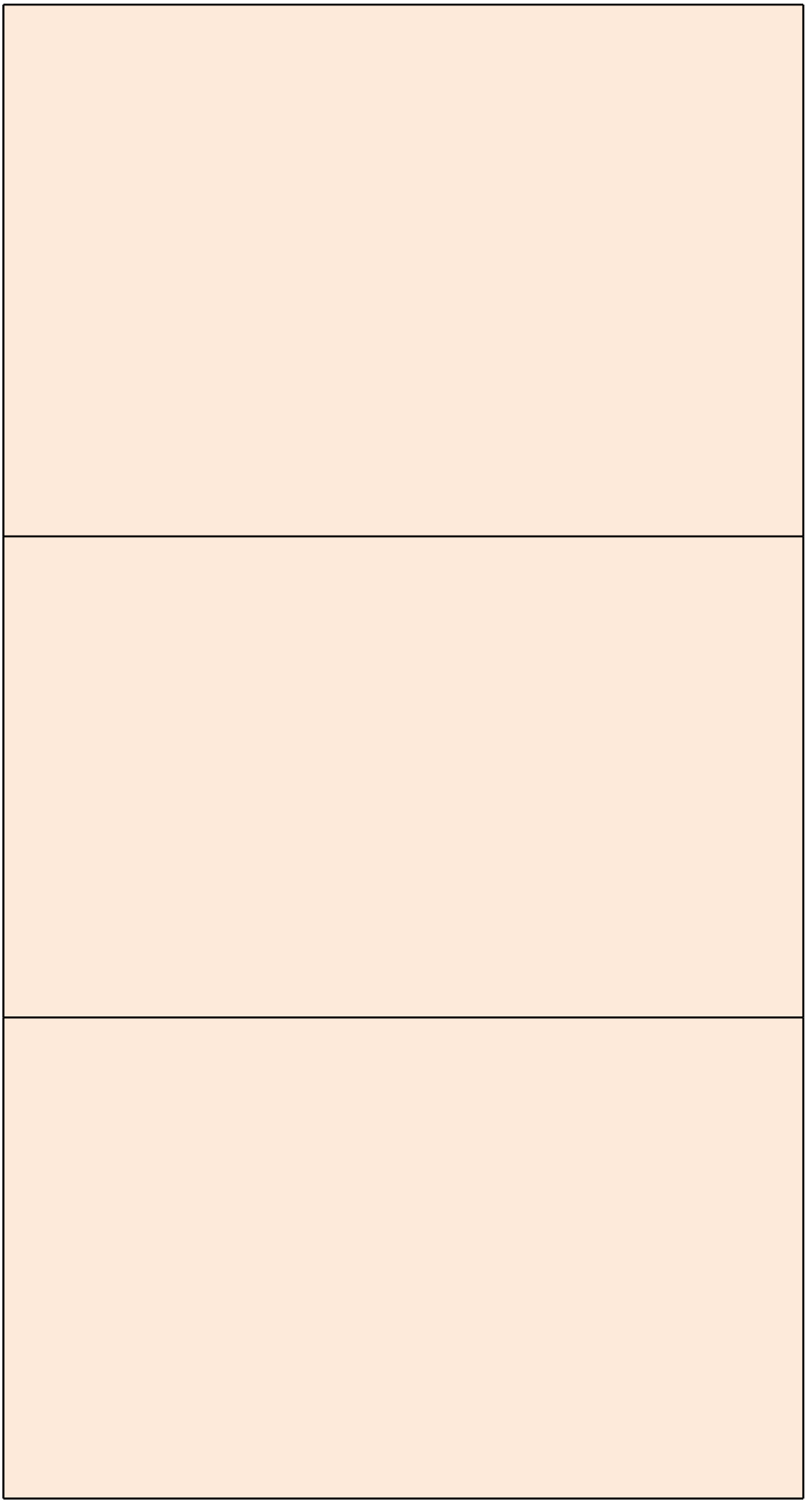


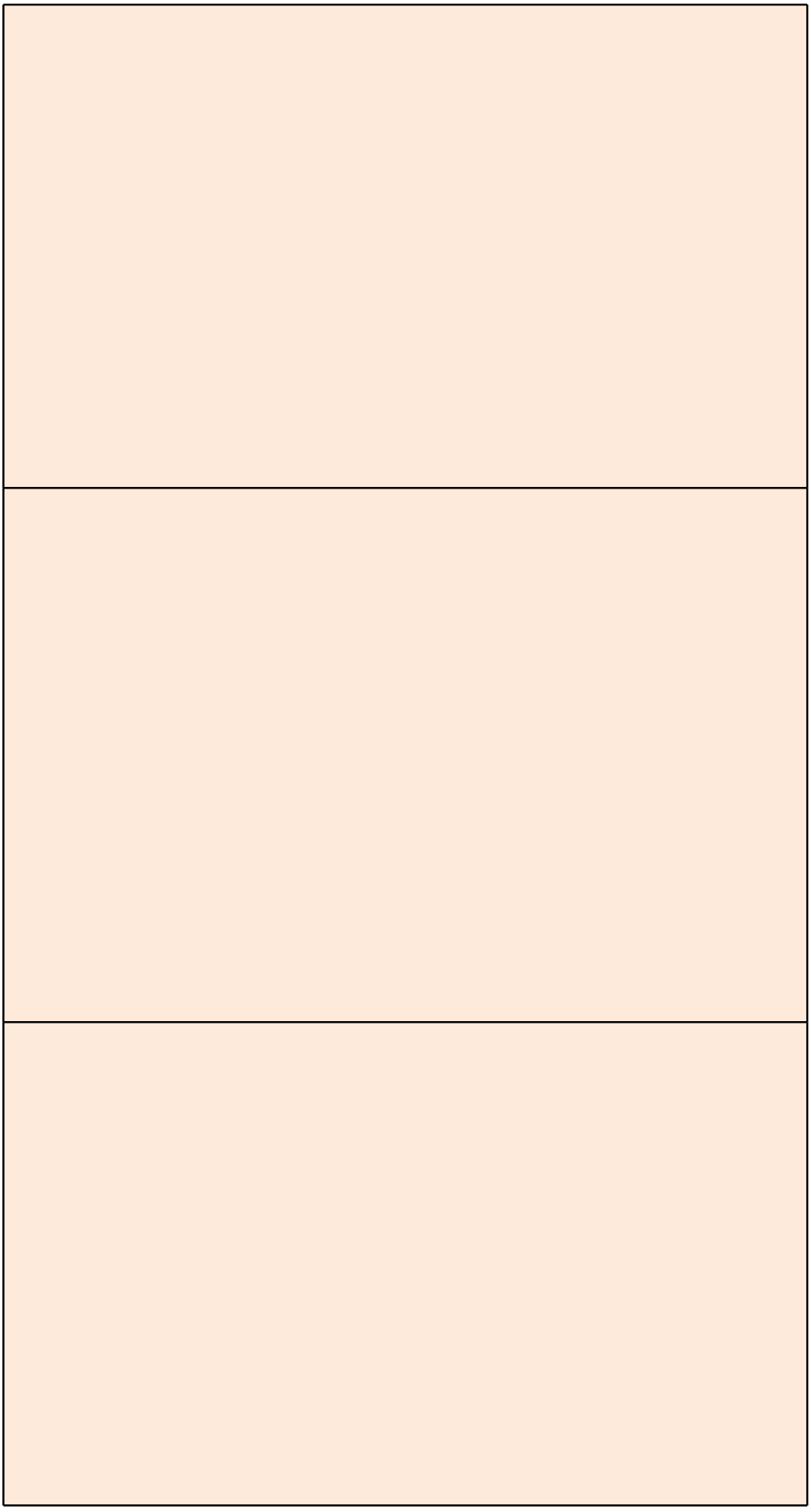


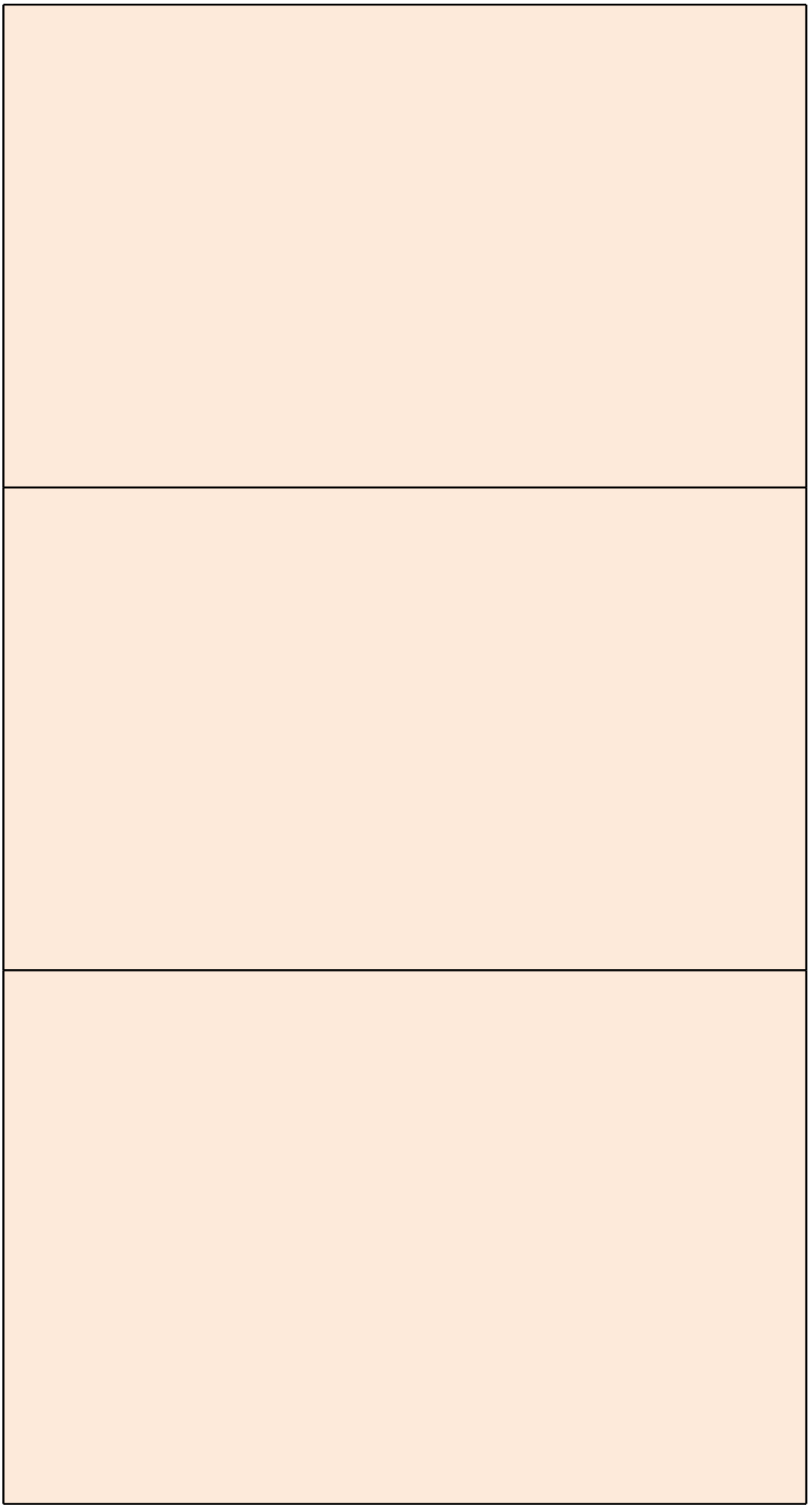


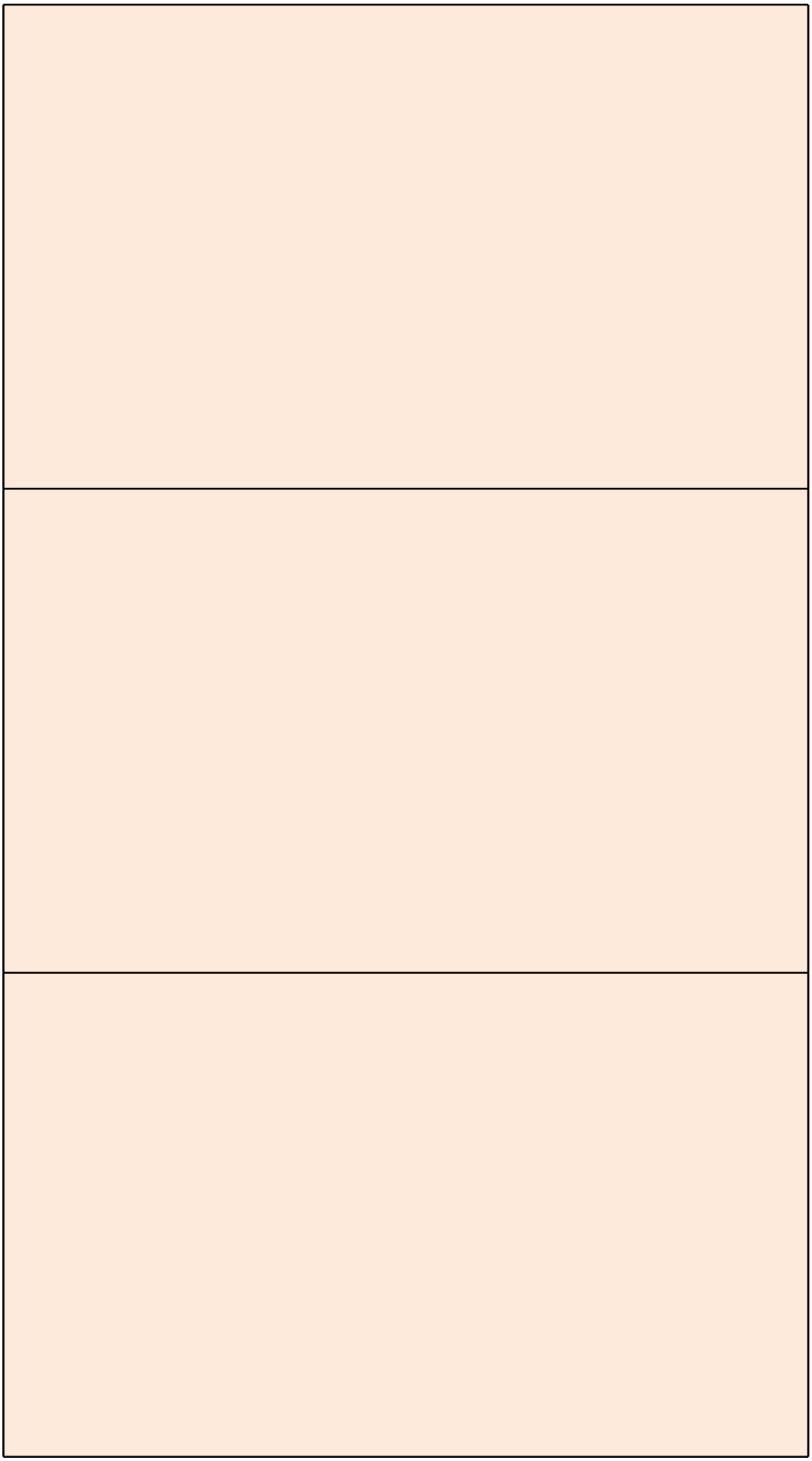


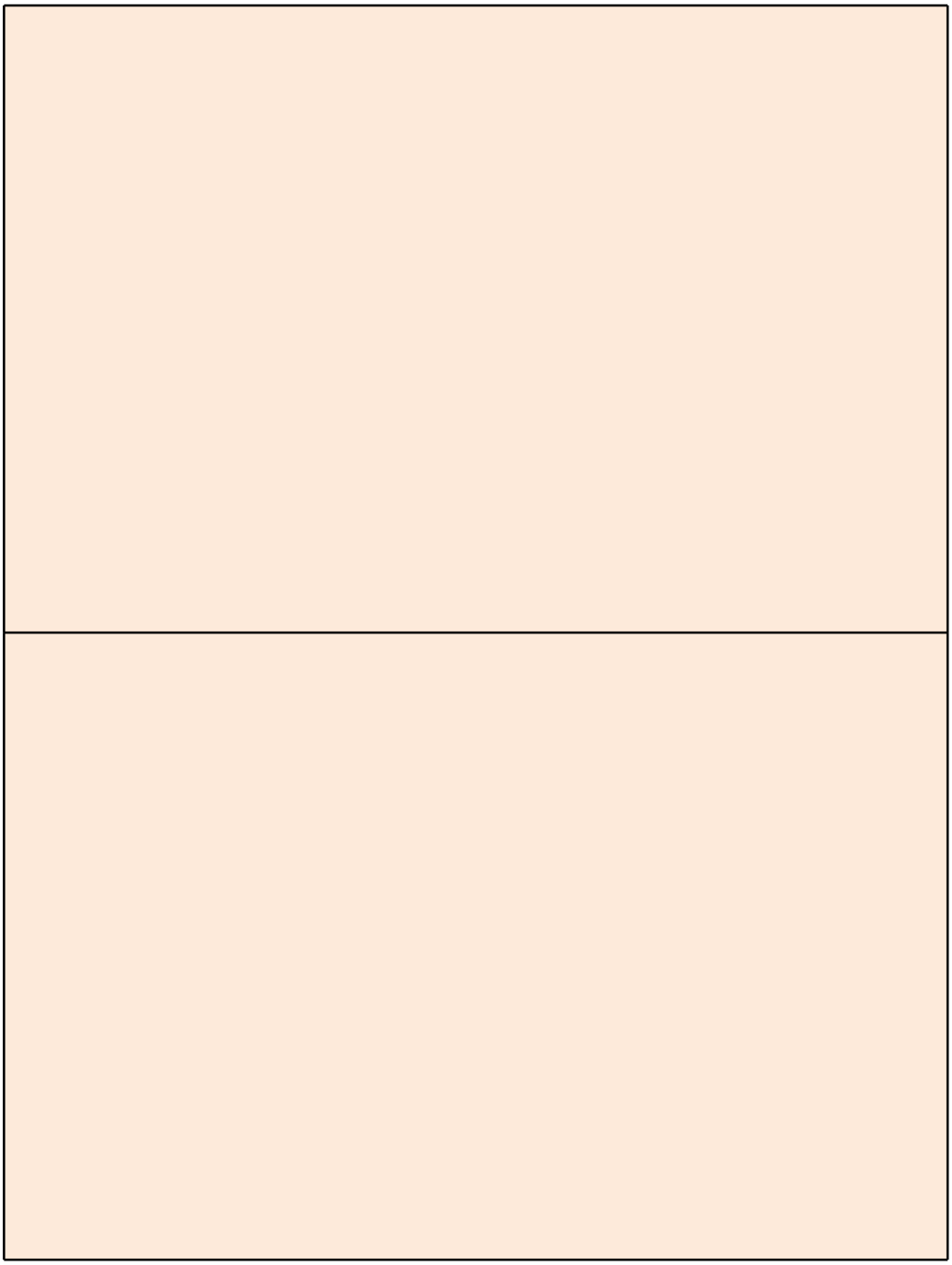


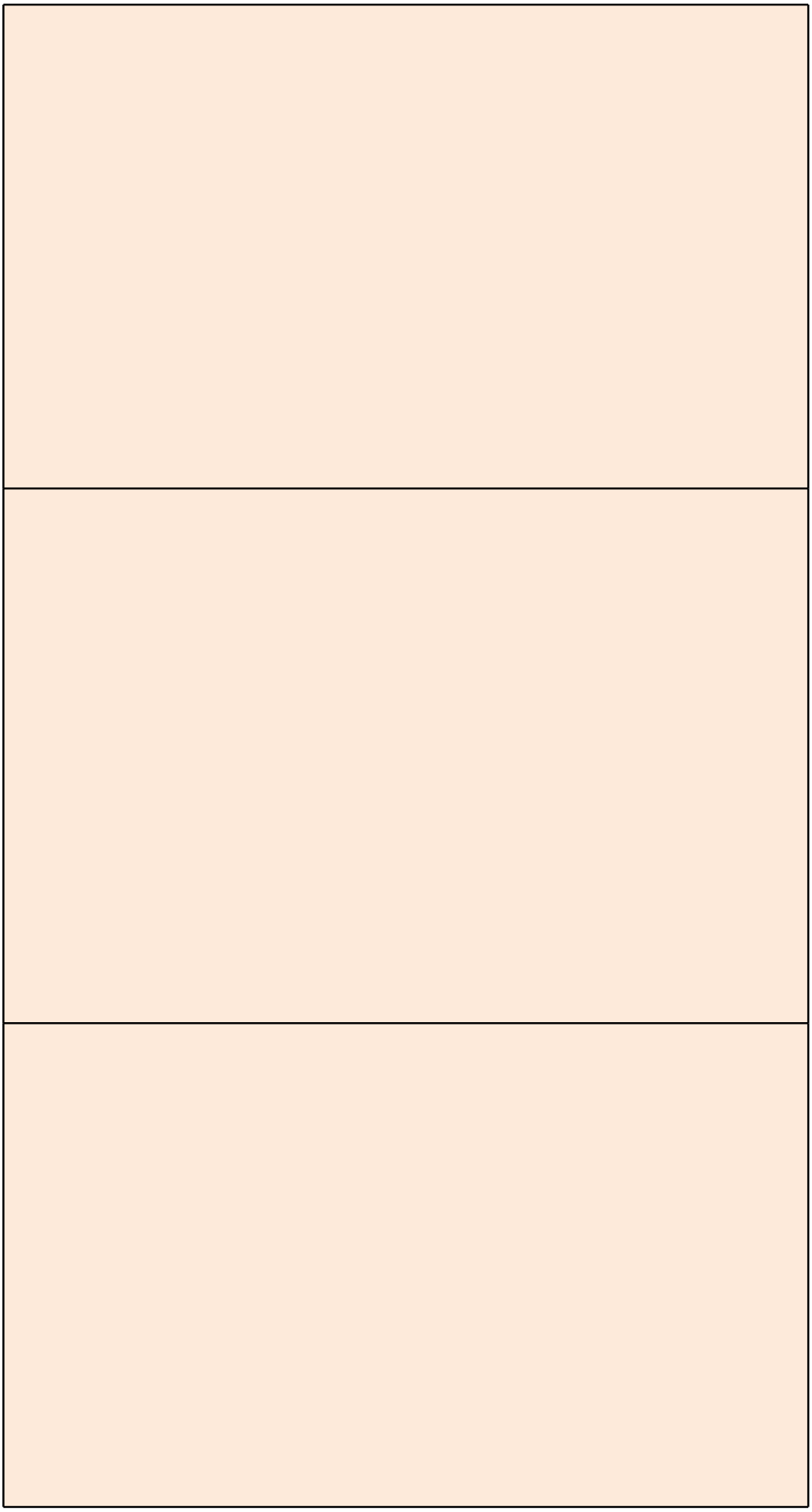


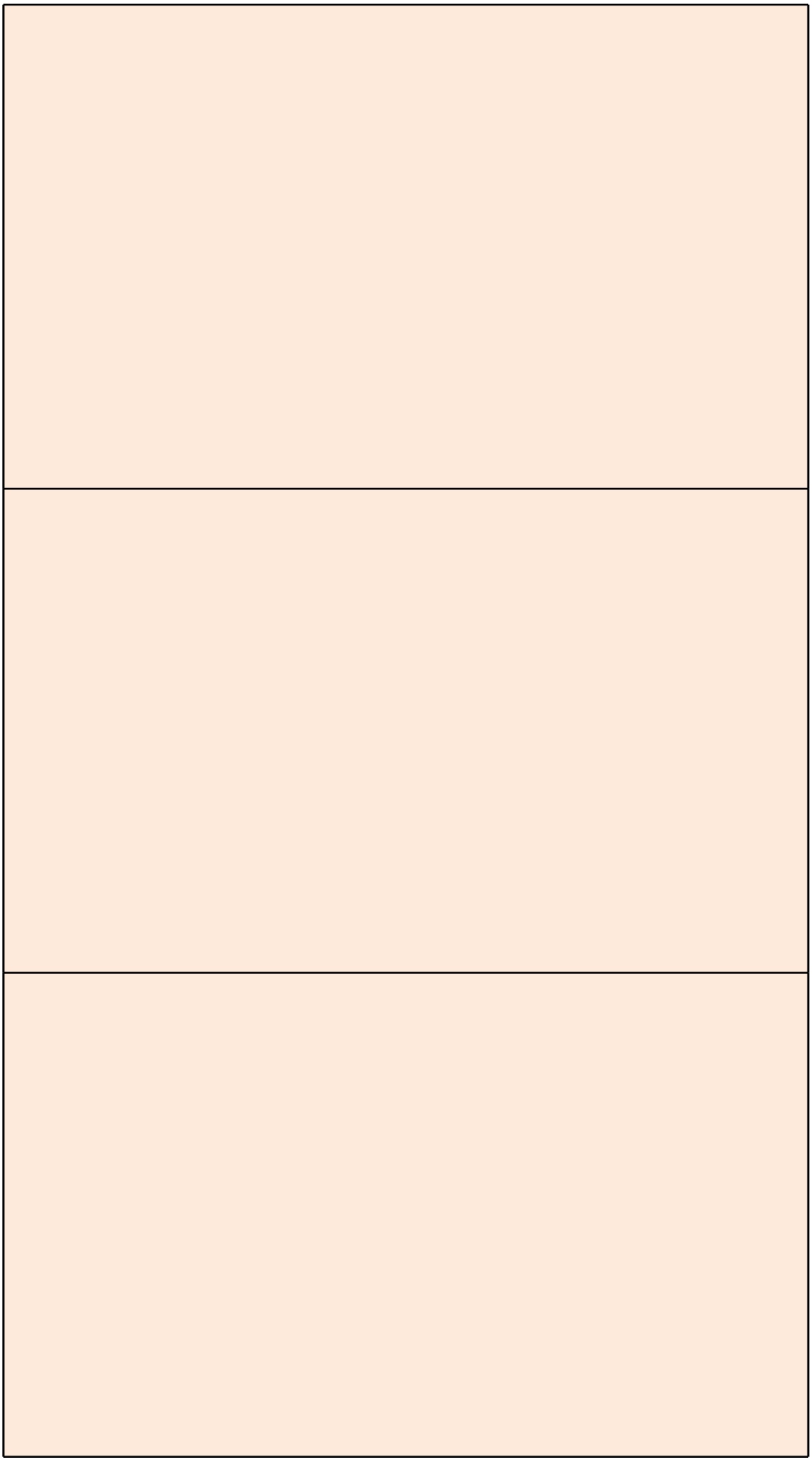


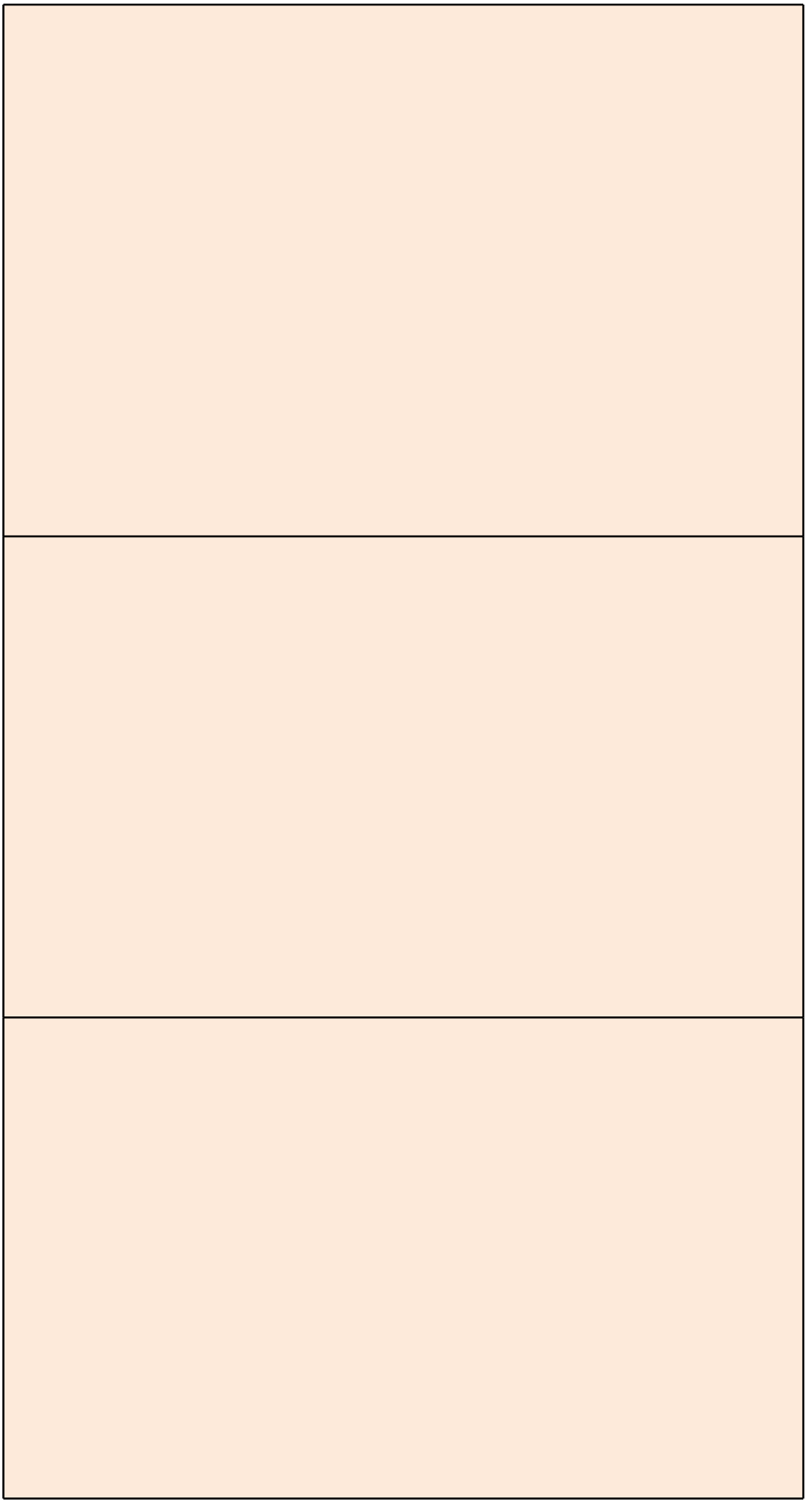


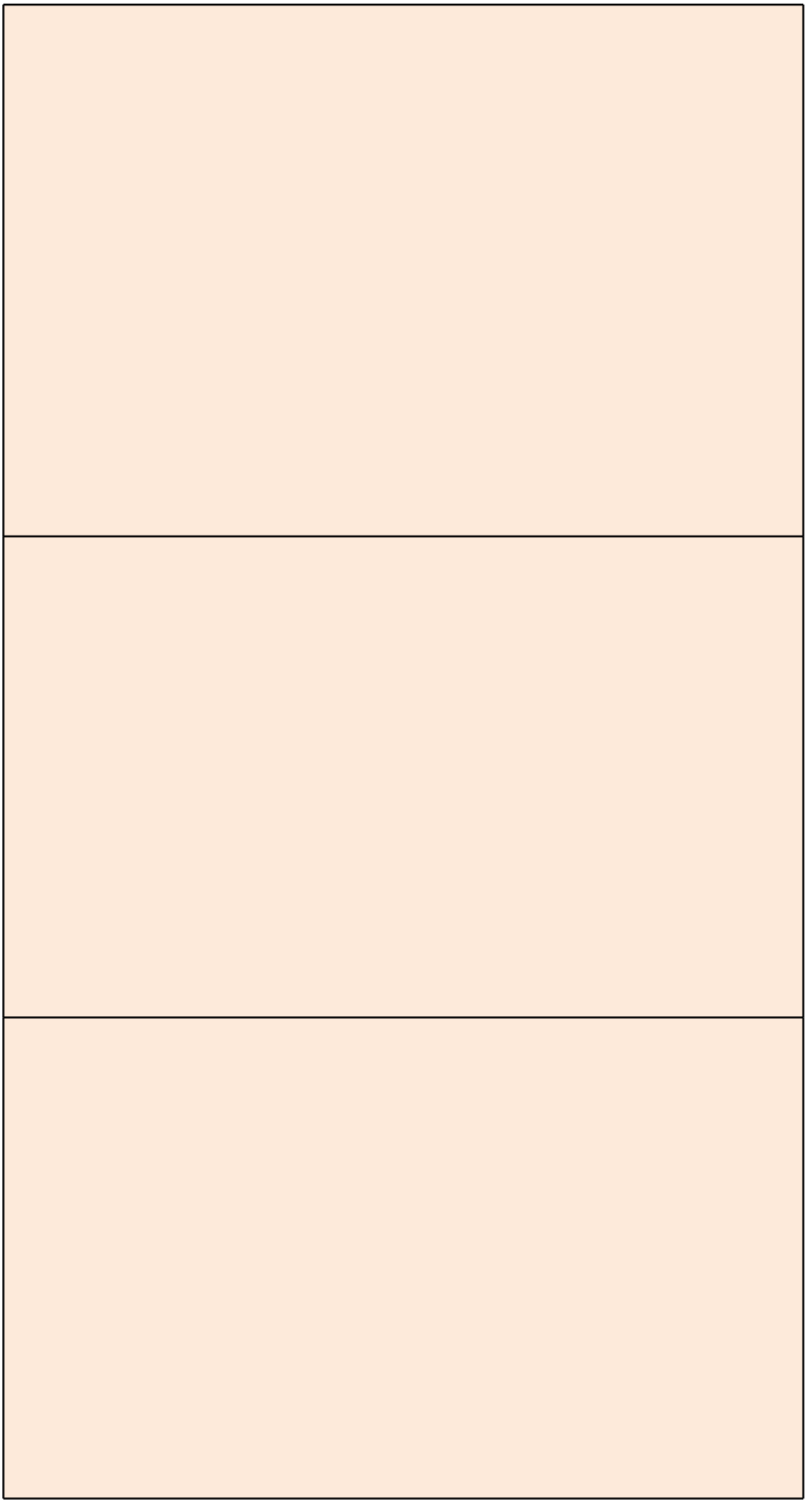


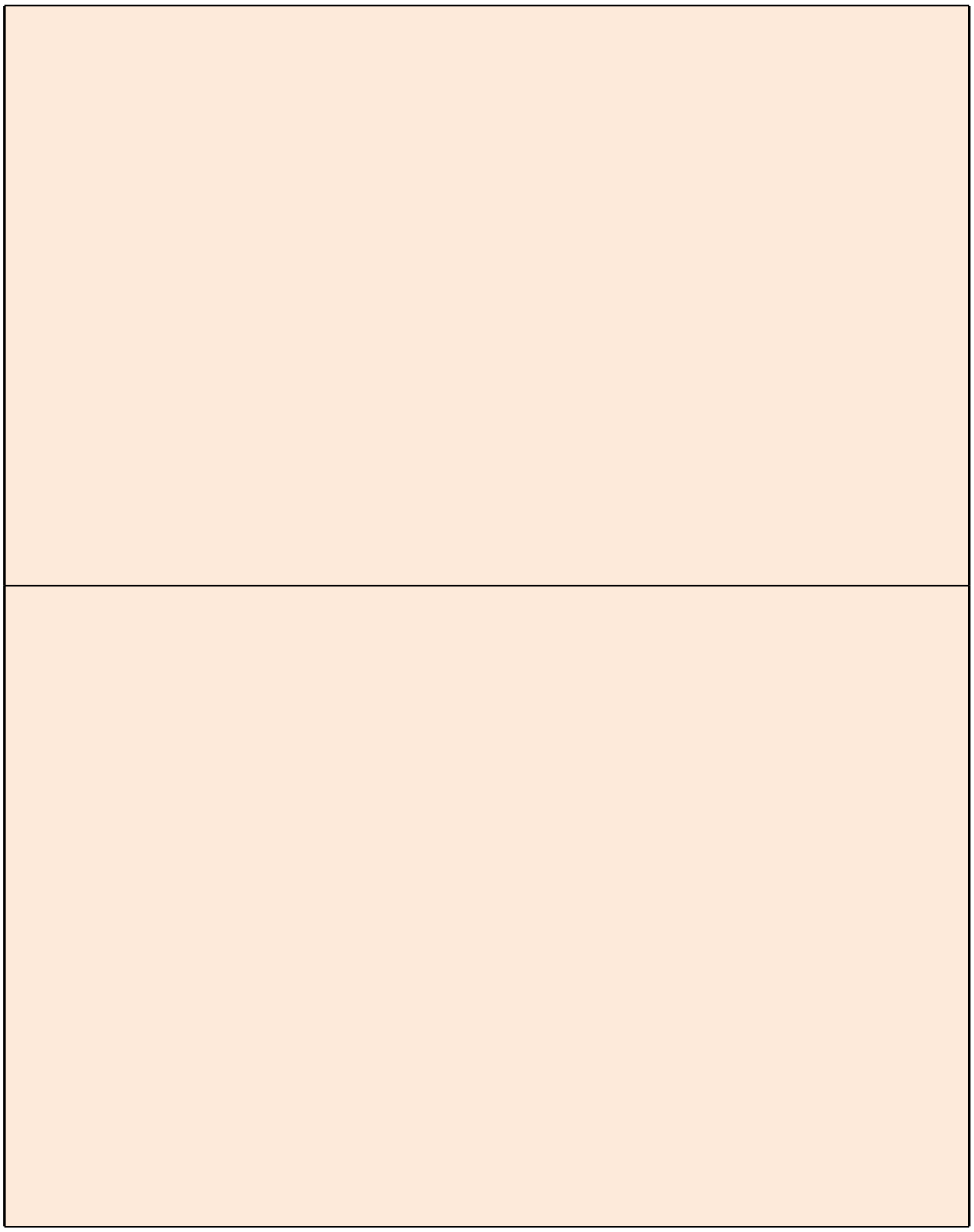


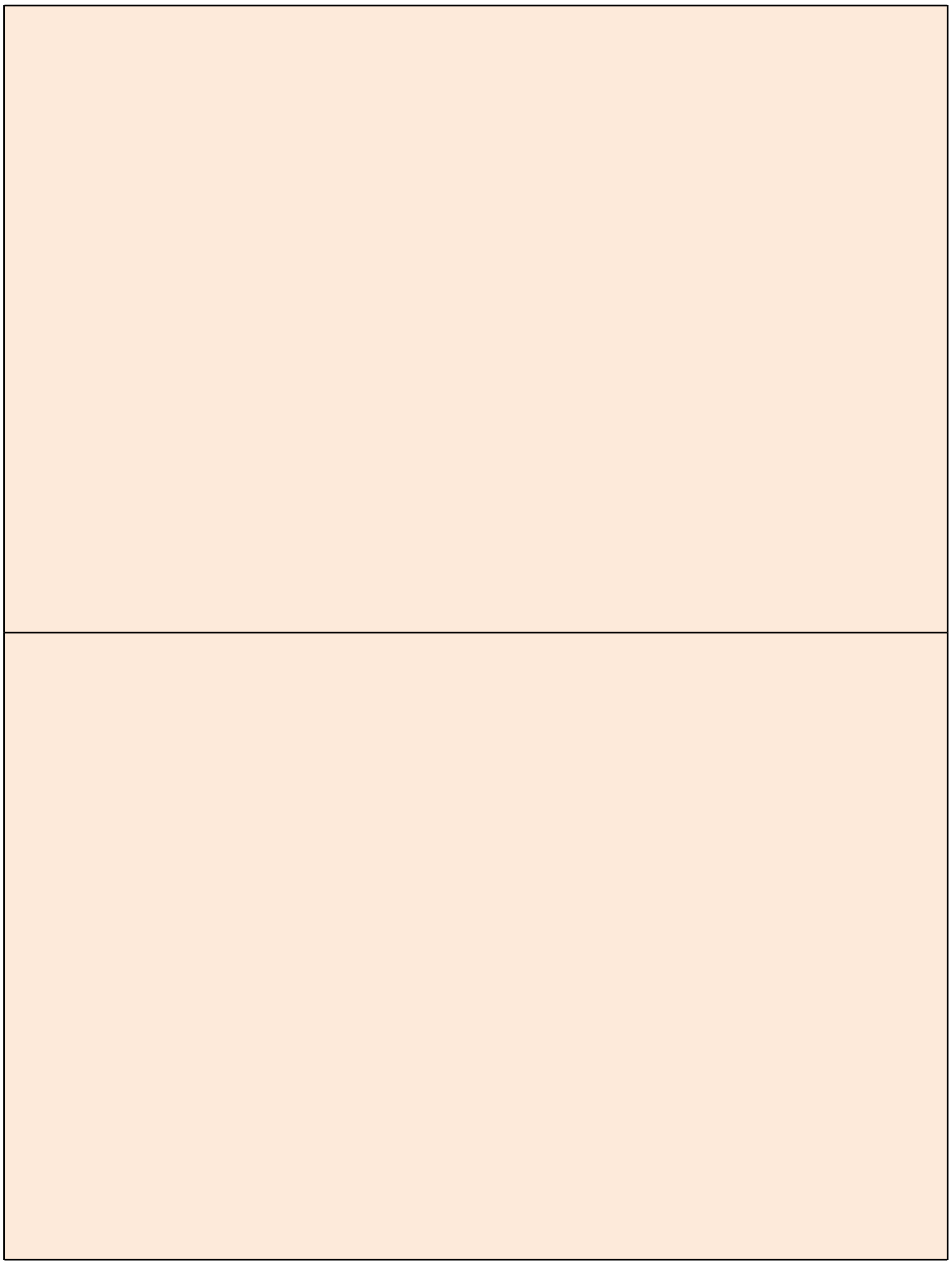




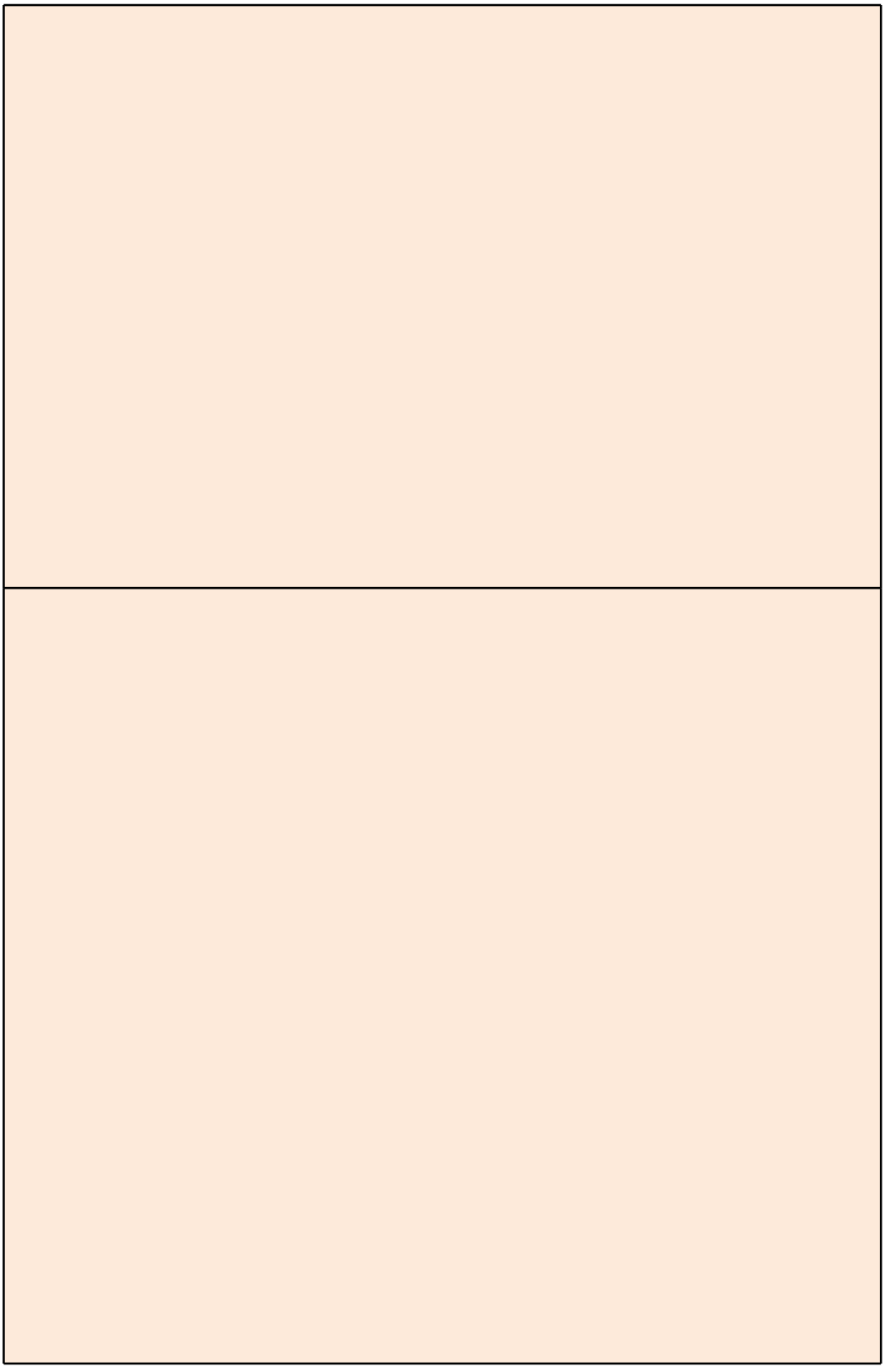


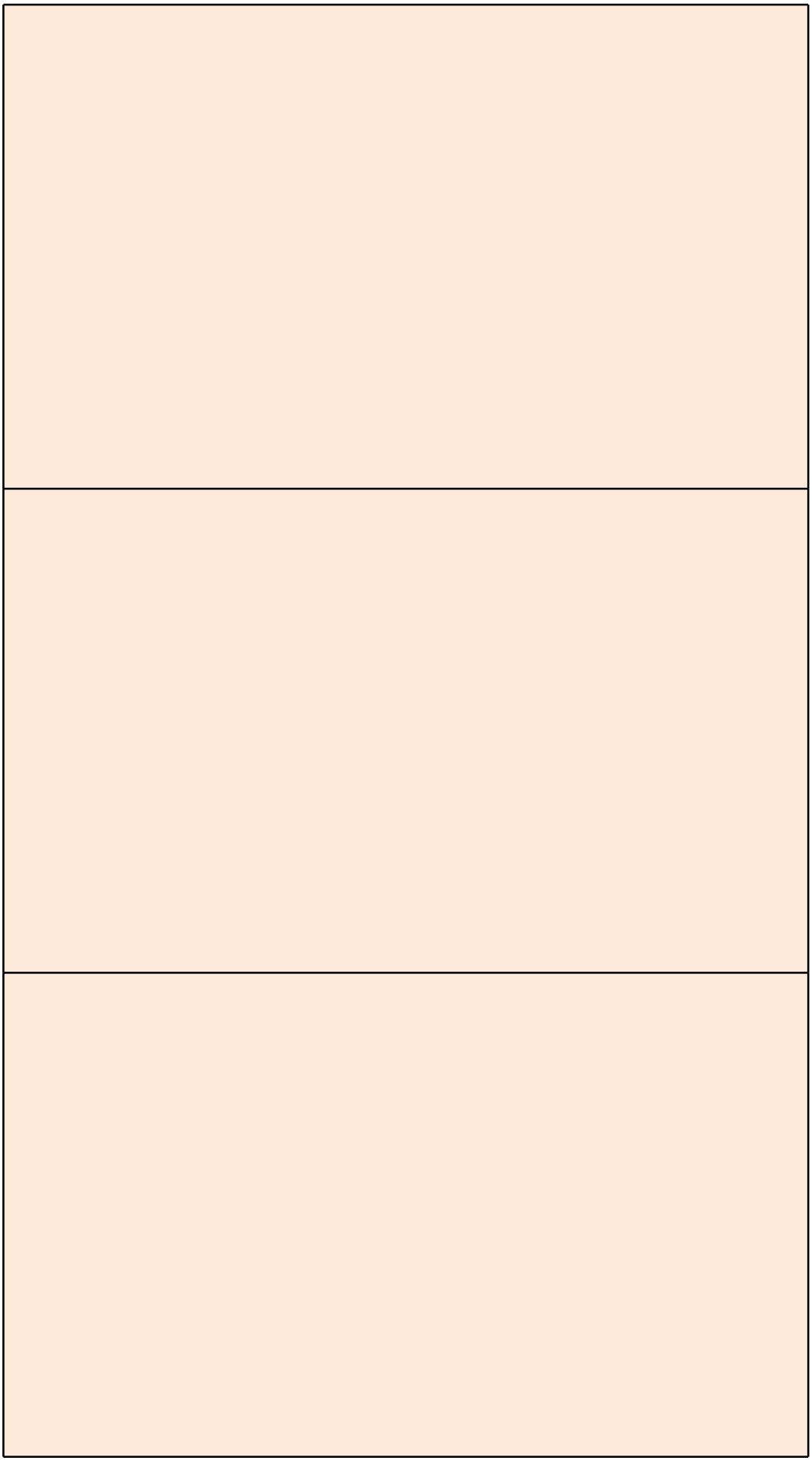


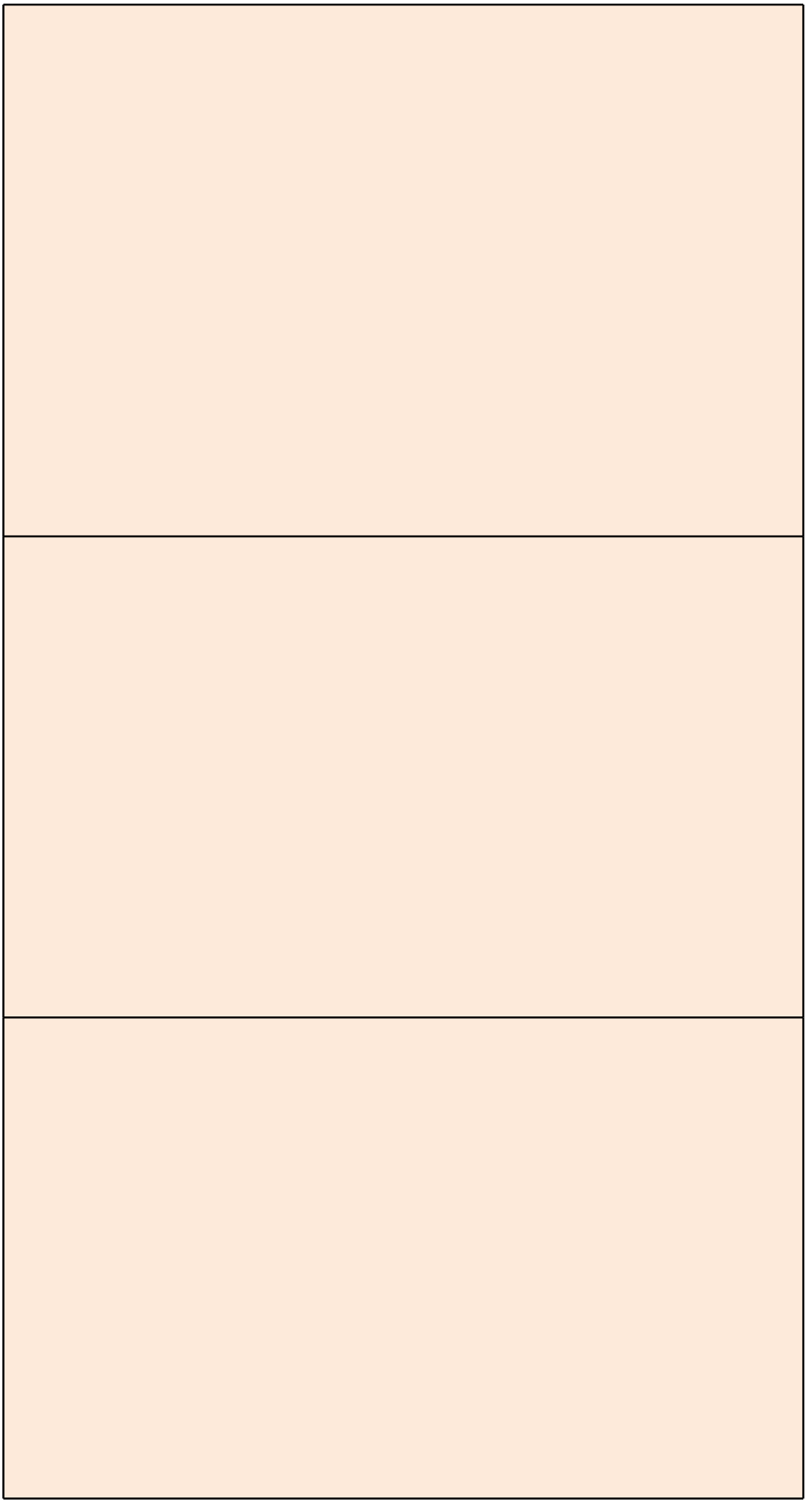


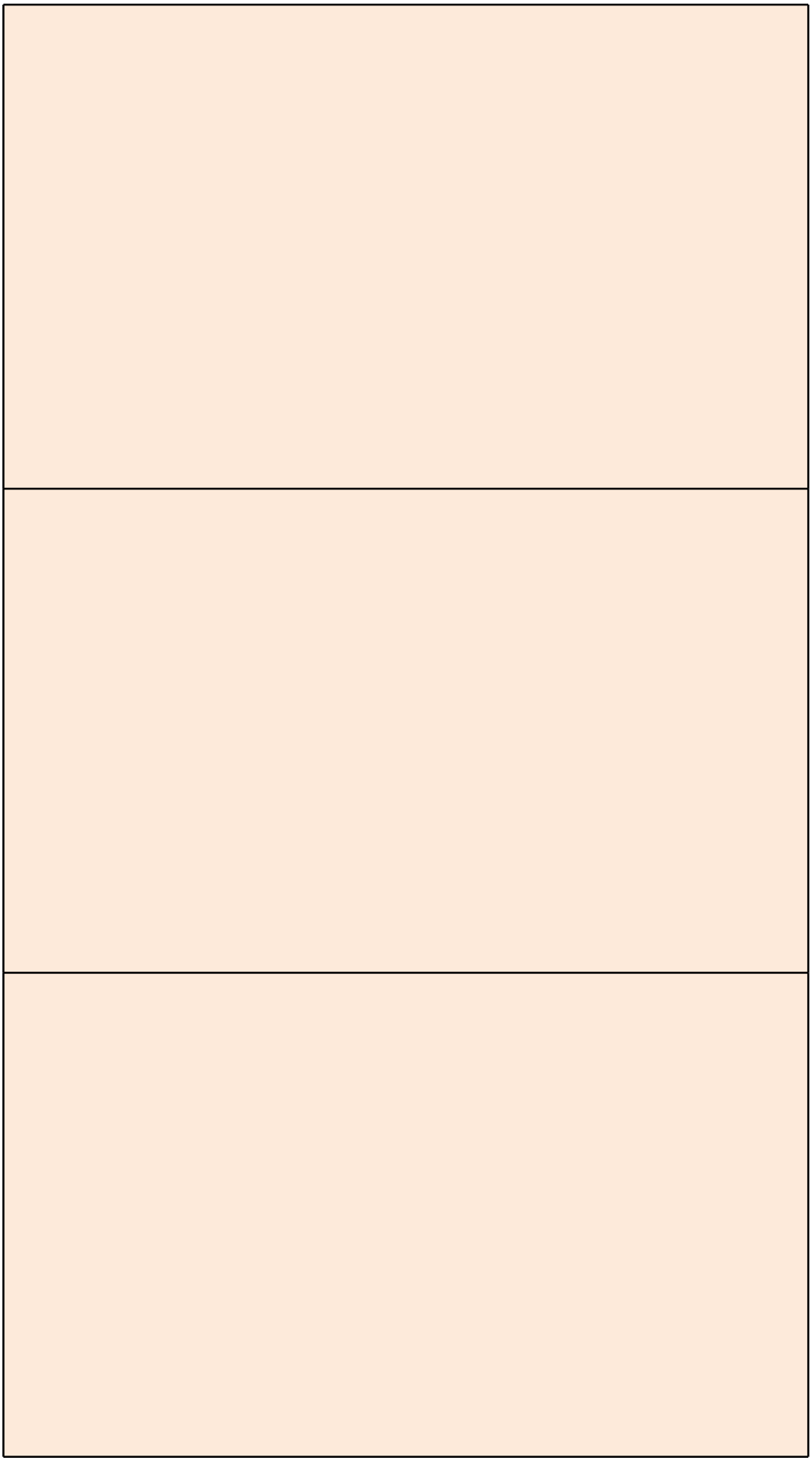


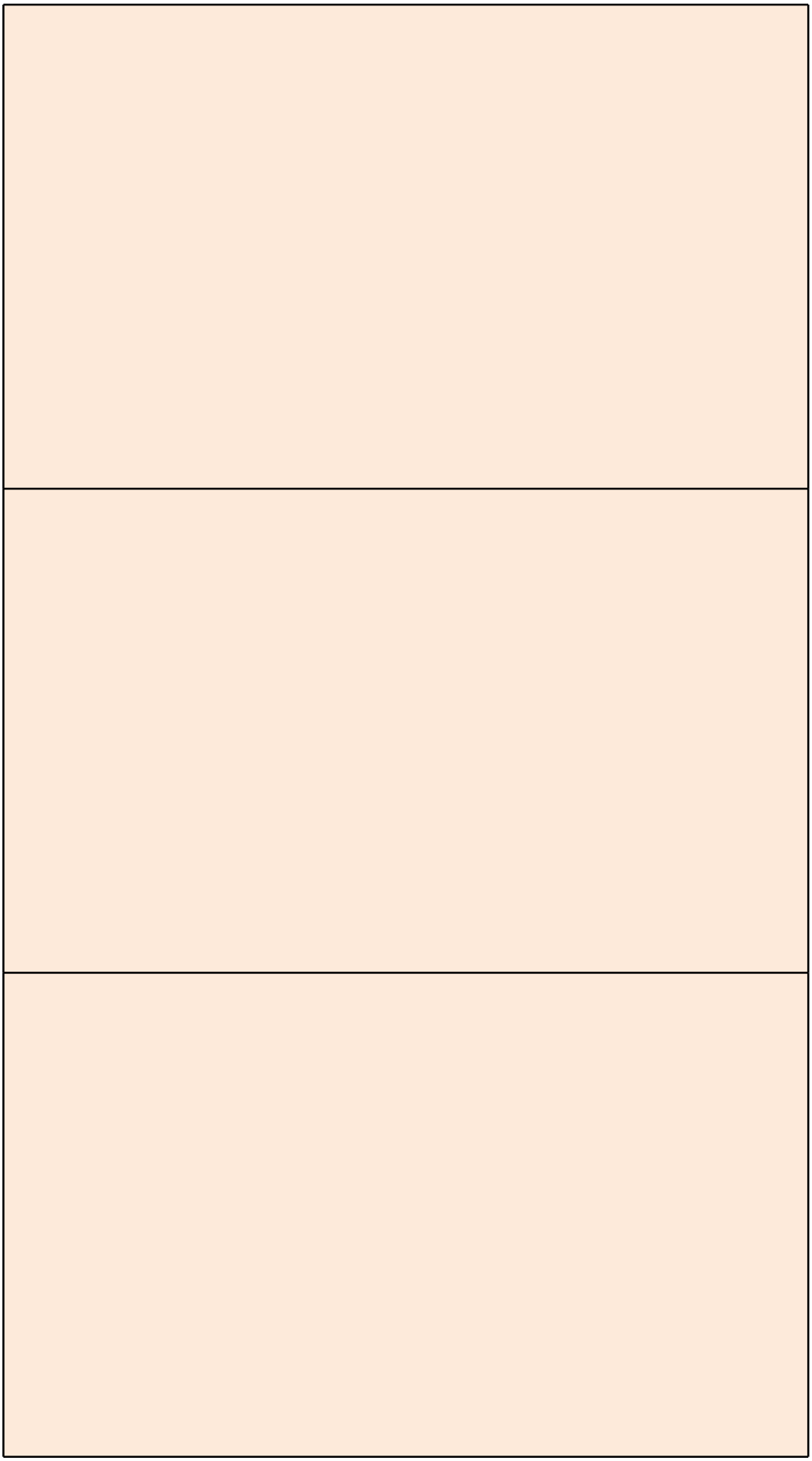
Ehdotuksen perustelut

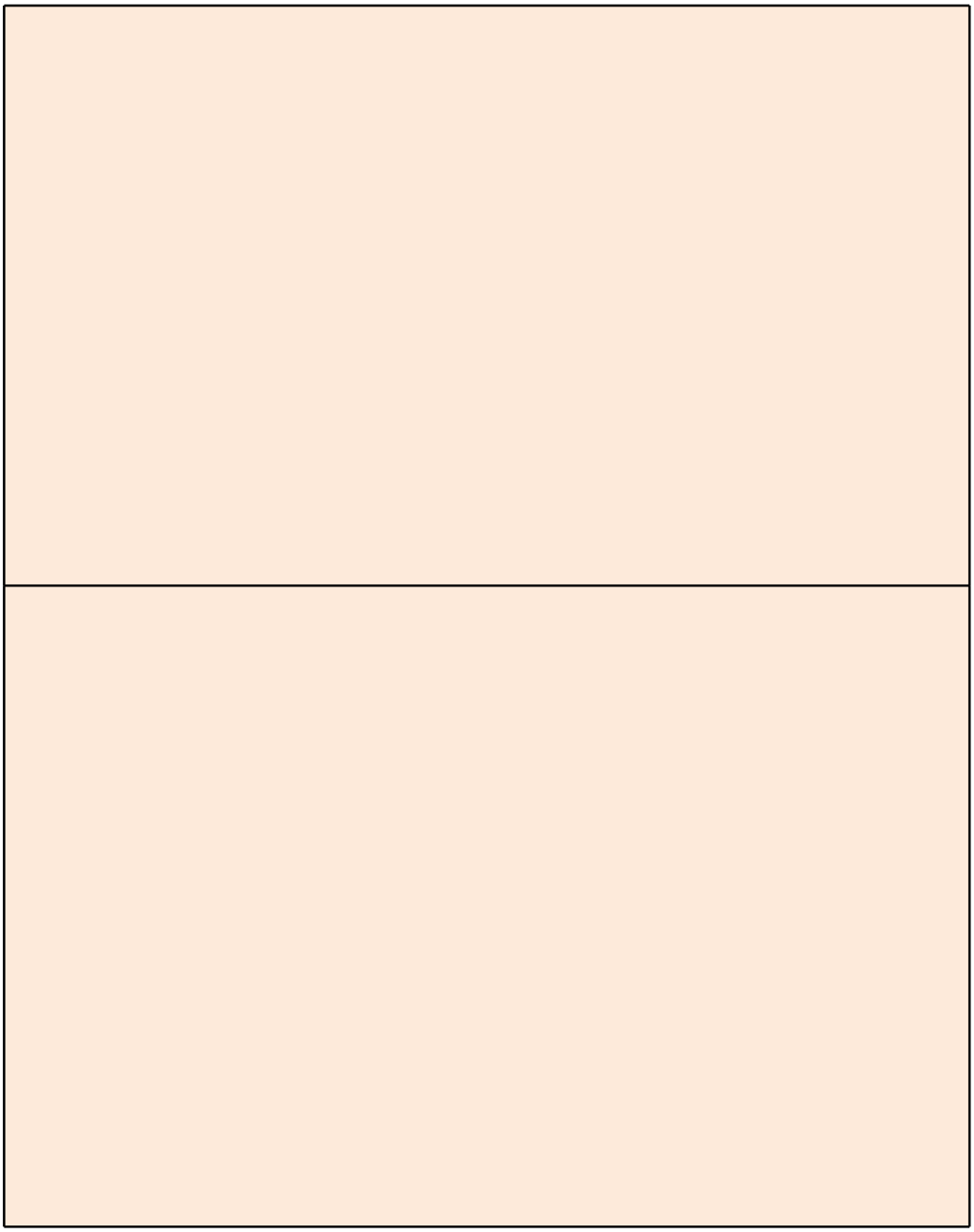


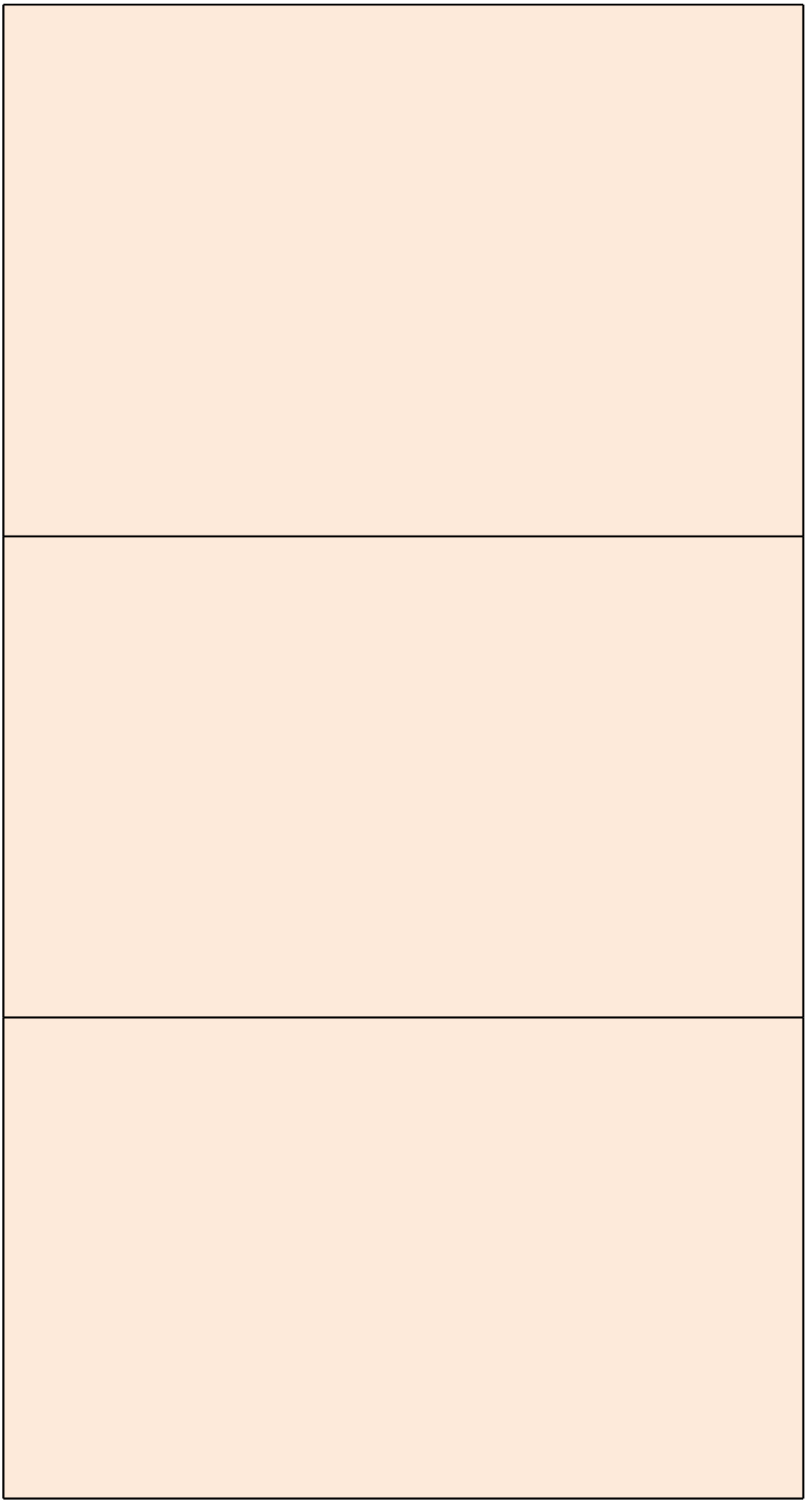


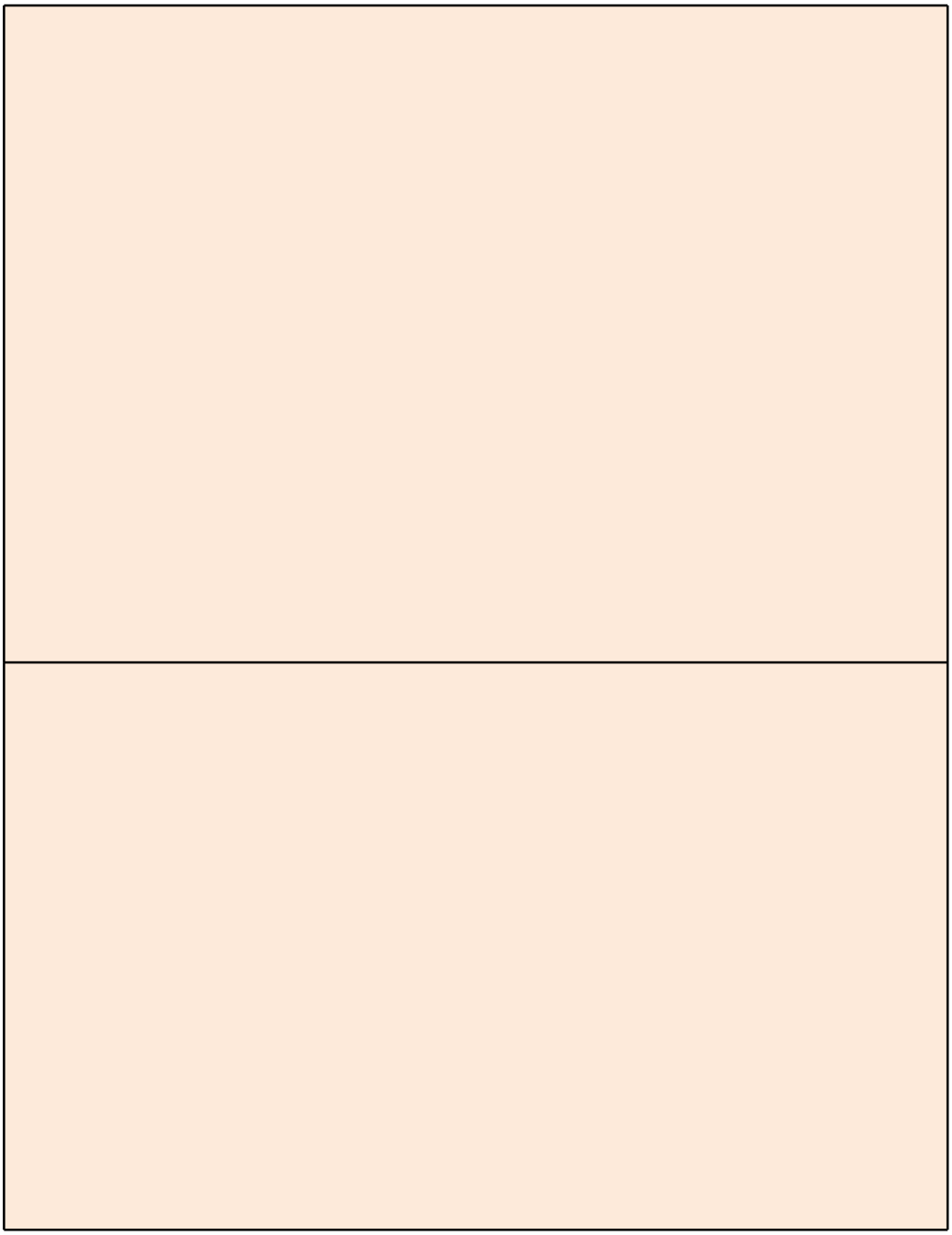


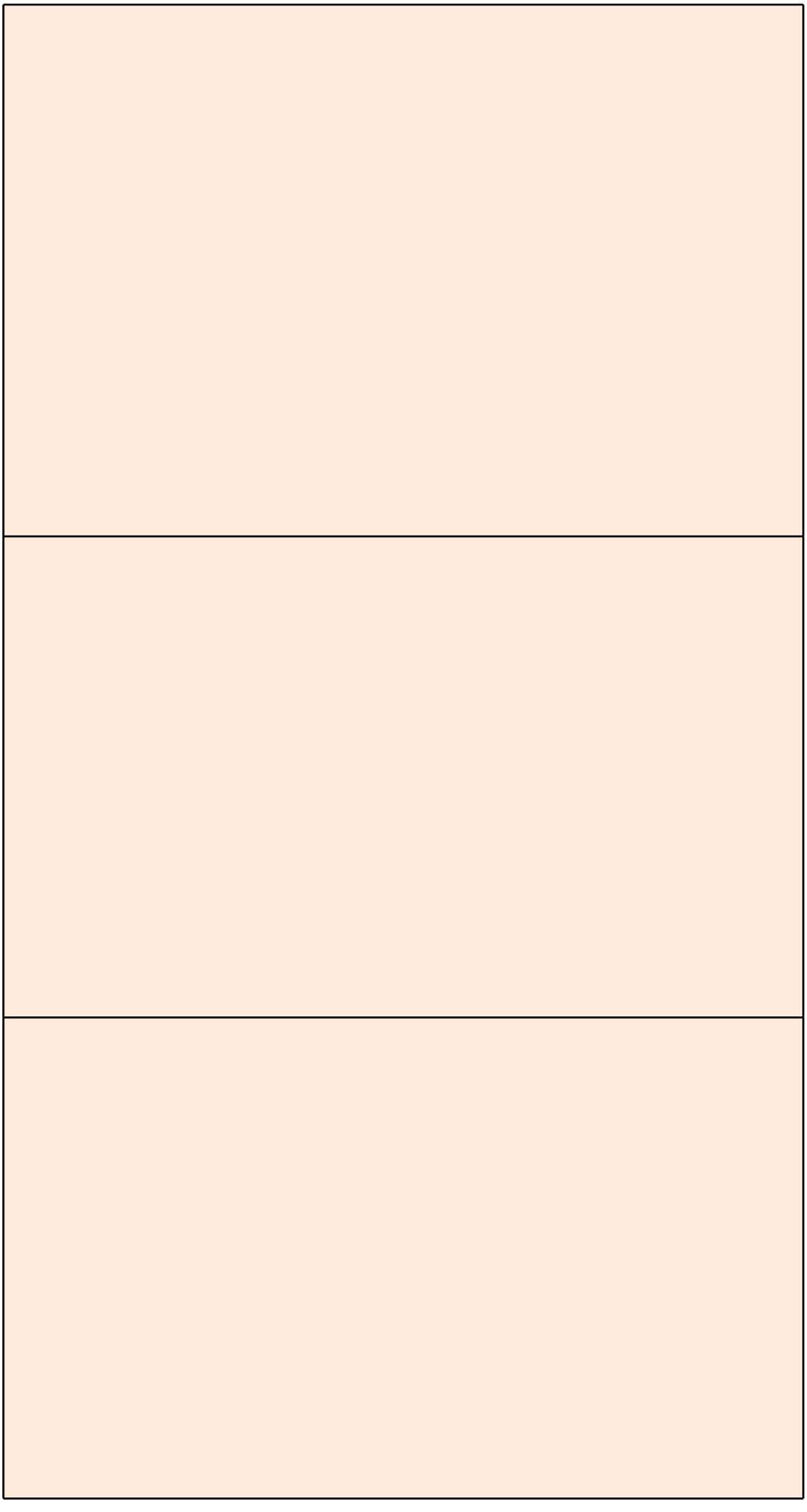


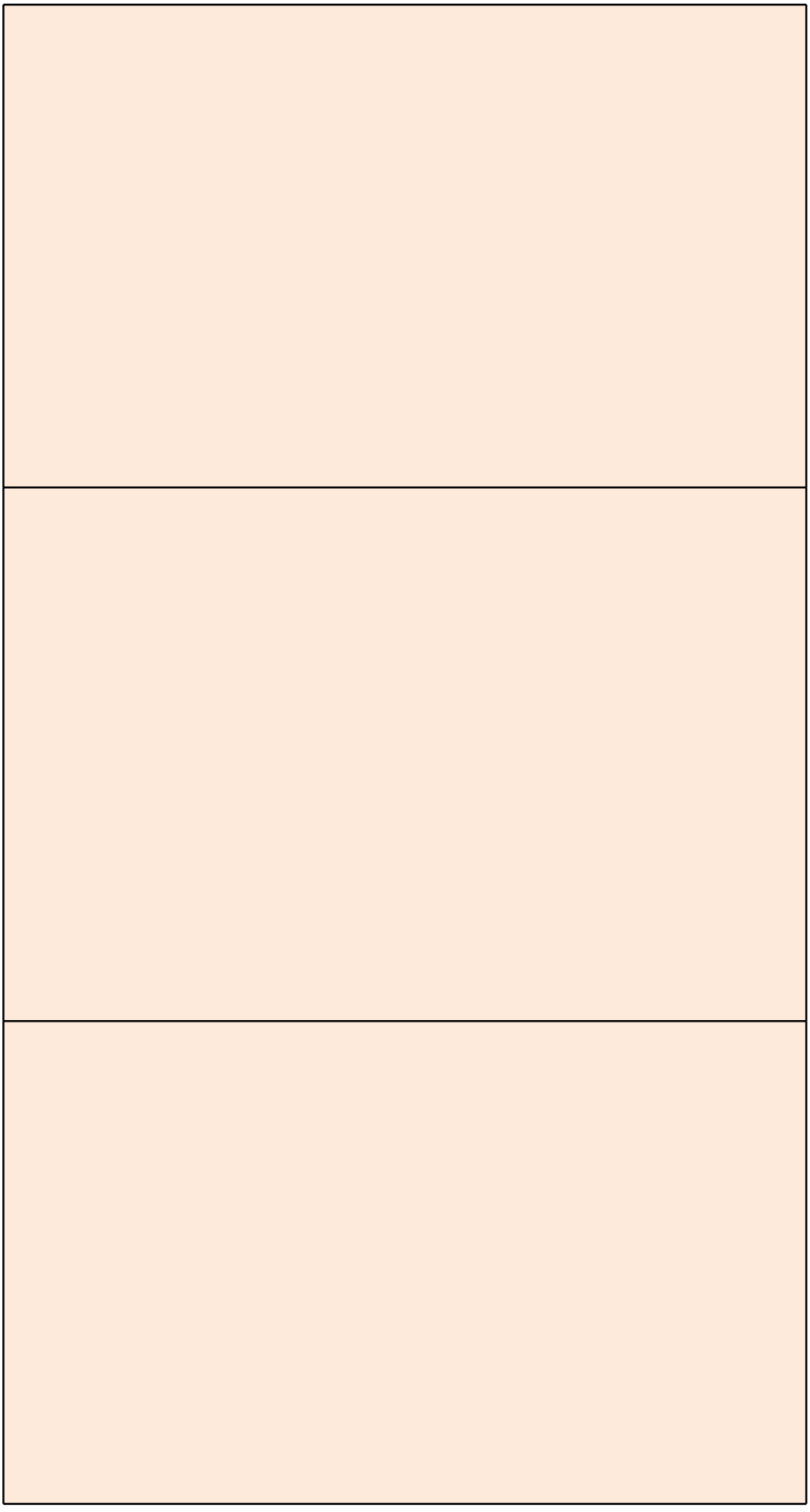


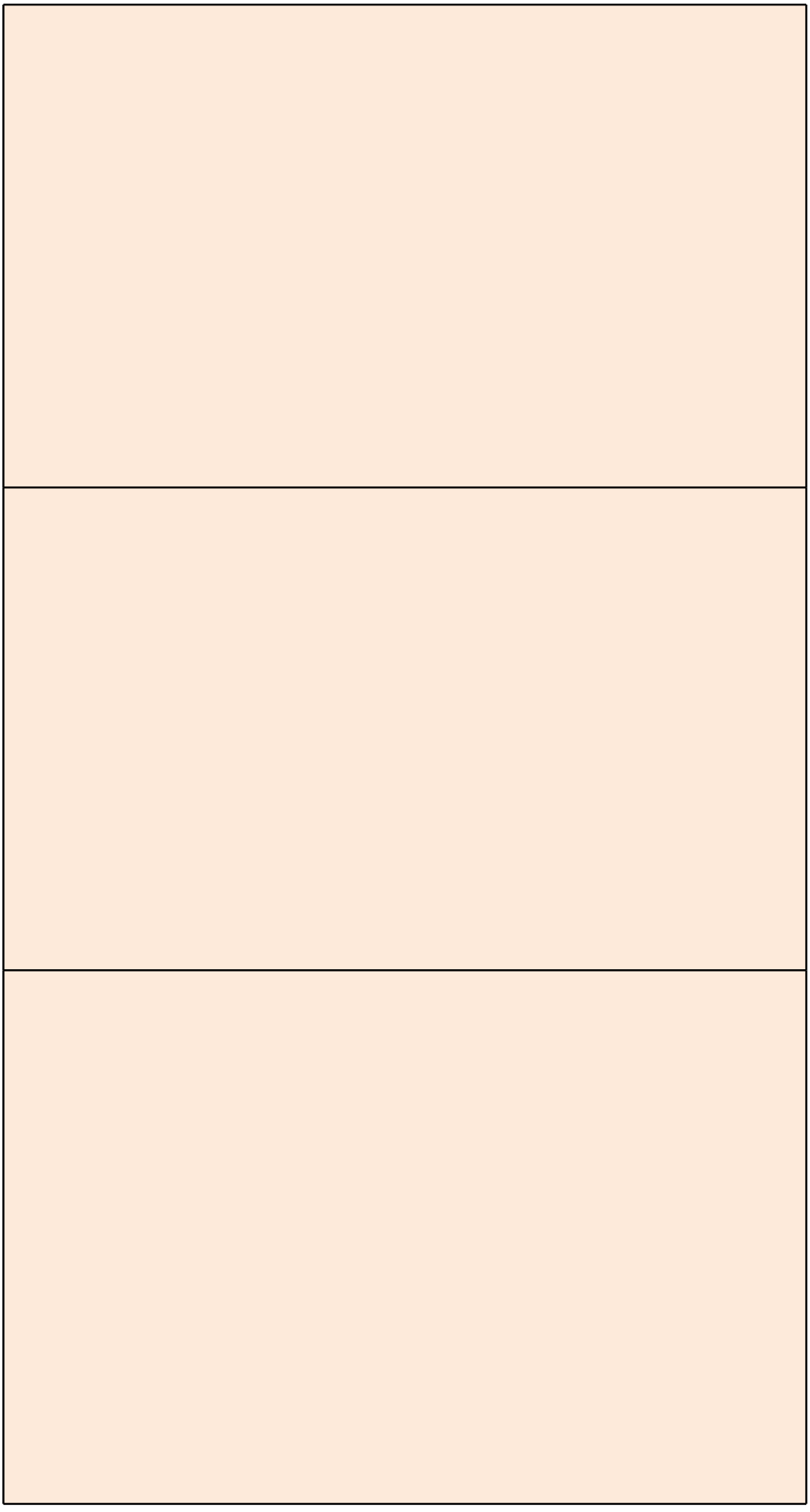


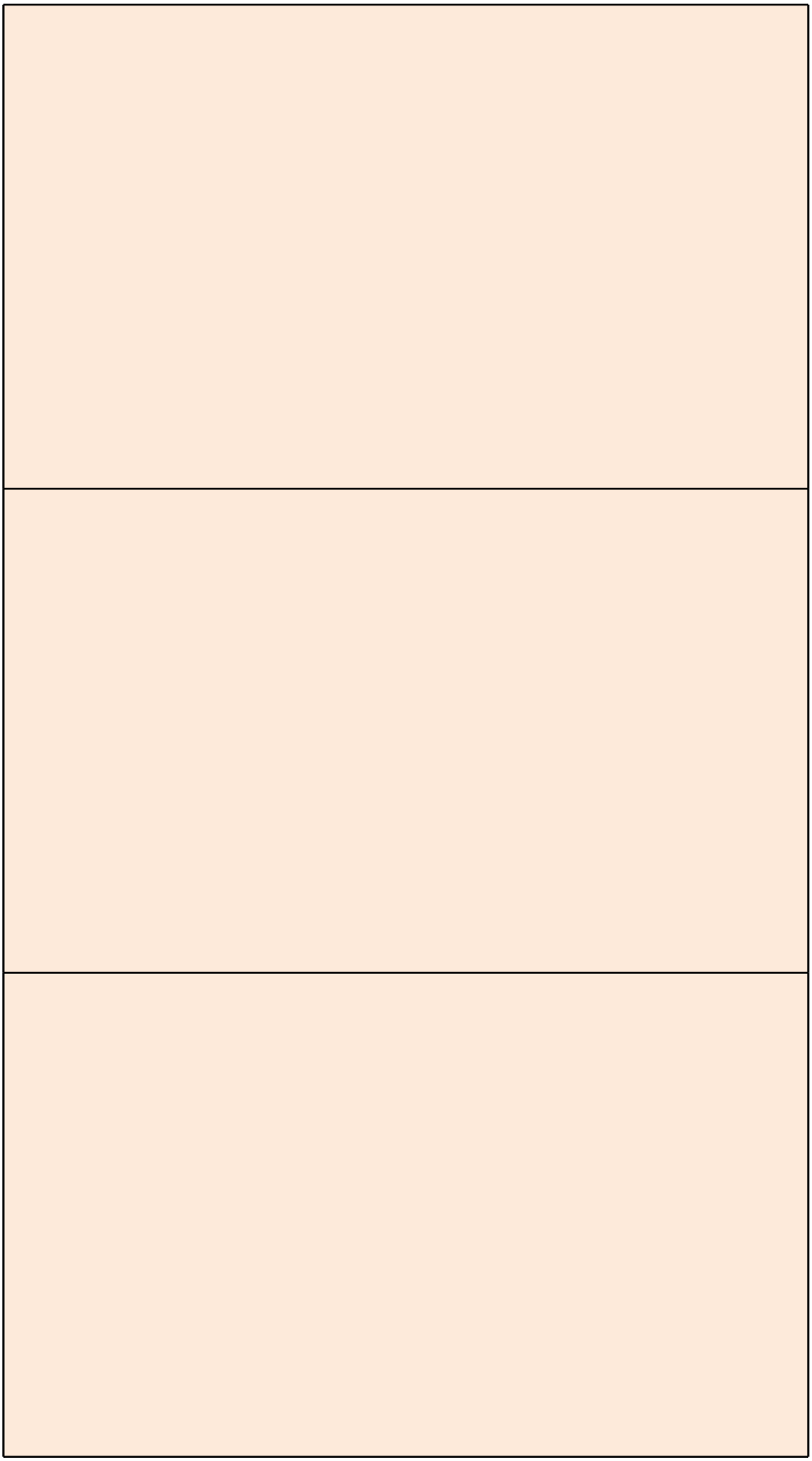


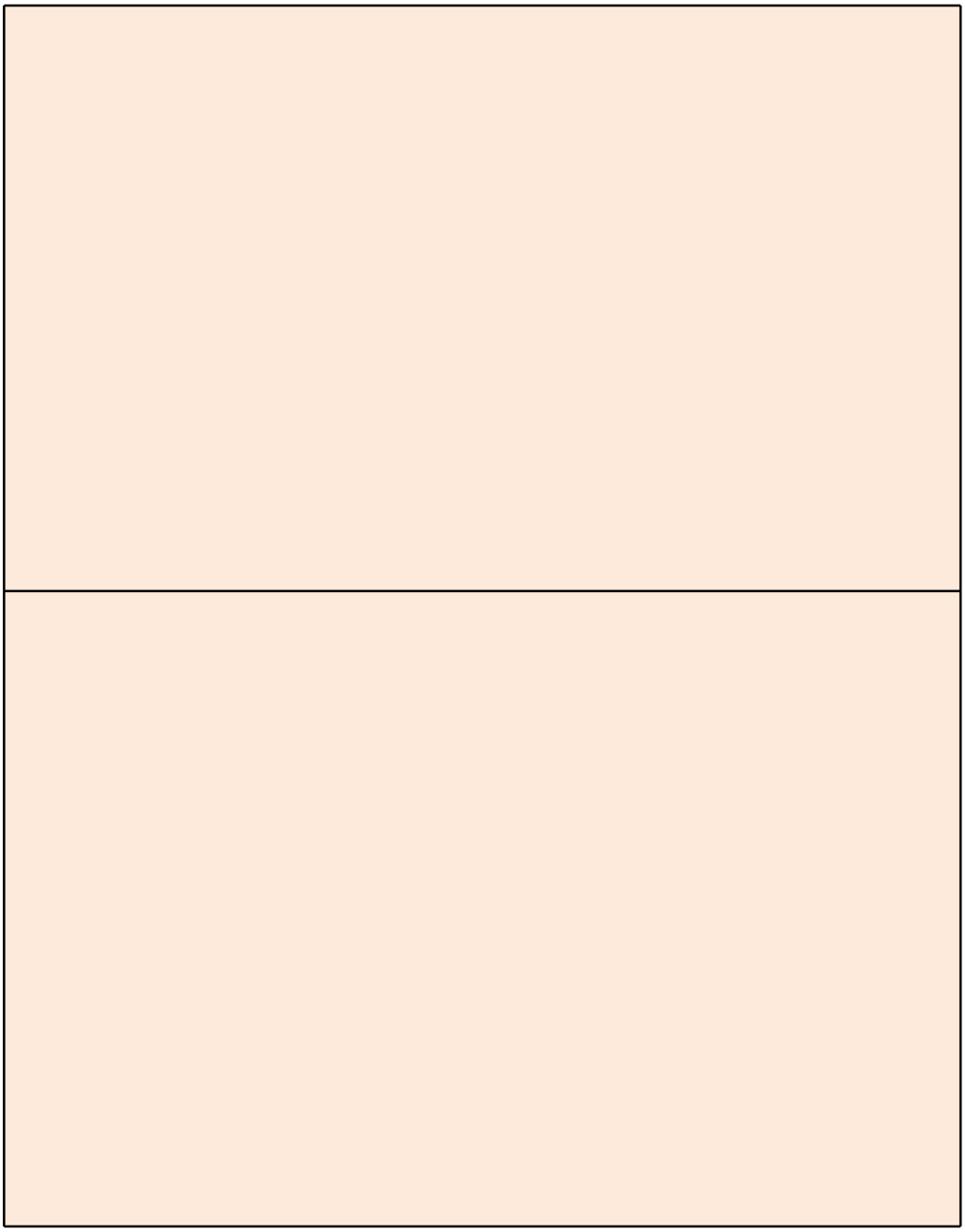


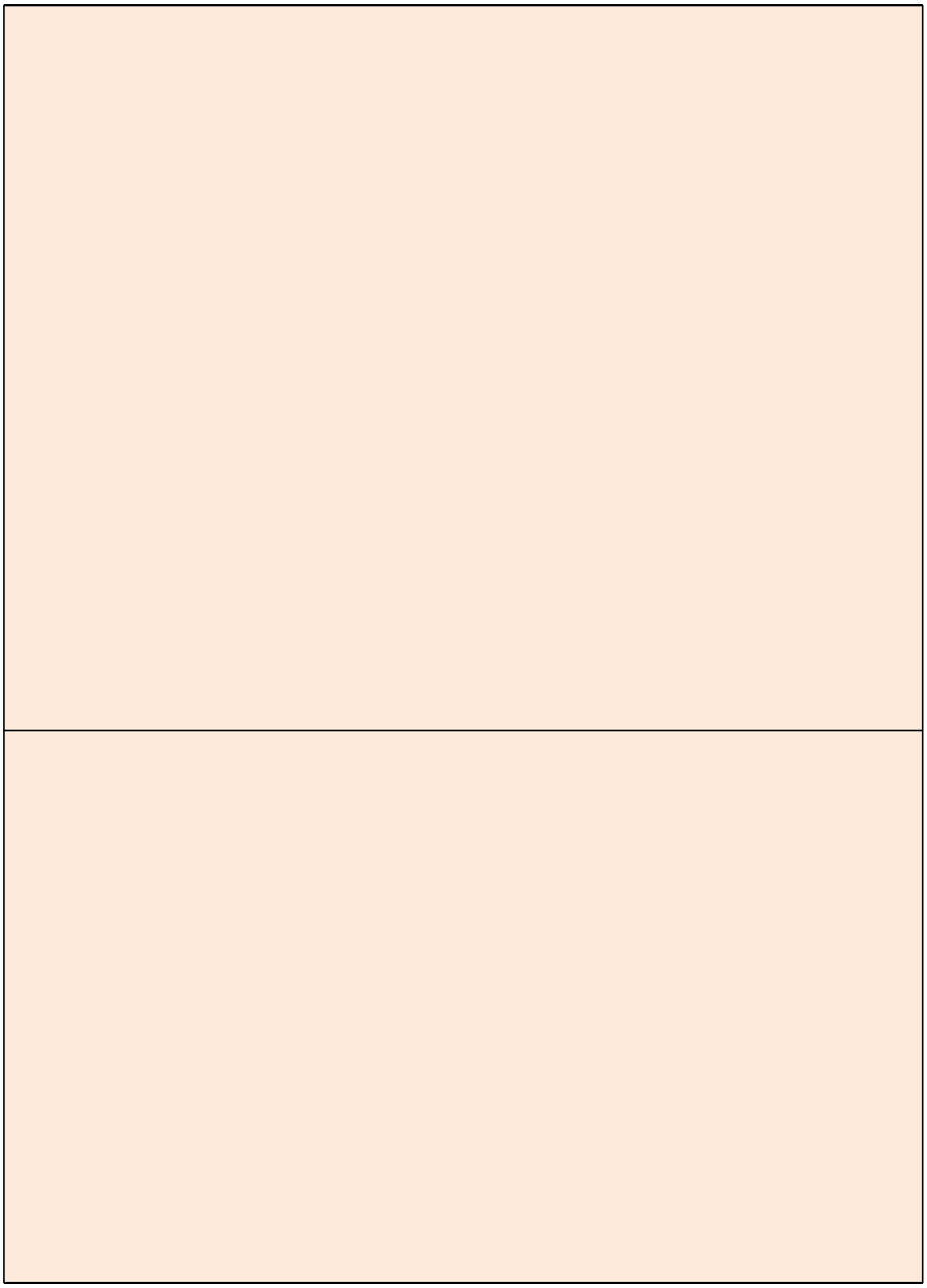


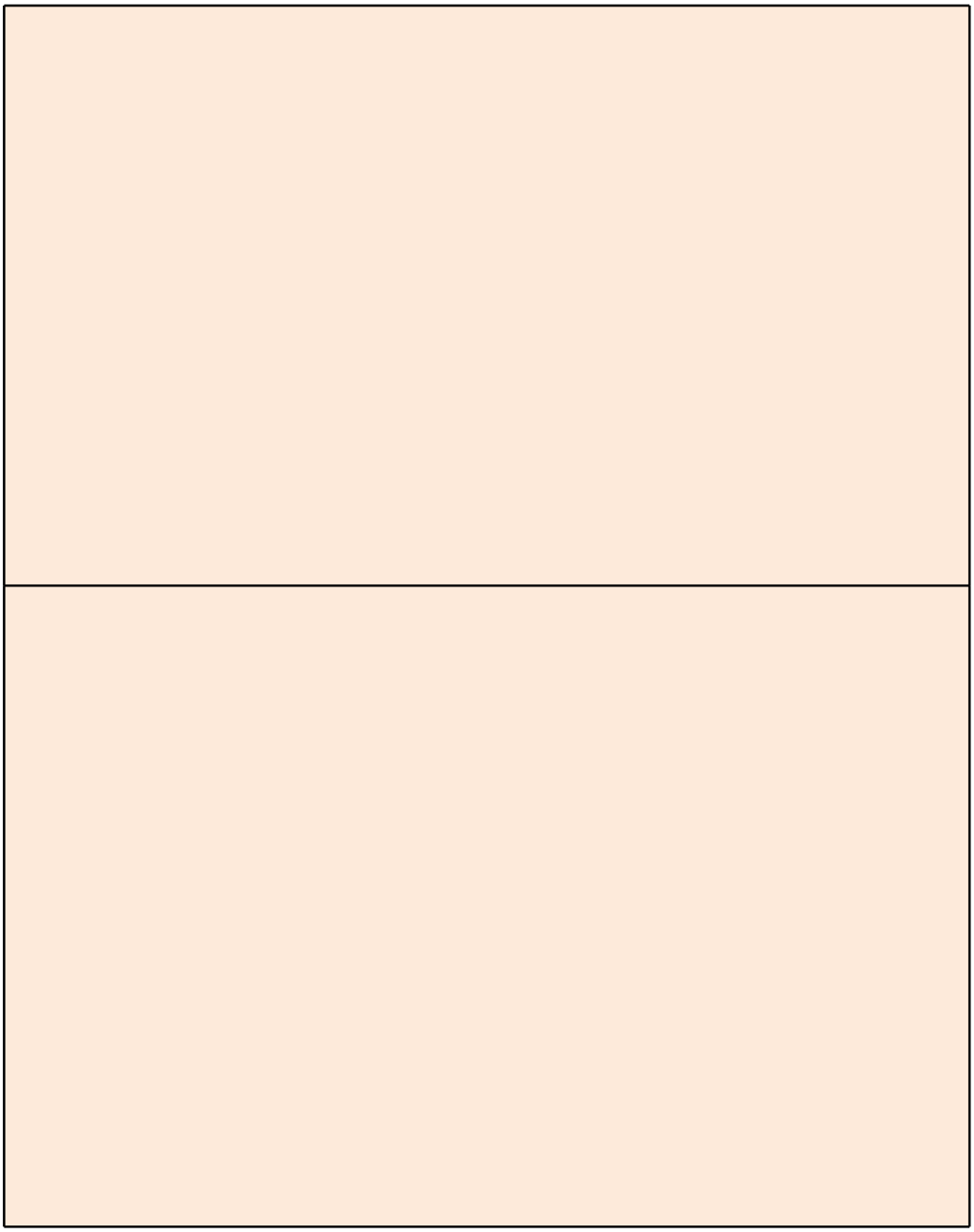


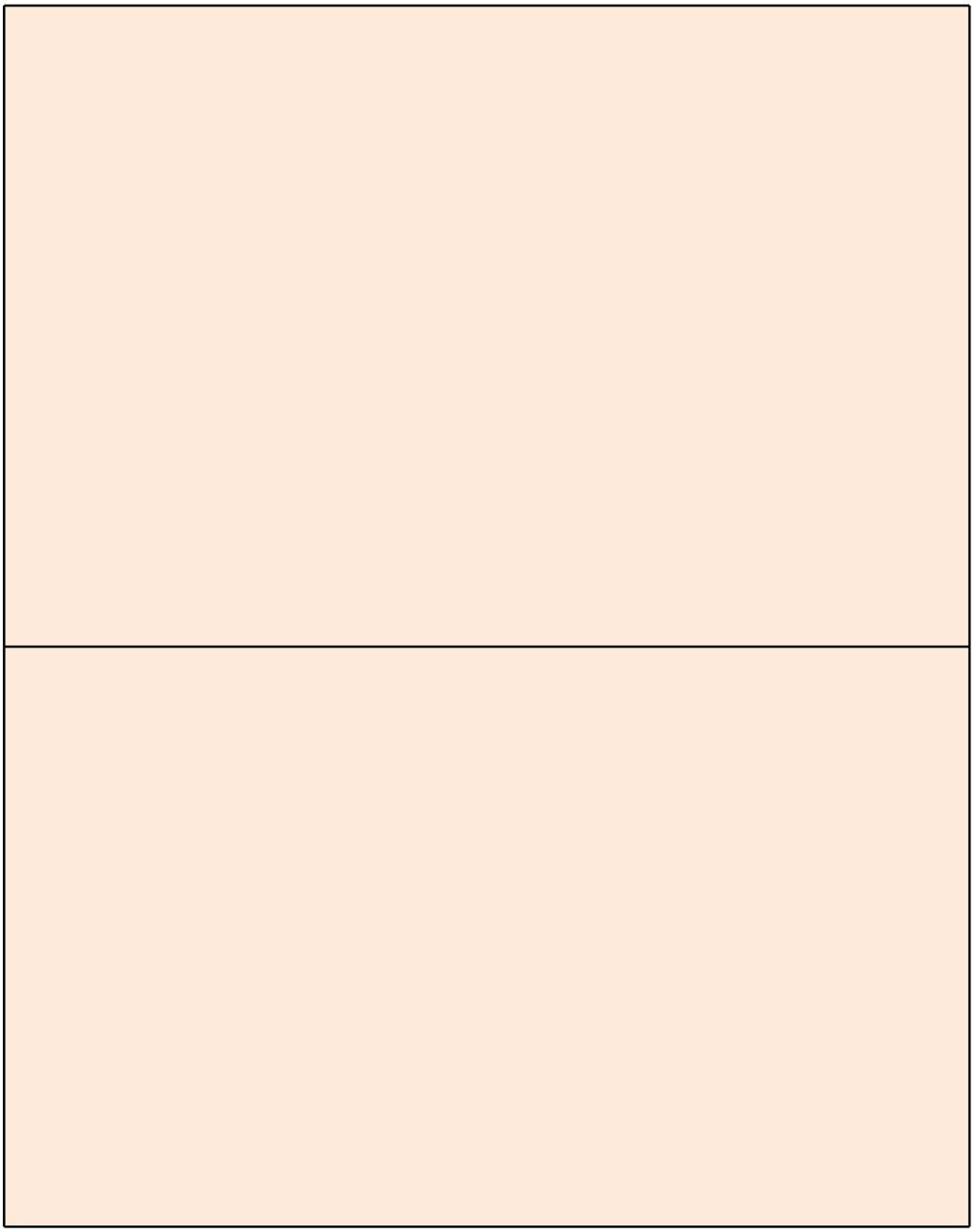


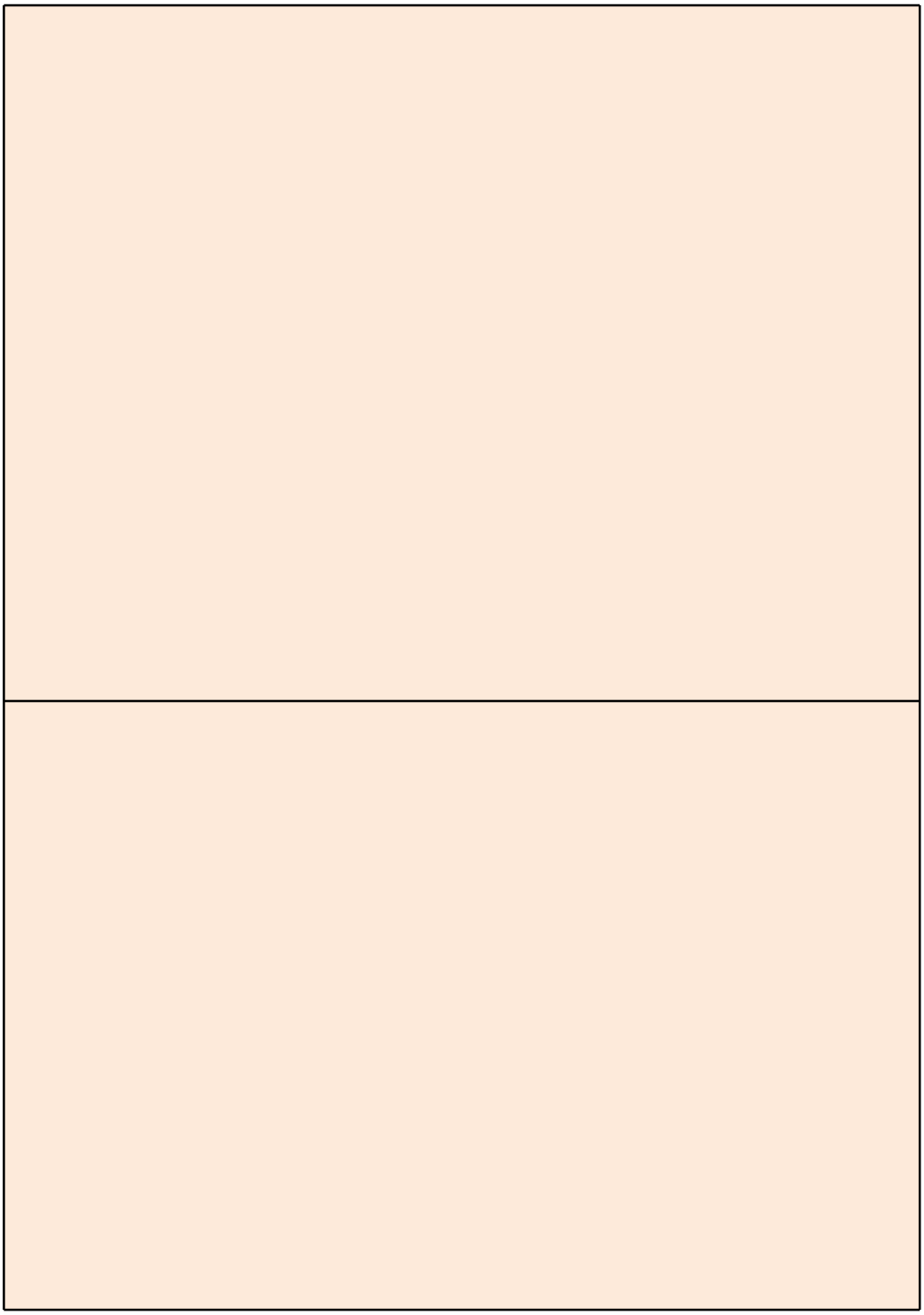


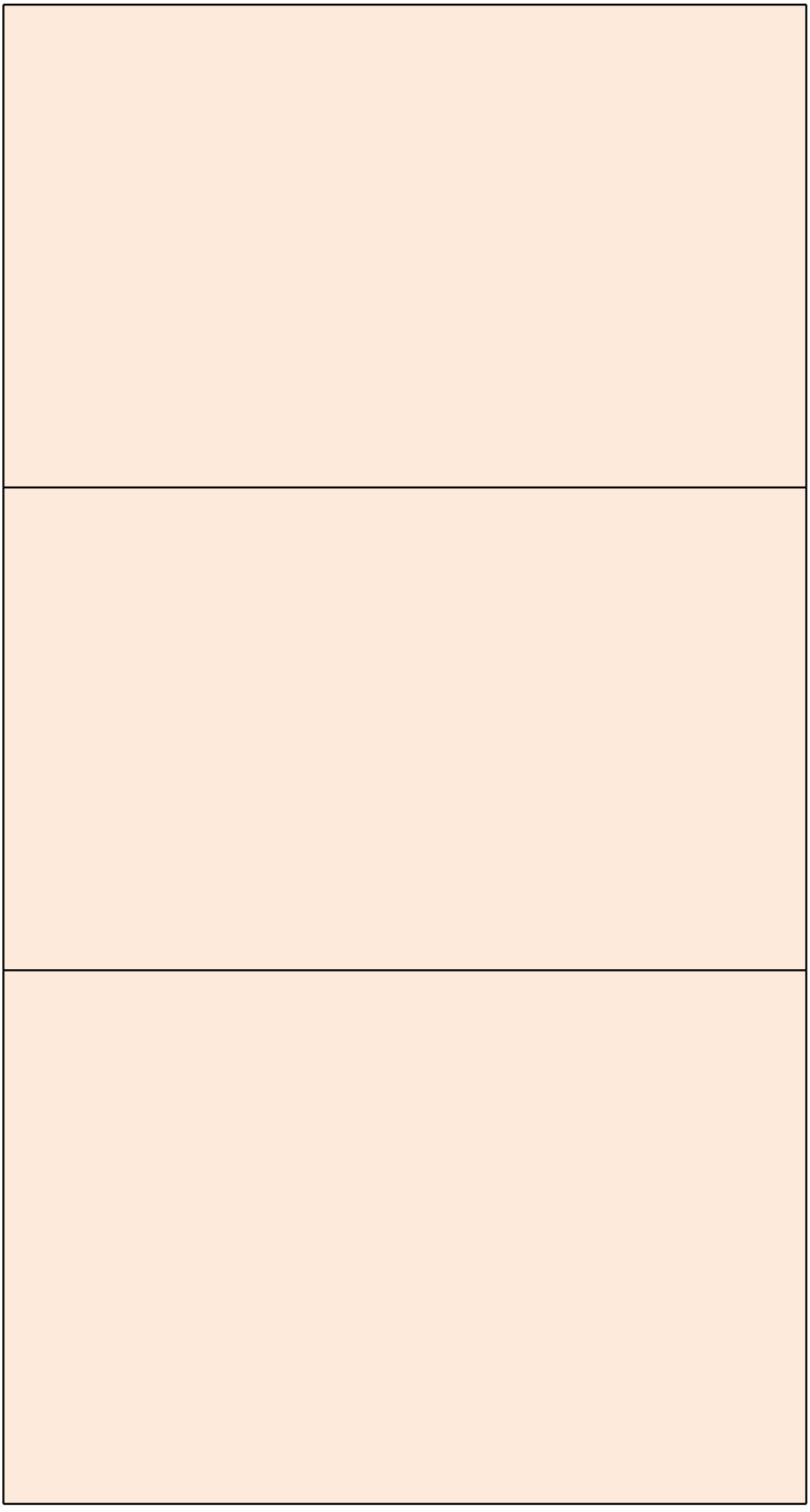


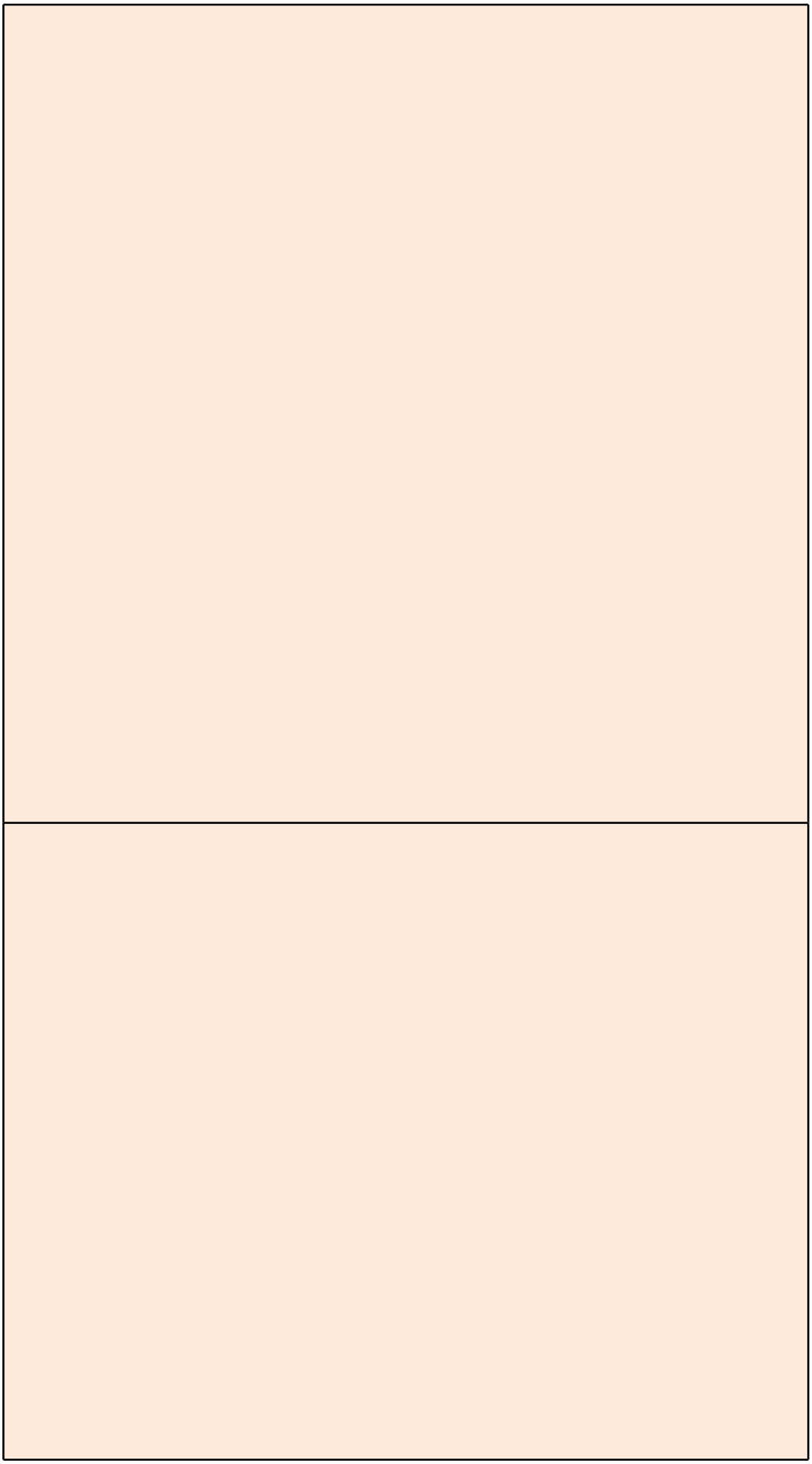


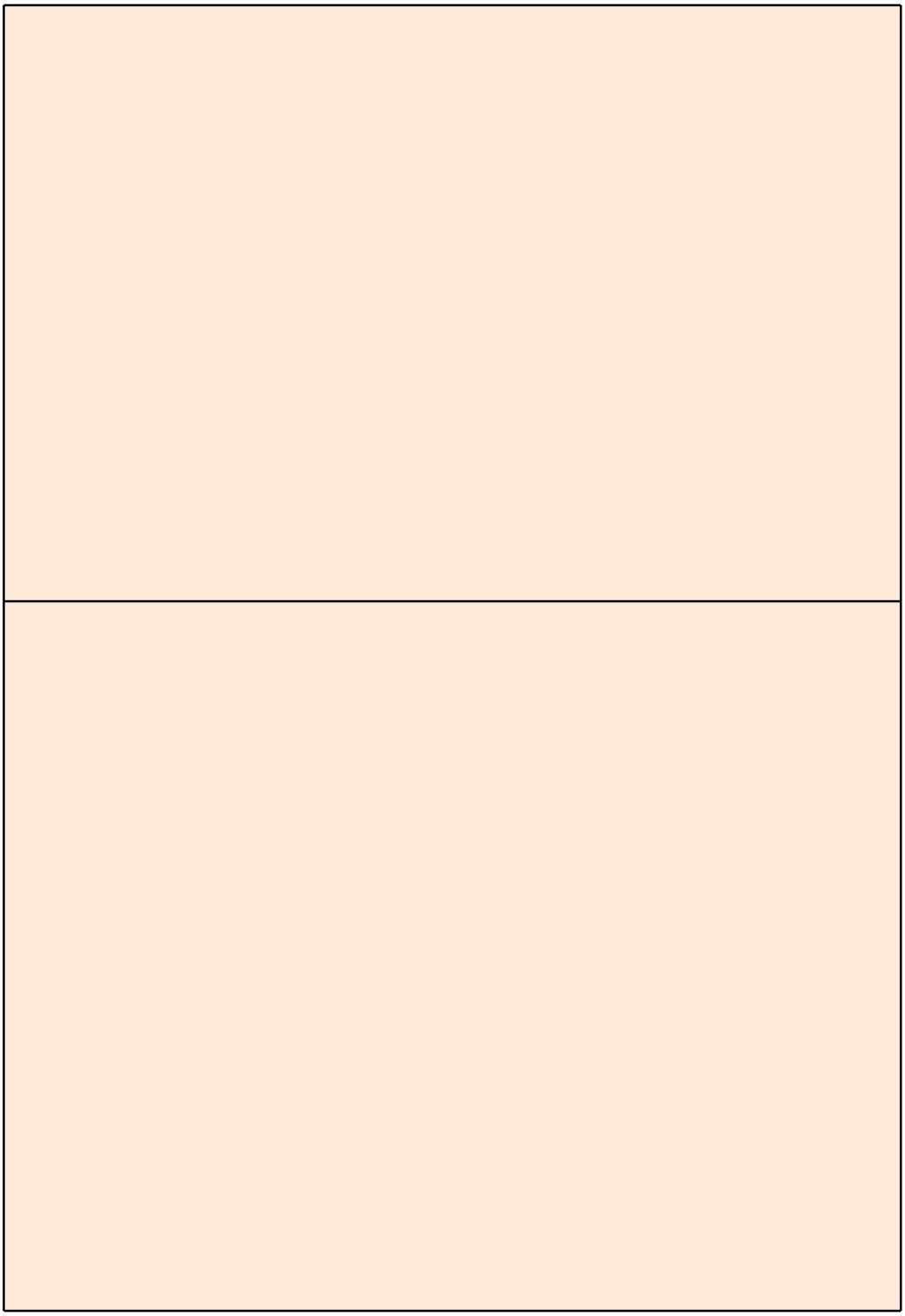


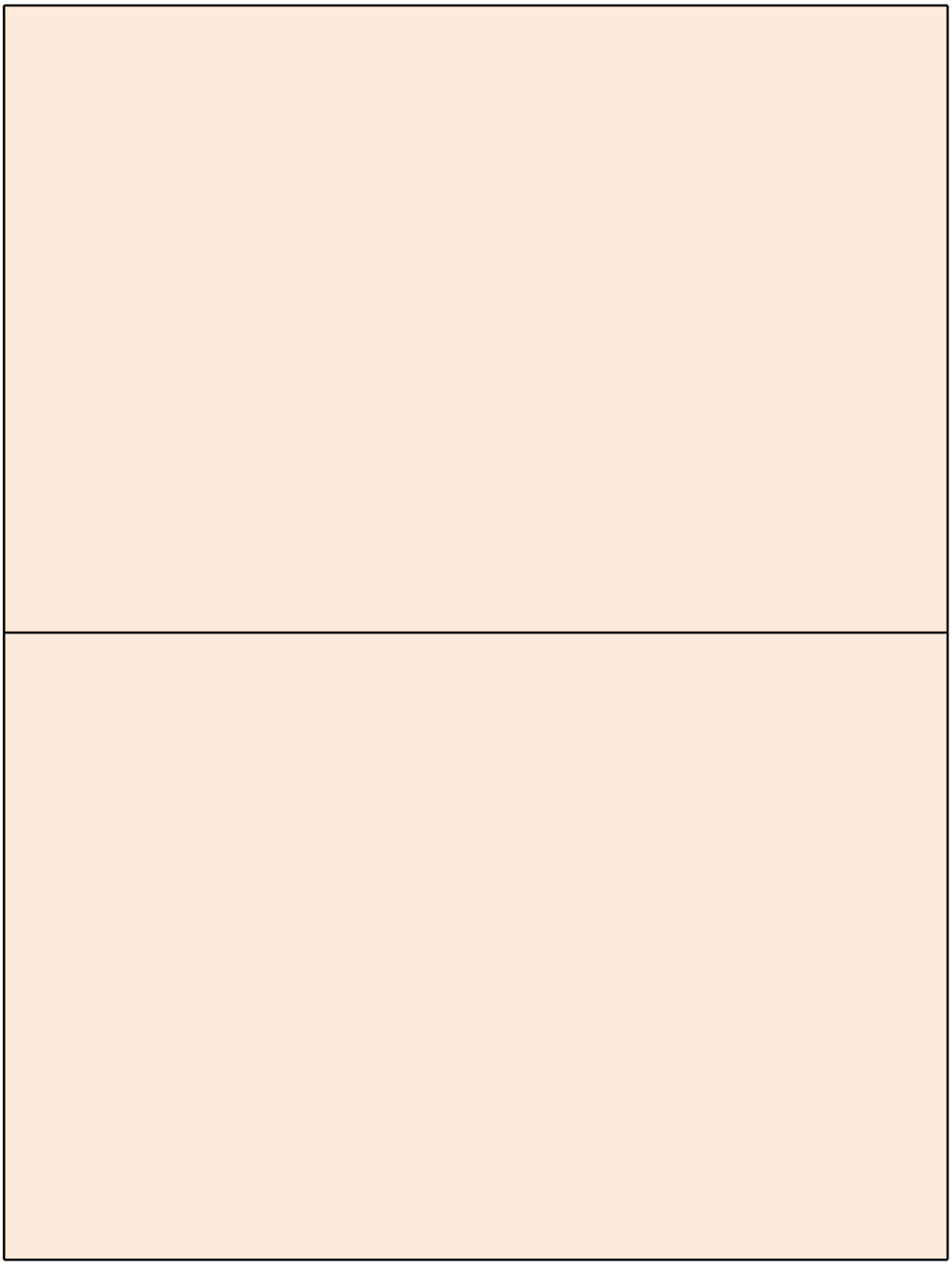


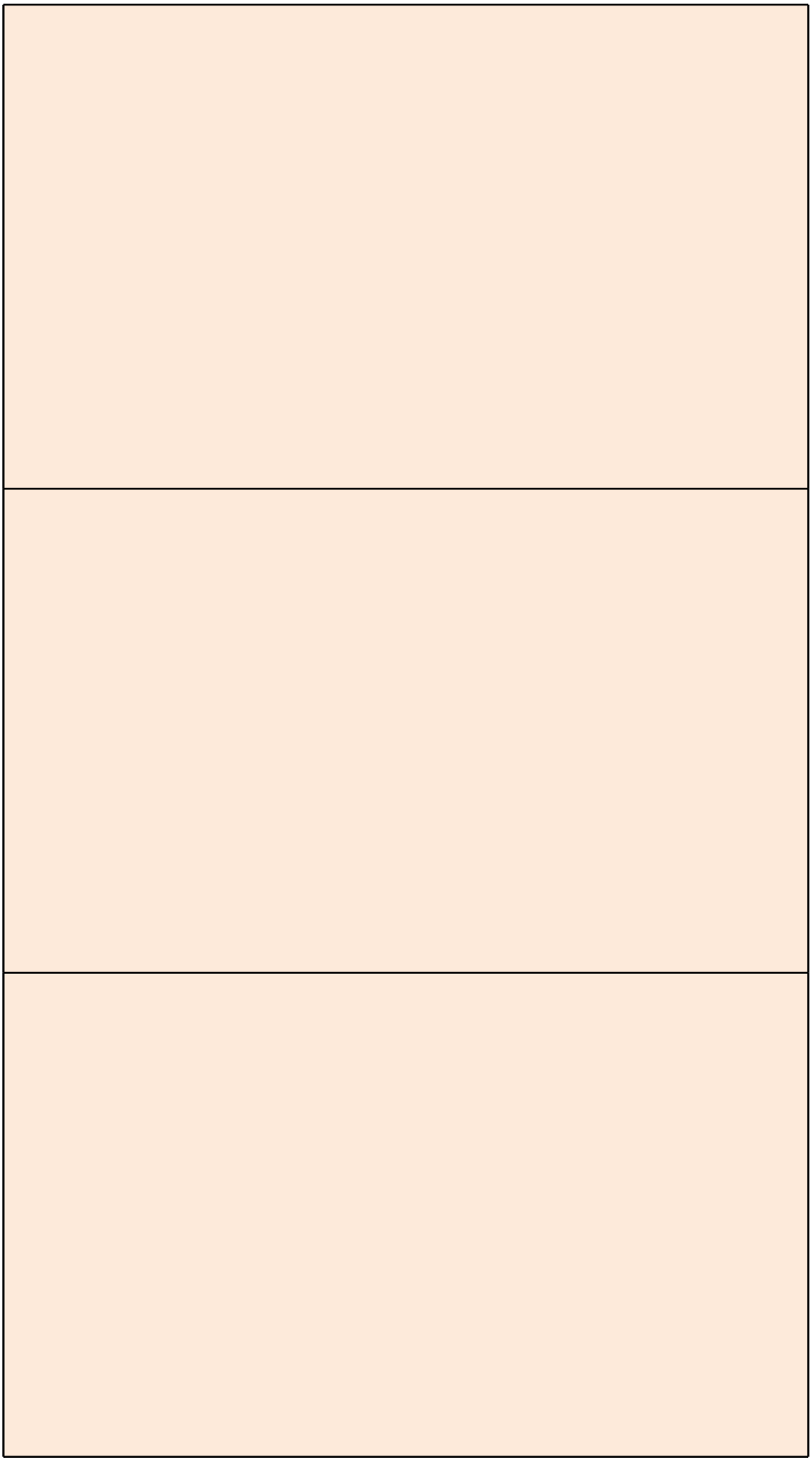


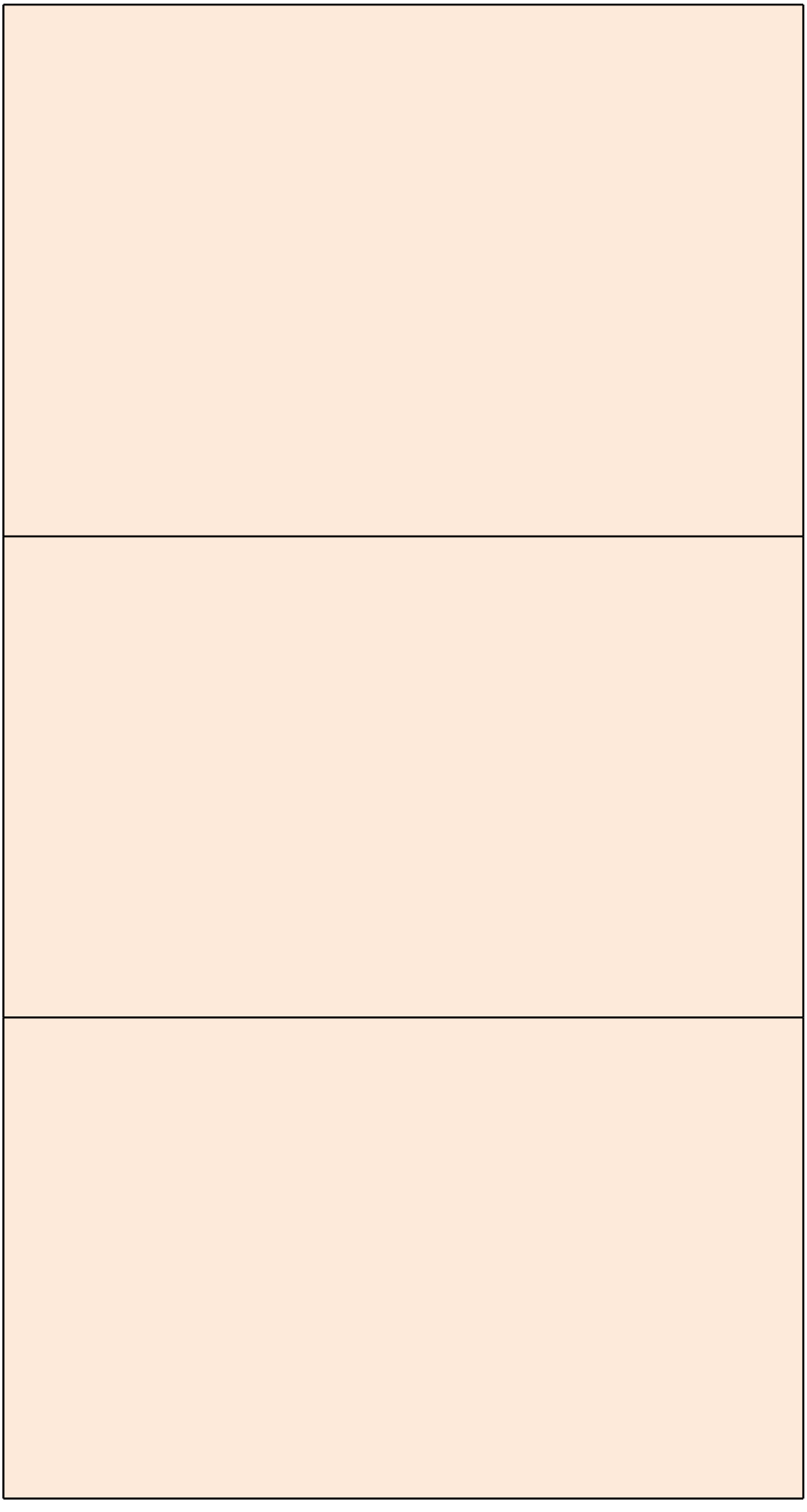


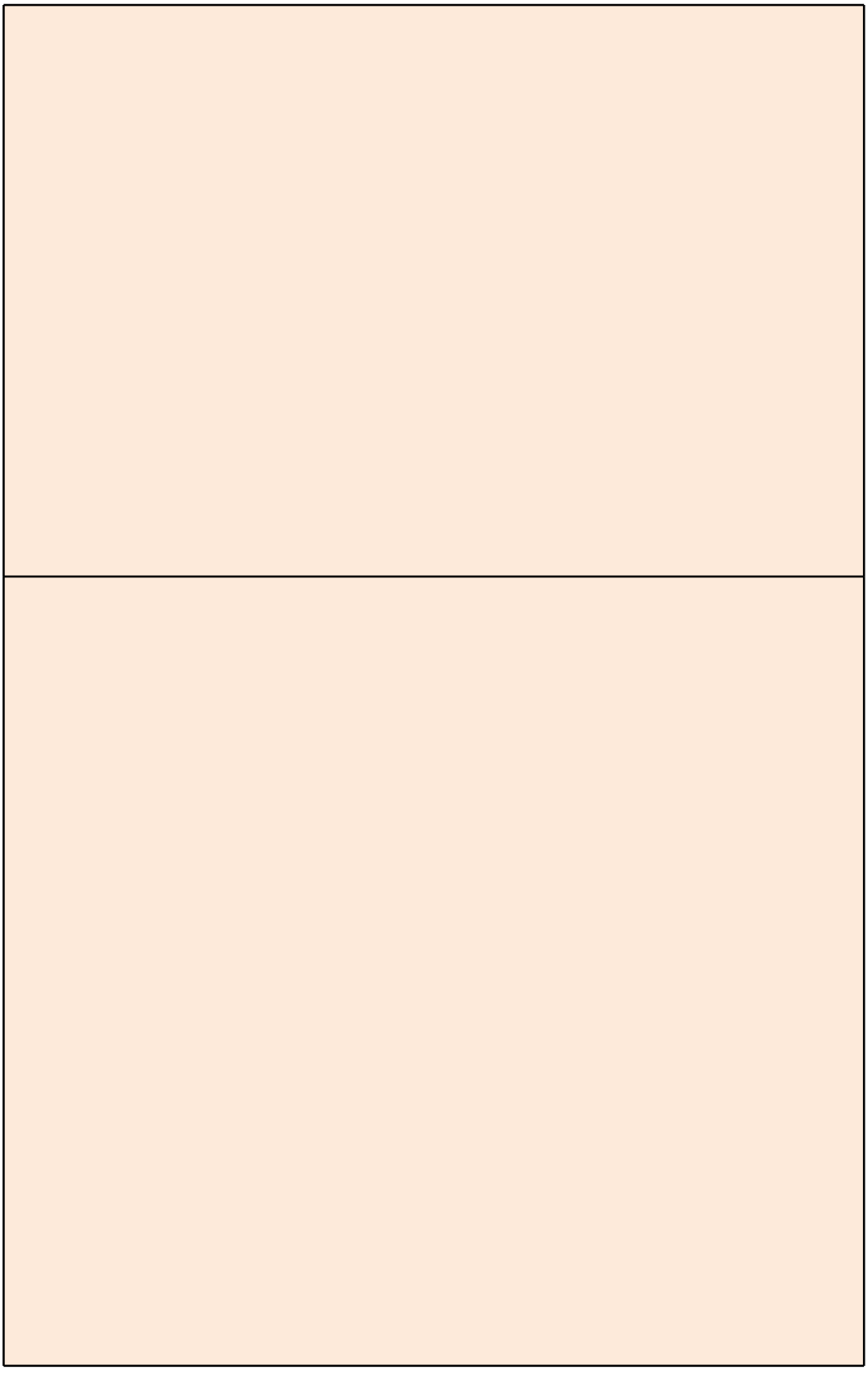


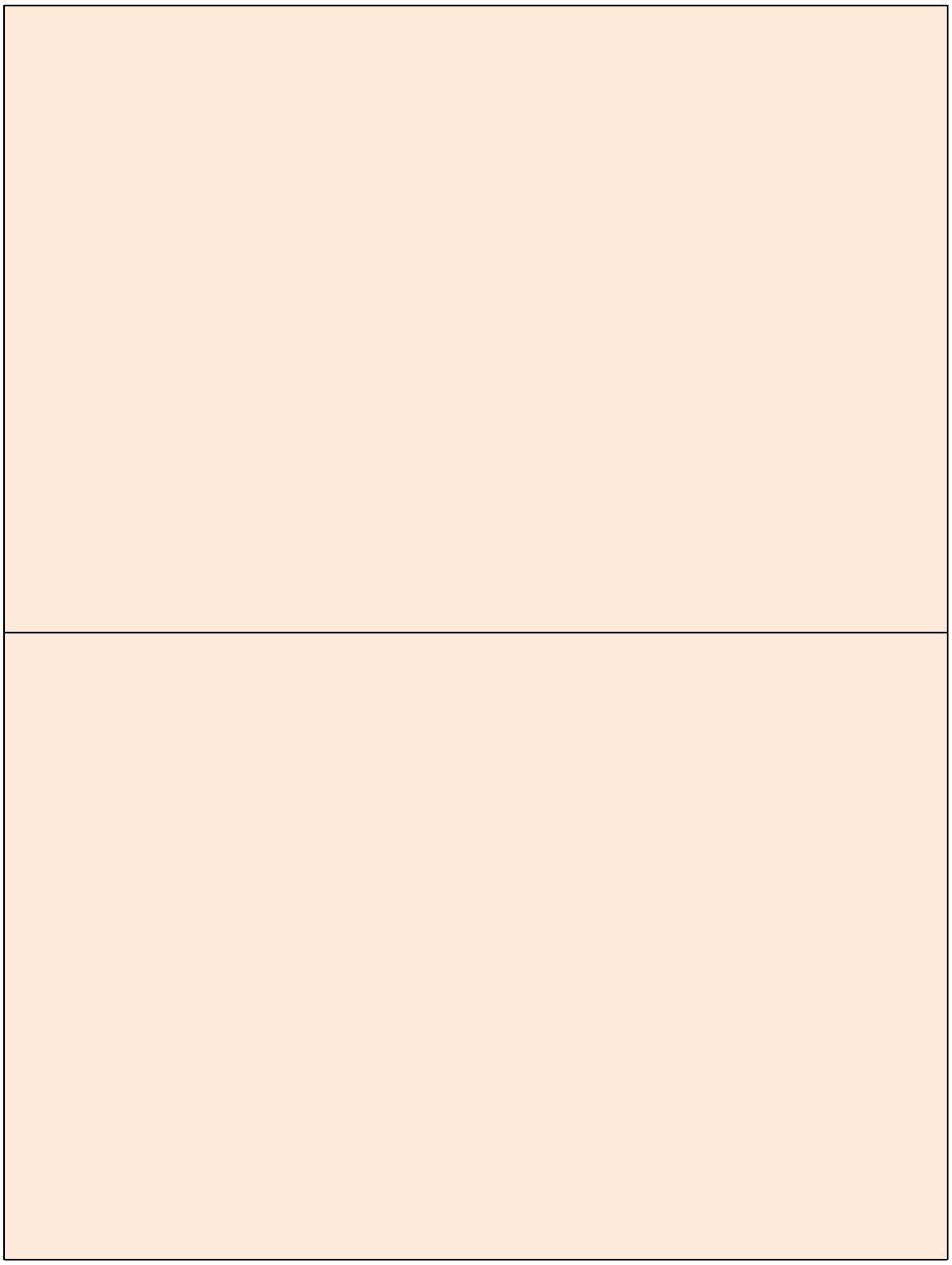


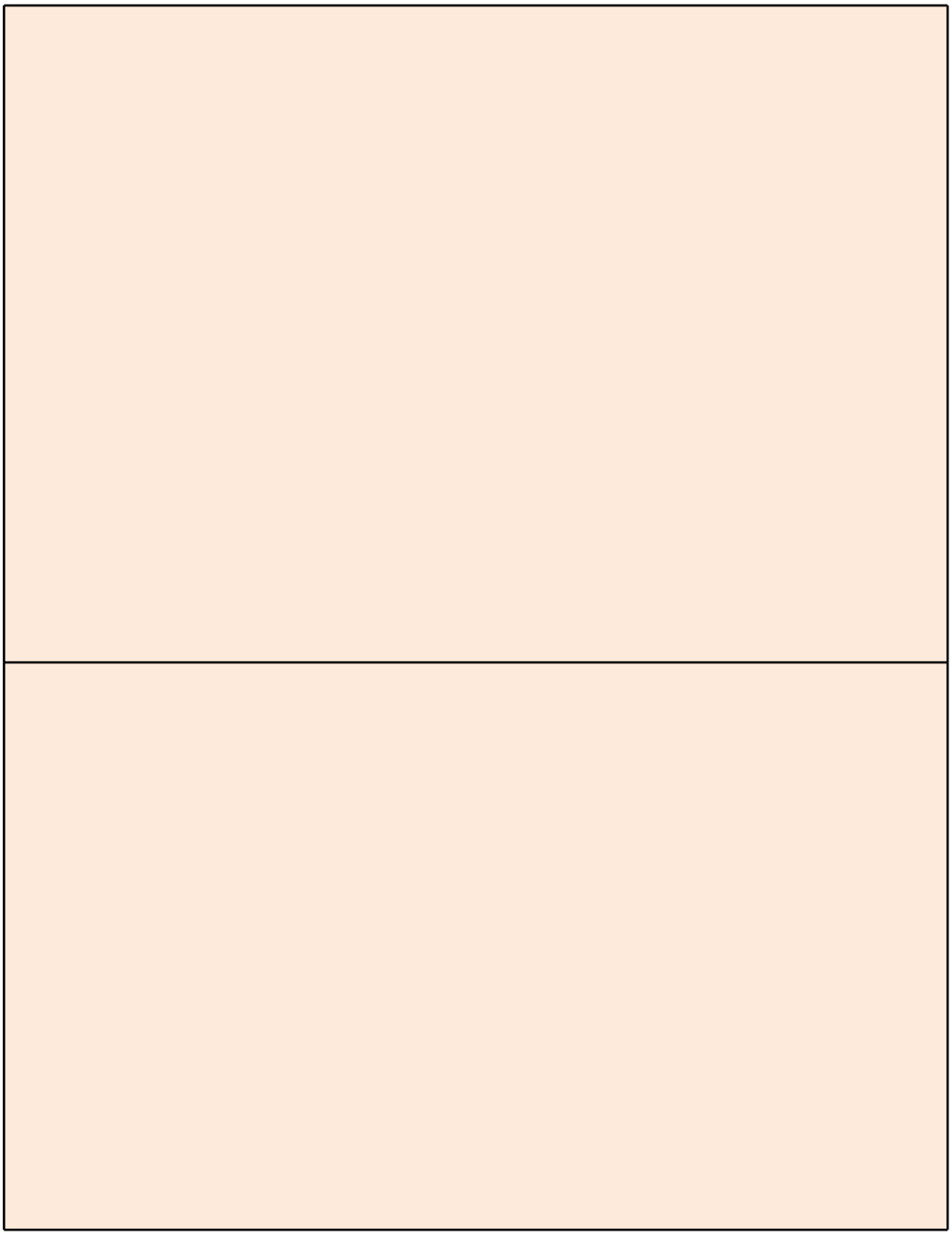


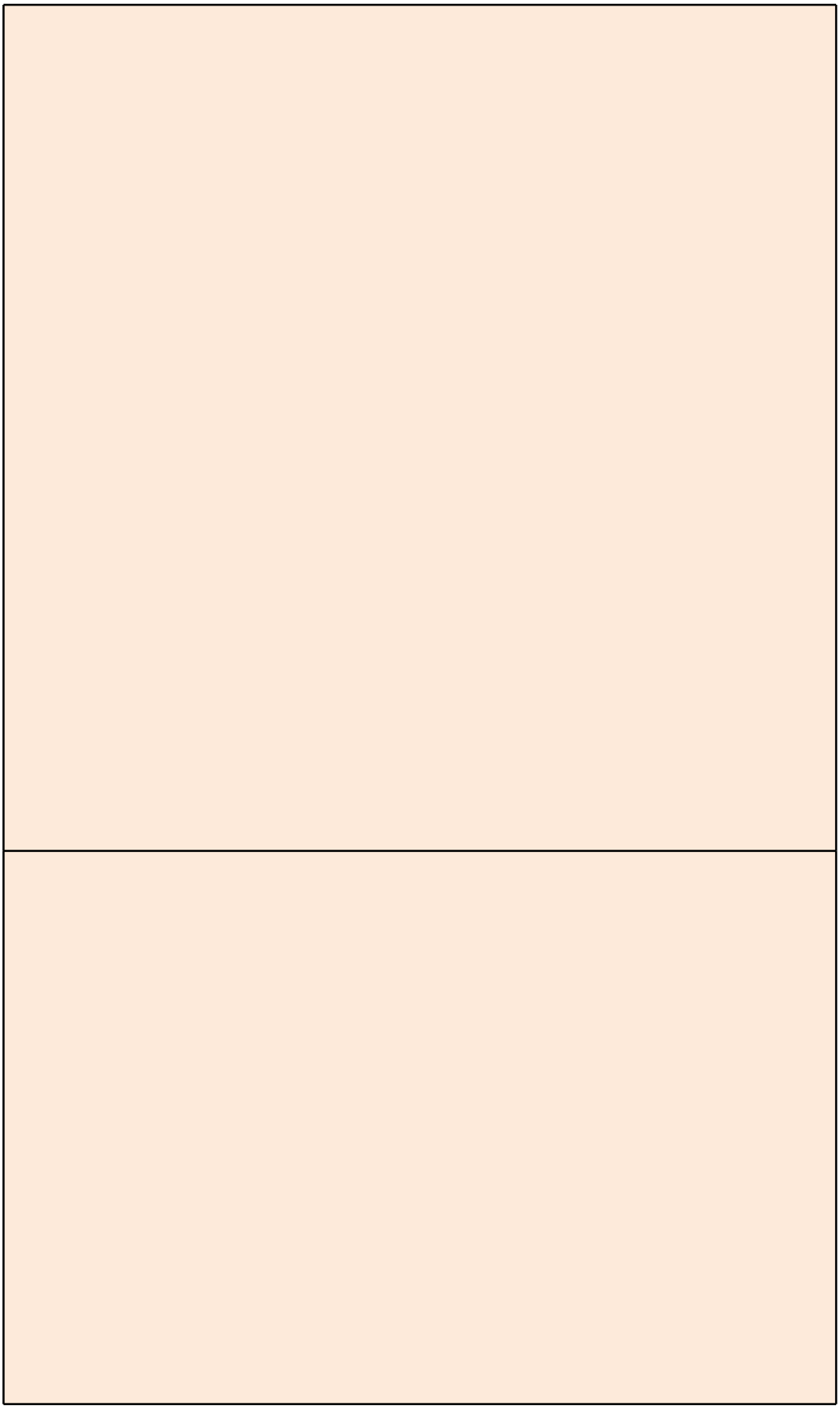


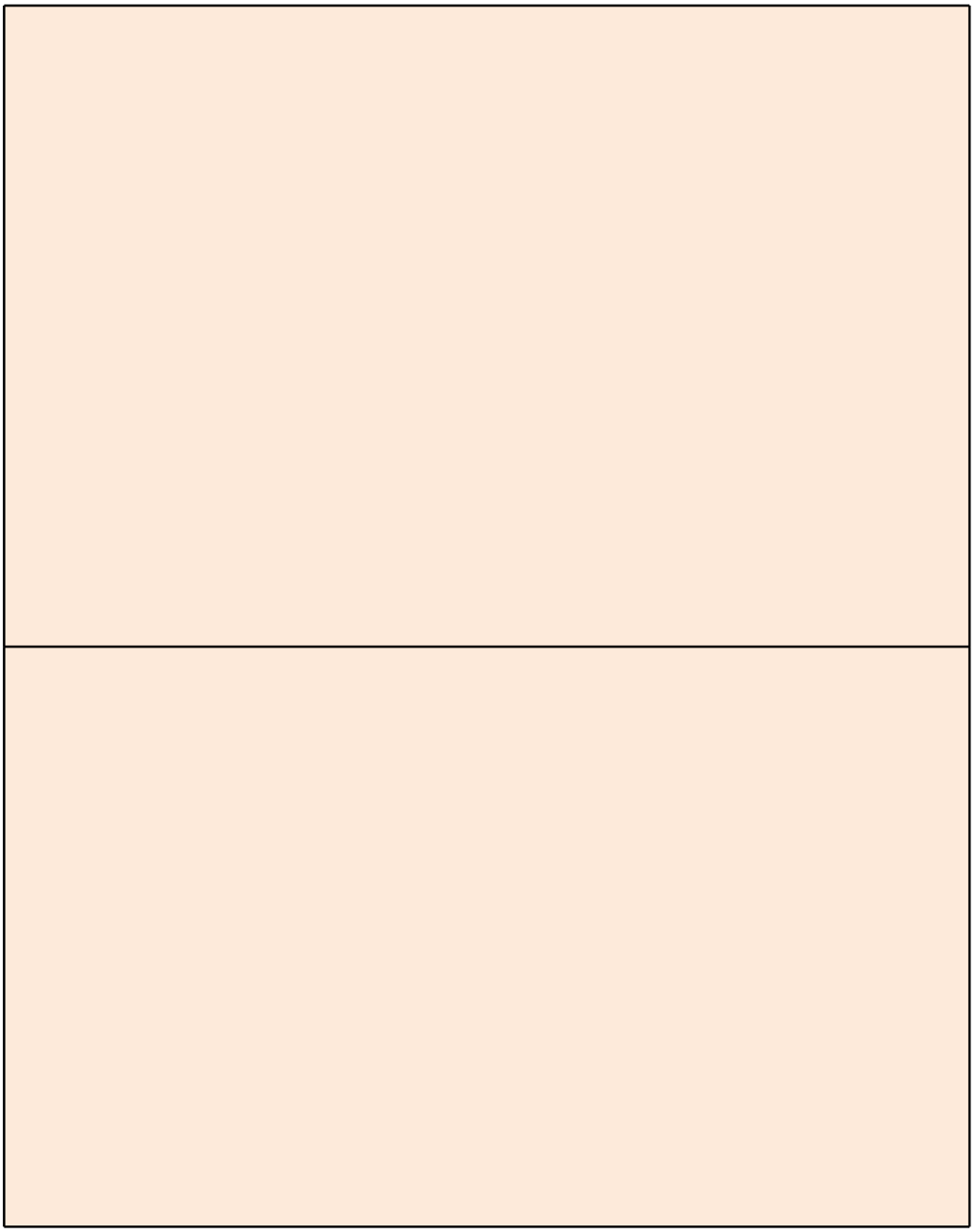


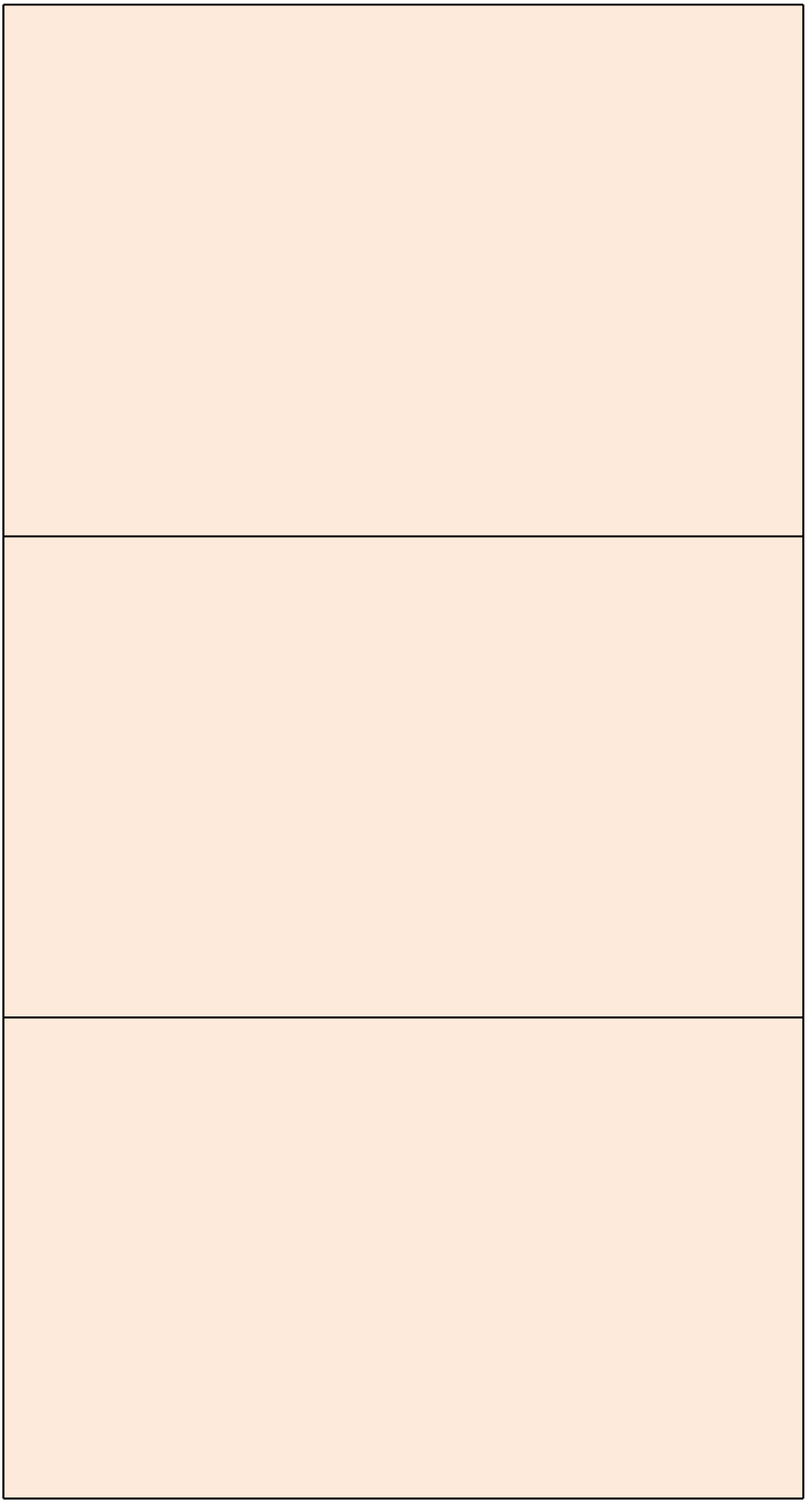


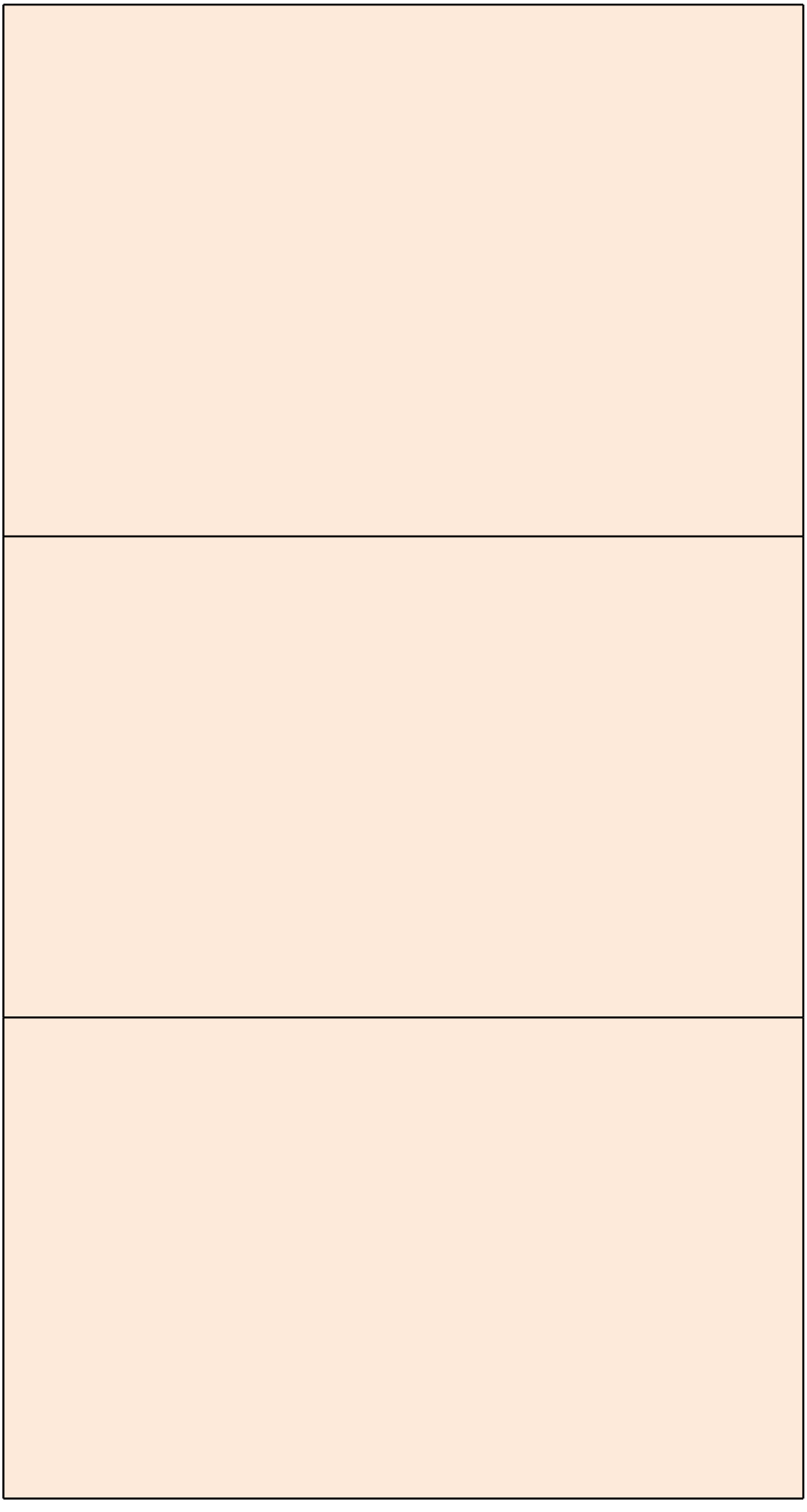


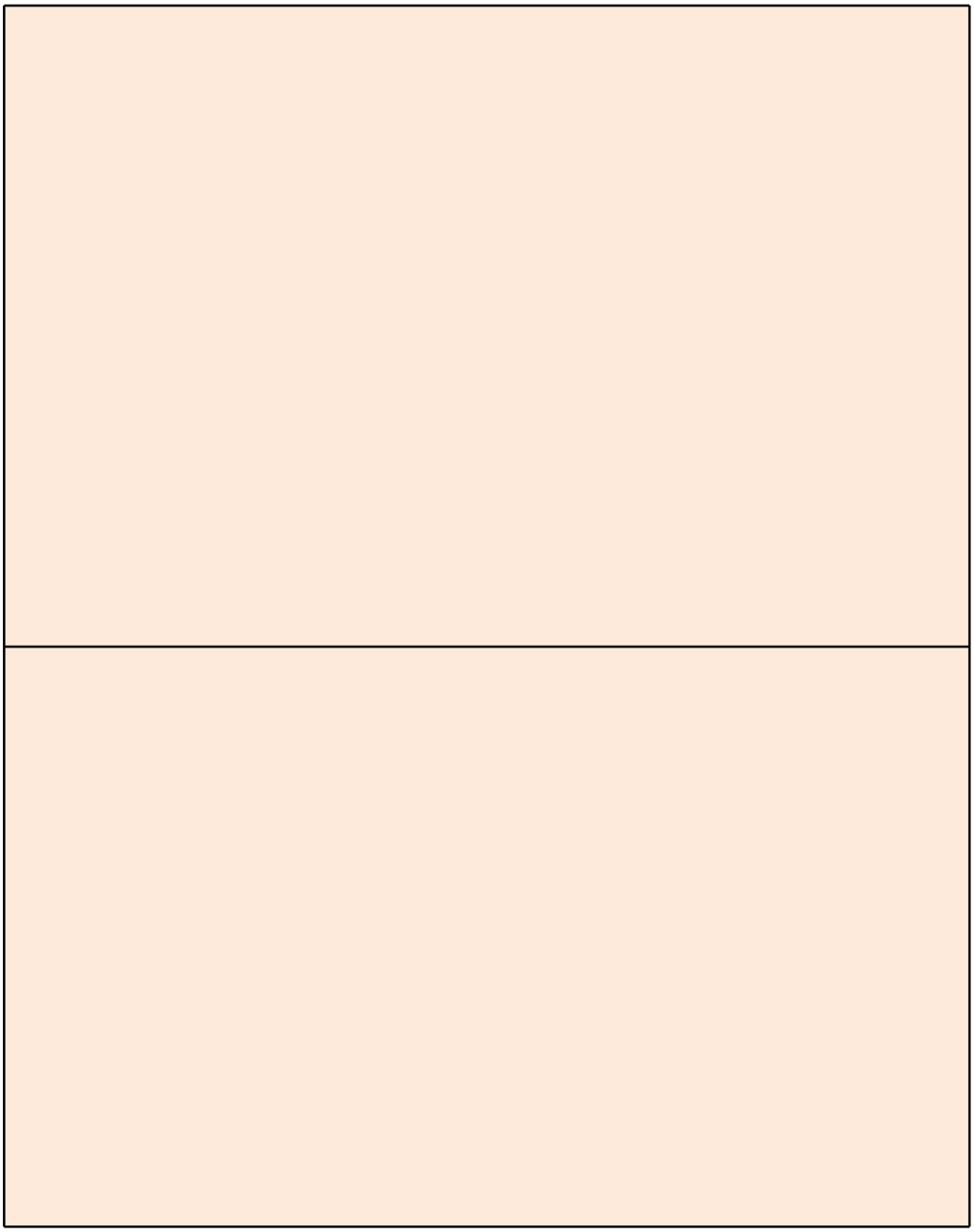


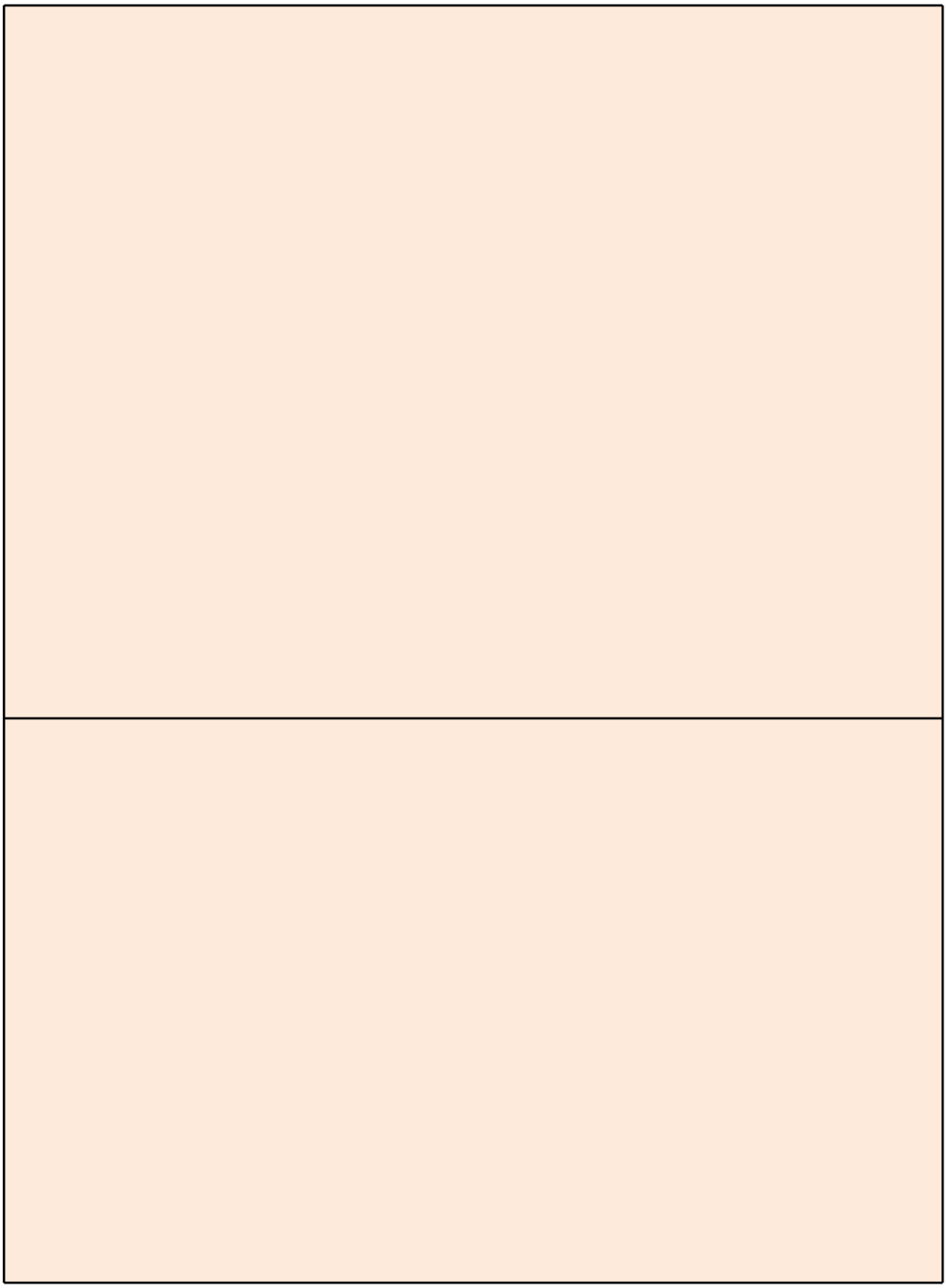


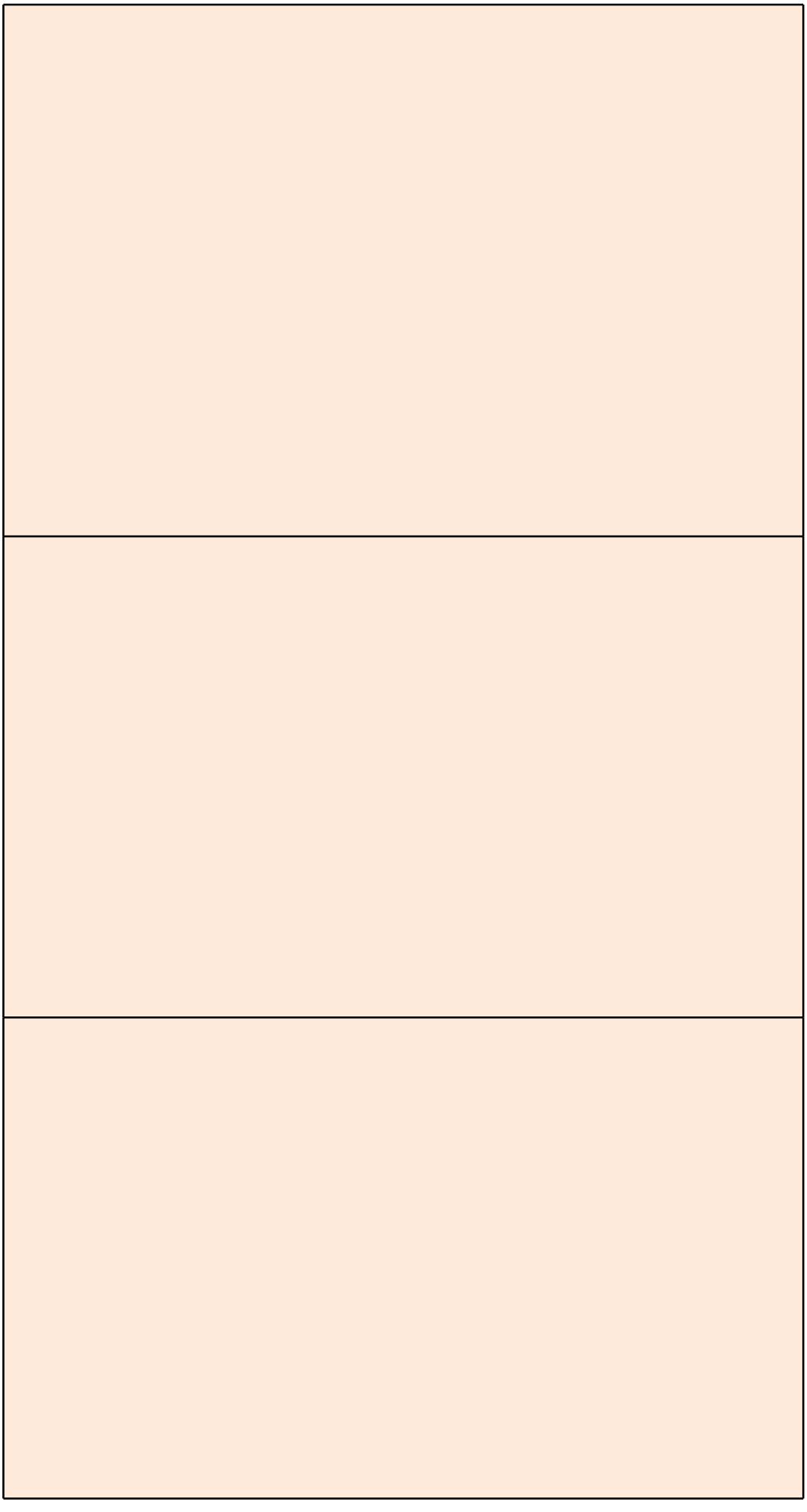


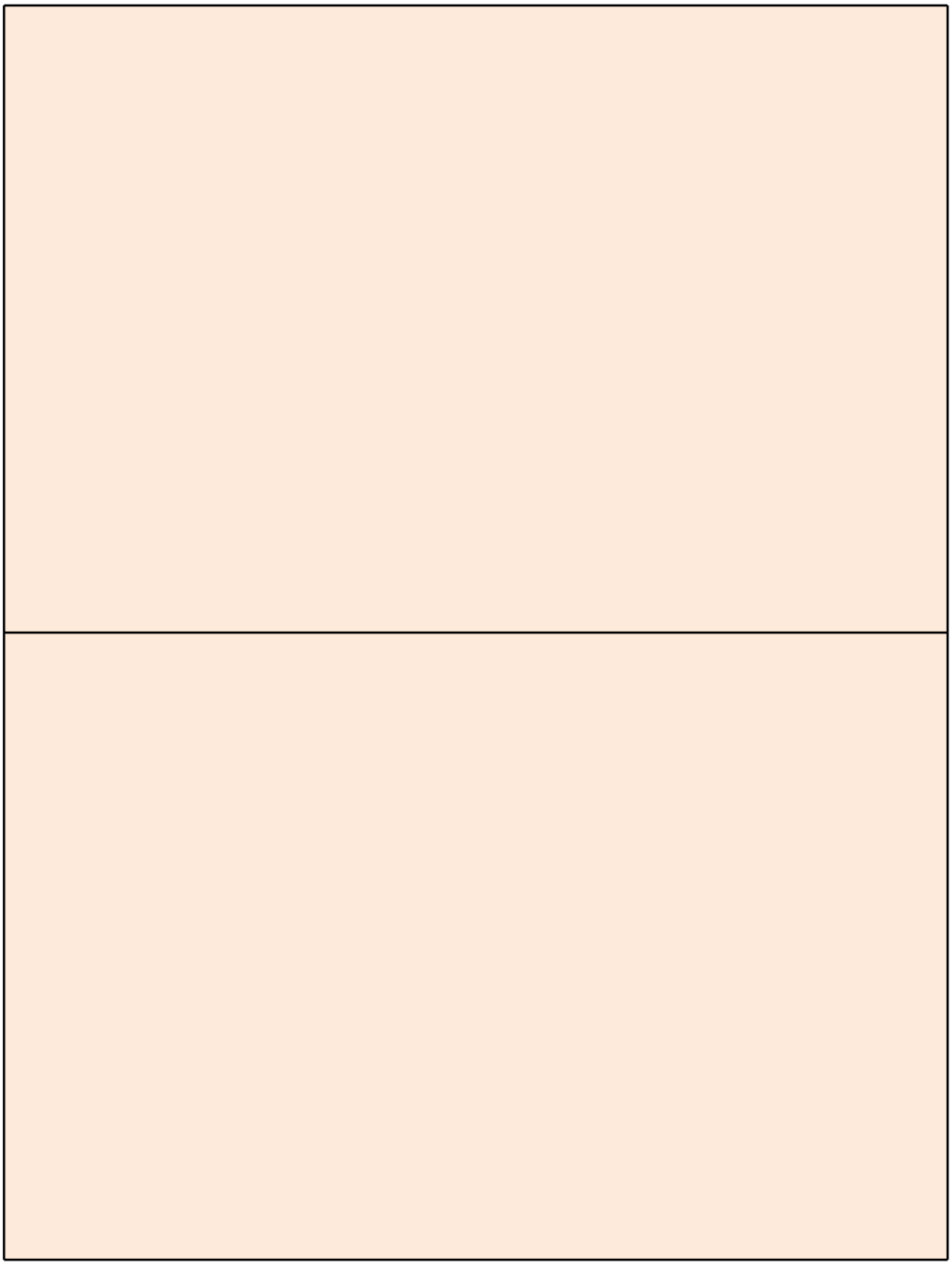


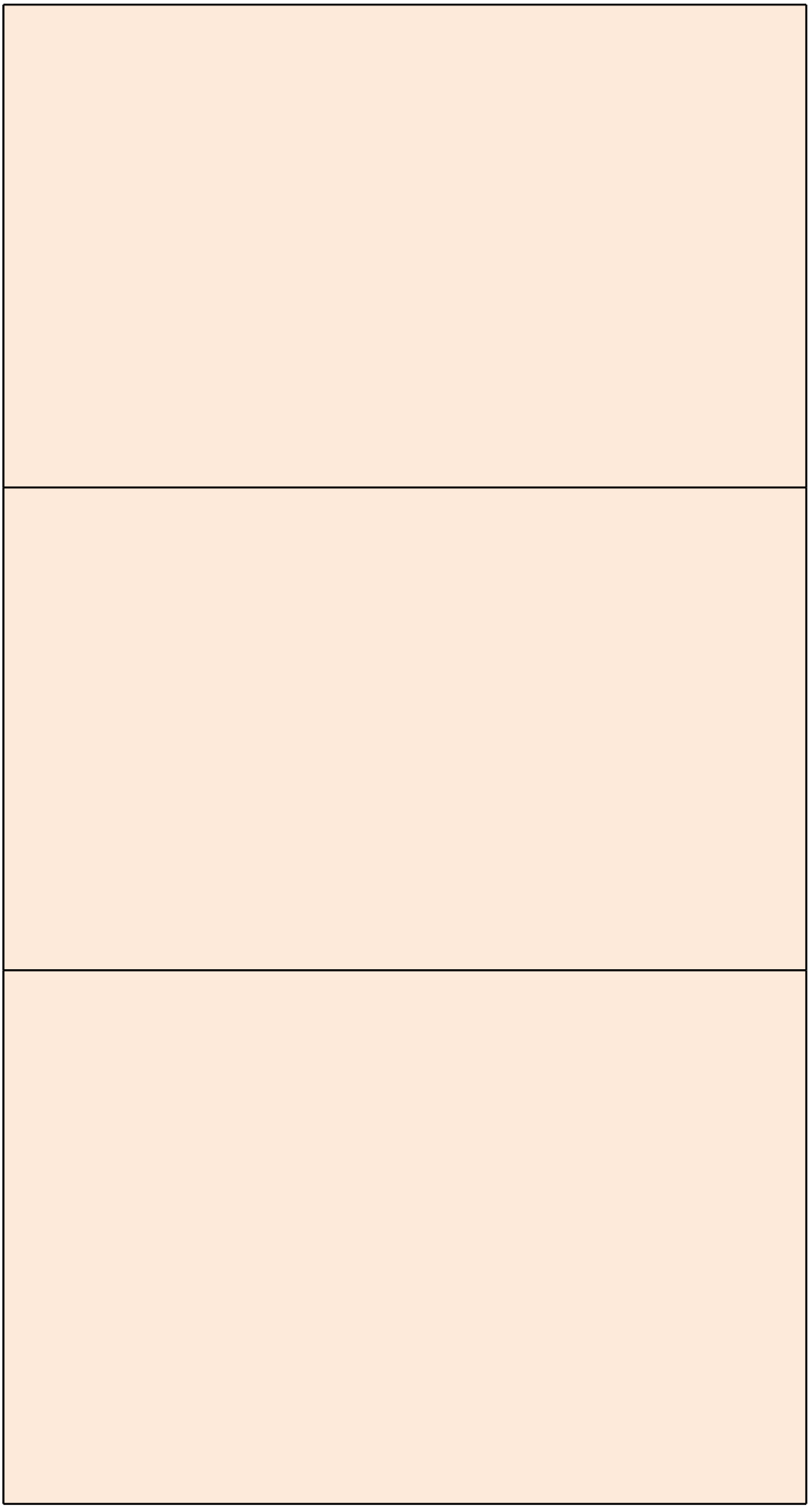


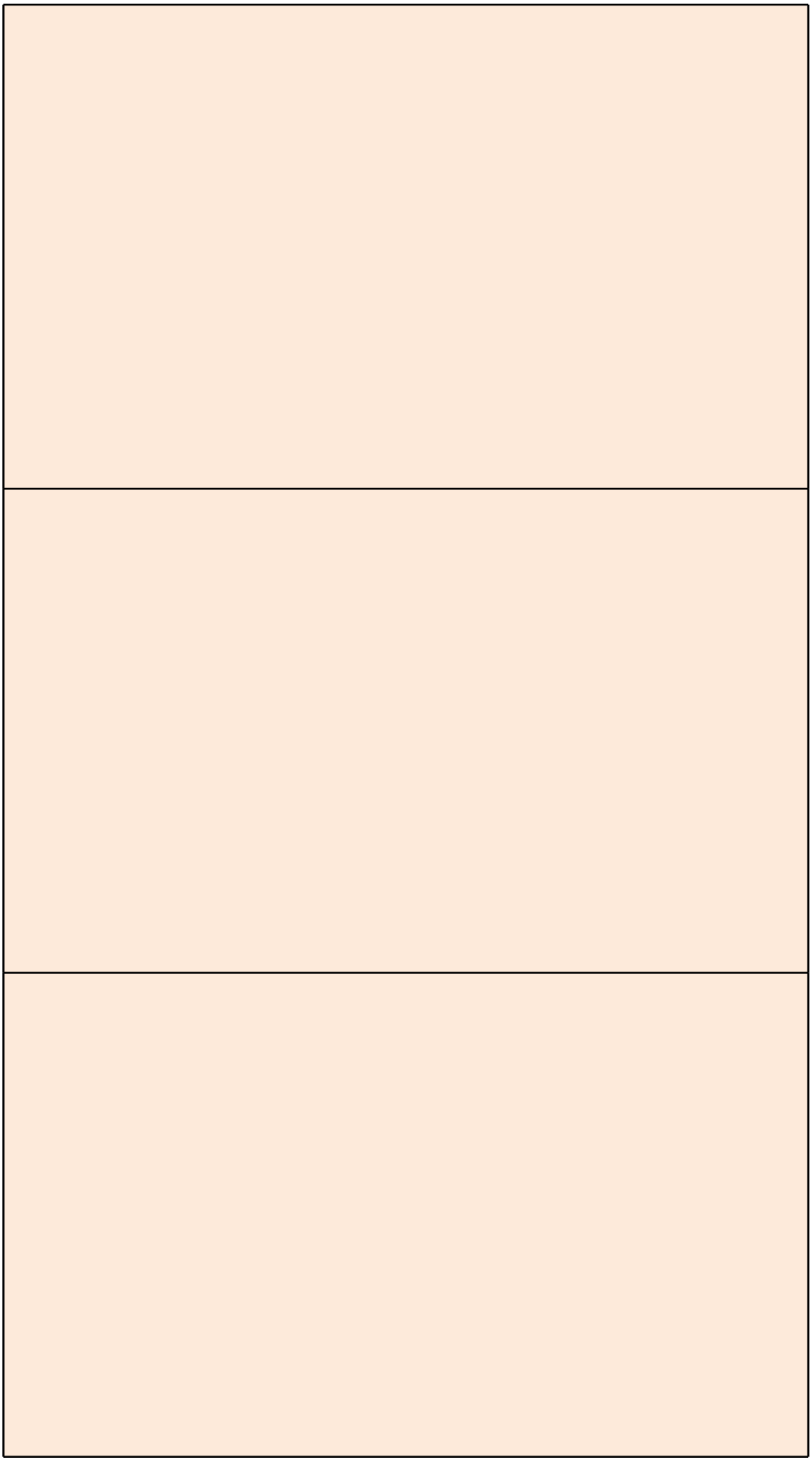




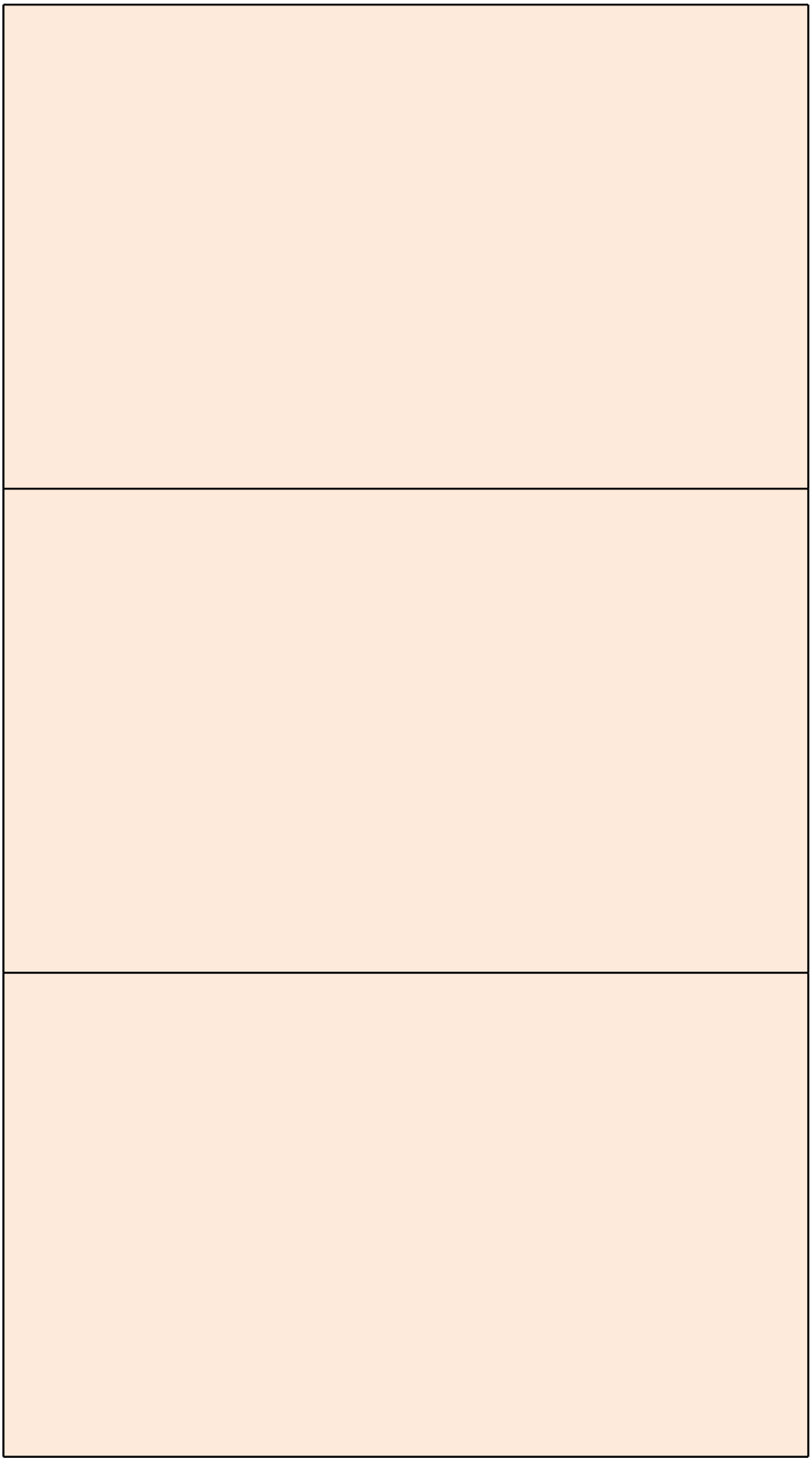


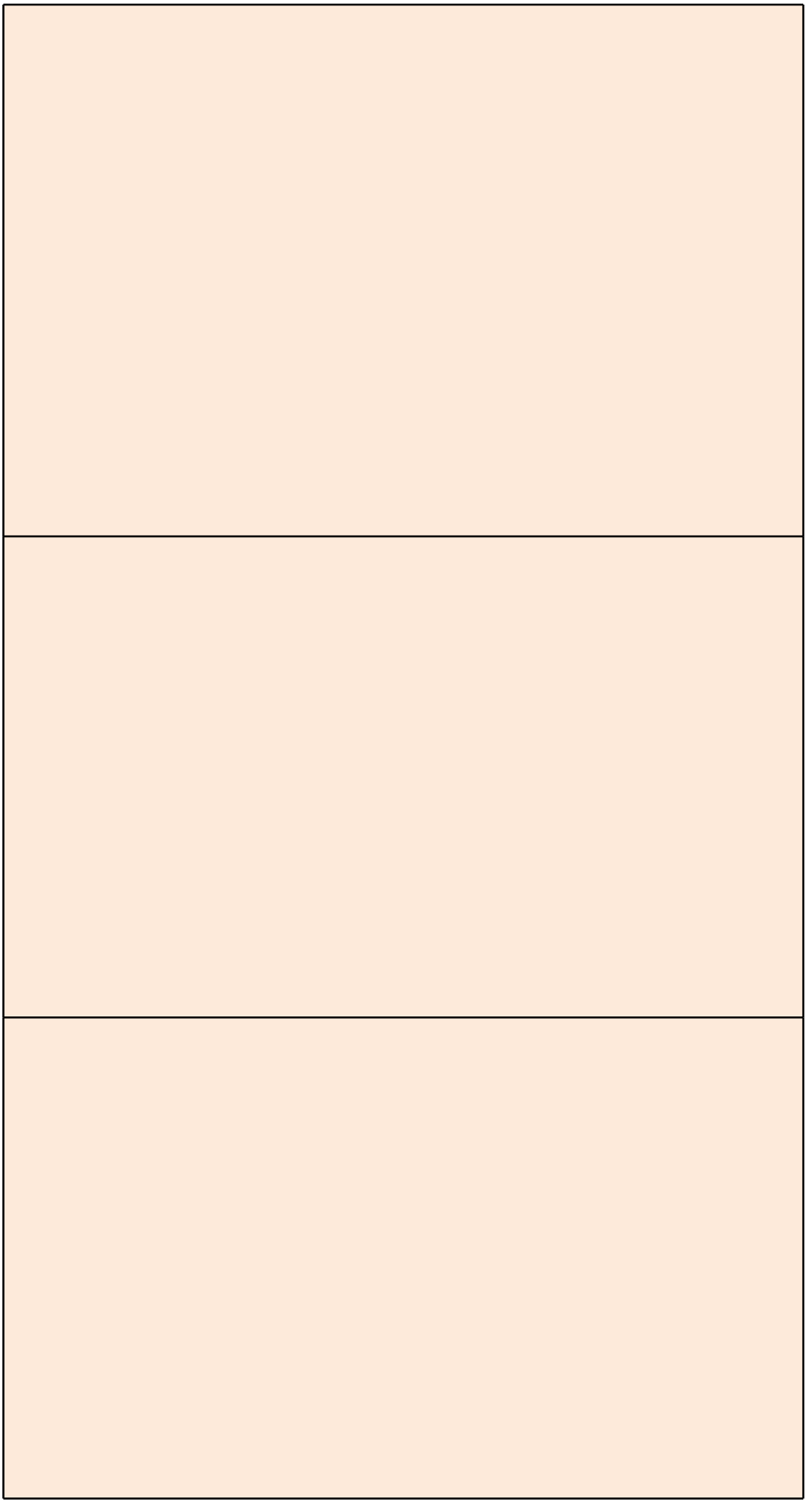


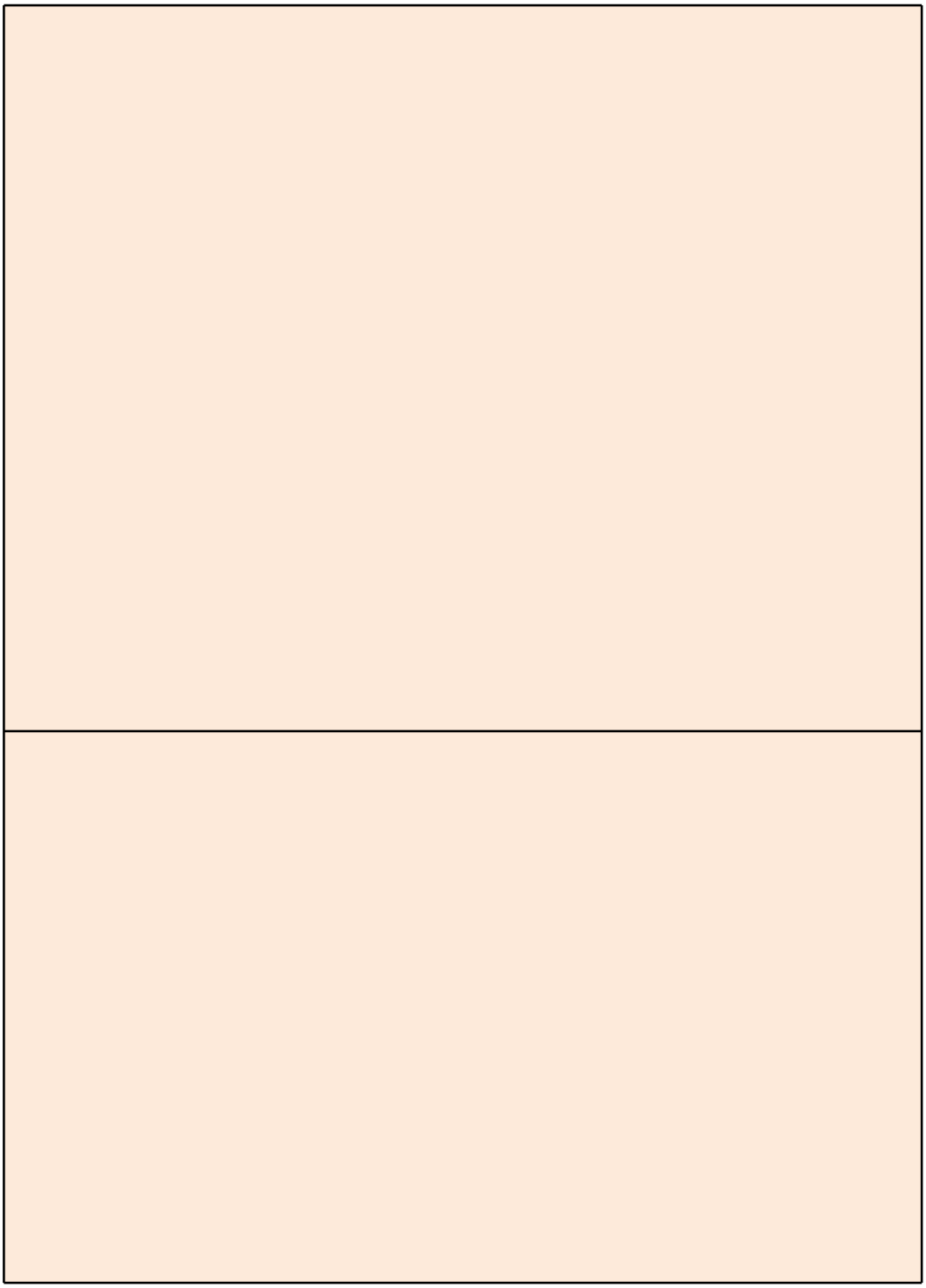


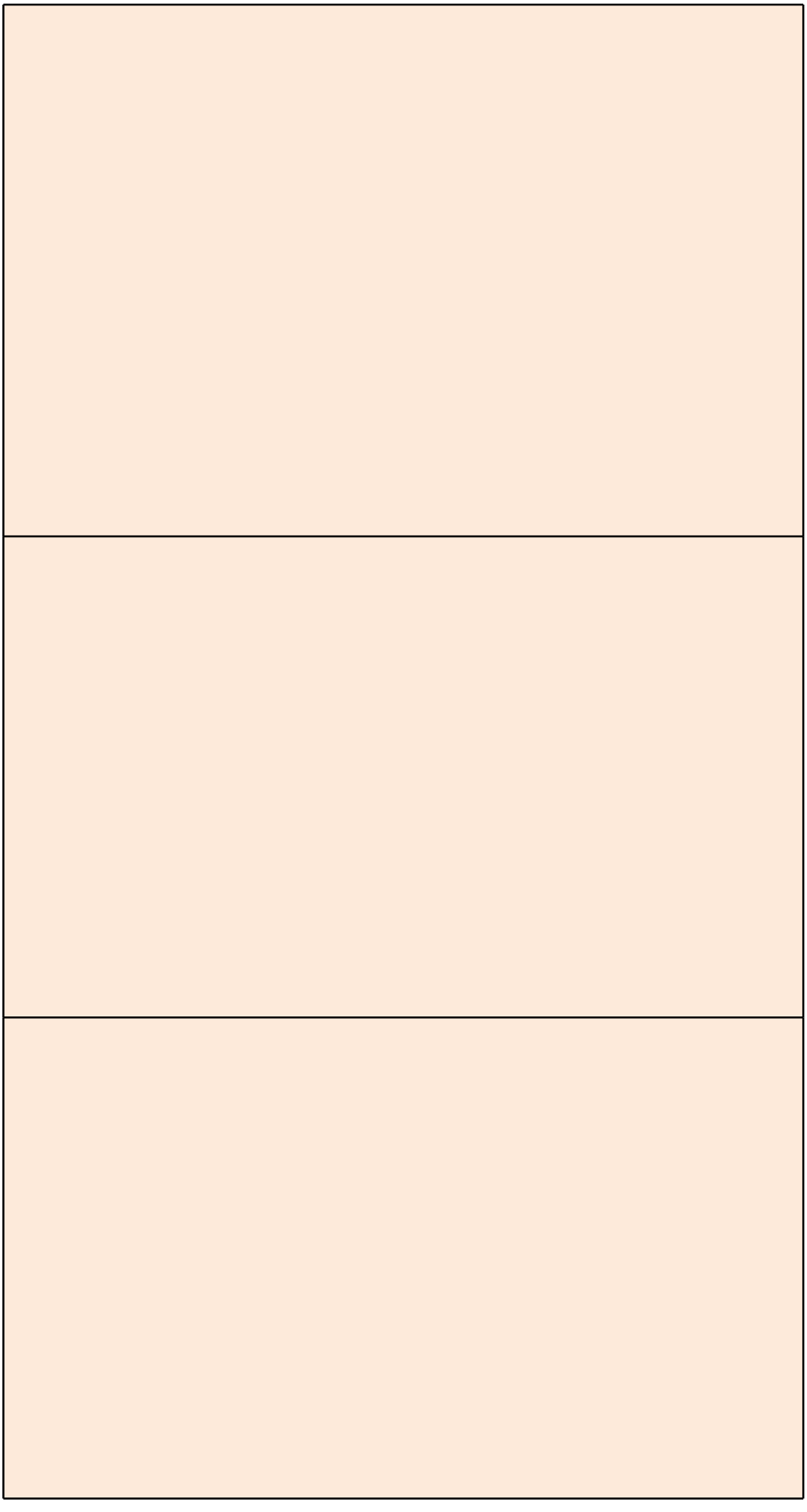


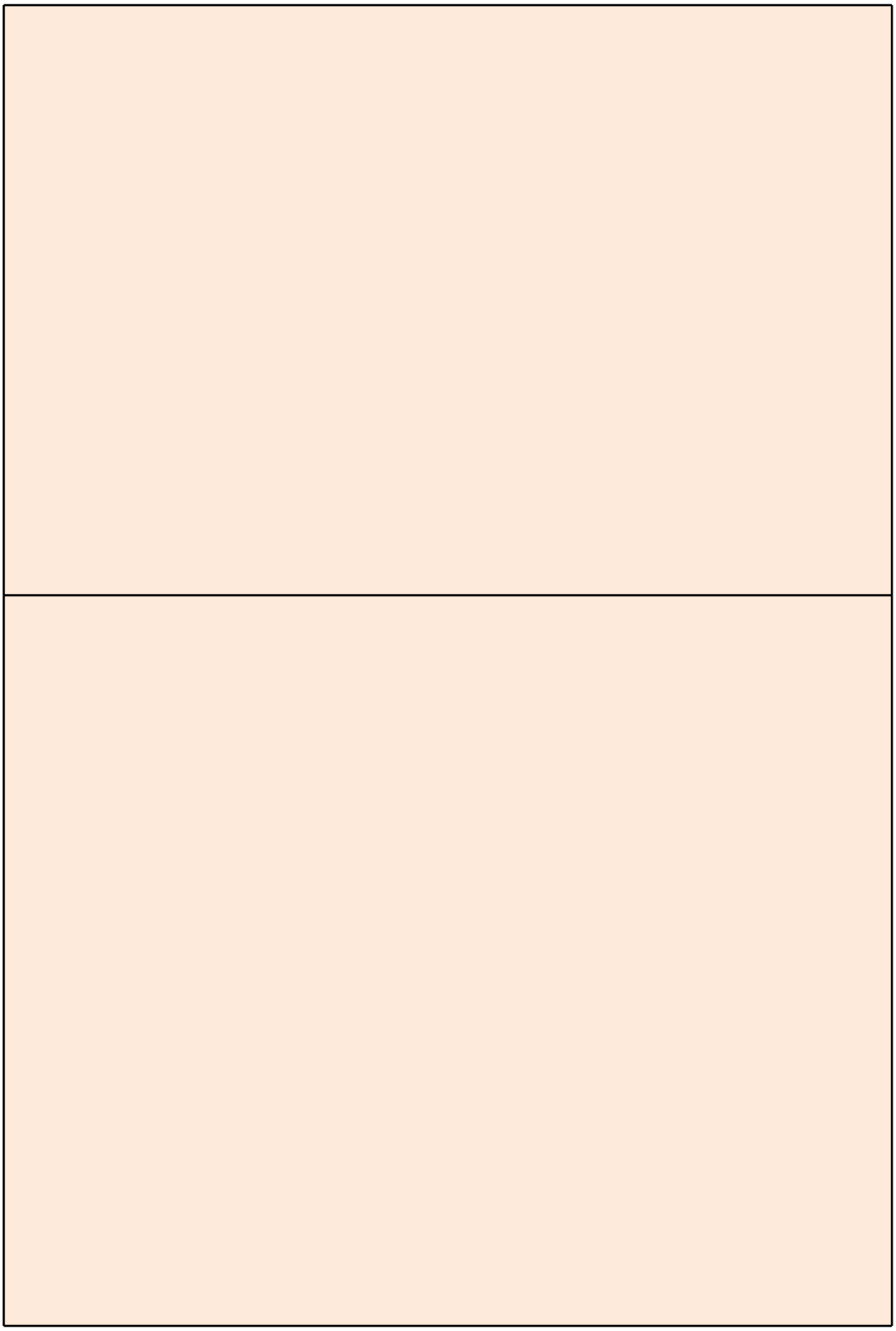
Uuden ydinenergialain 149 § "Turvallisuustarkastus voidaan jättää tekemättä poliisille, pelastustoimelle, Rajavartiolaitokselle tai puolustusvoimille taikka riskiperusteisesti muulle henkeen, terveyteen tai omaisuuteen kohdistuvan vakavan uhkan torjuntaan osallistuvalle henkilölle sekä näiden mukana oleville ajoneuvoille ja tavaroille." Määräyksen luonnoksessa Rajavartiolaitos ja puolustusvoimat oli jätetty luettelematta.

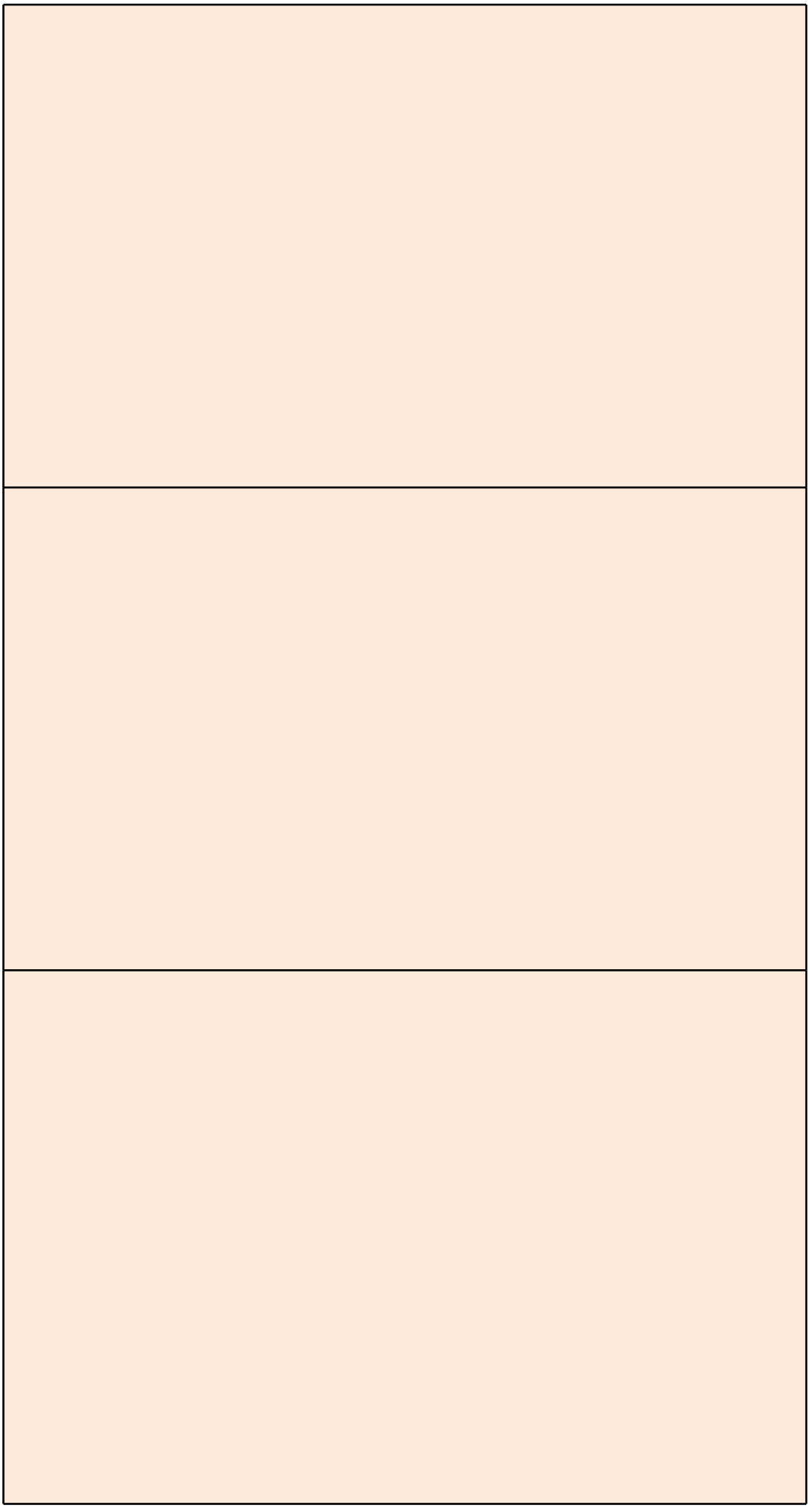


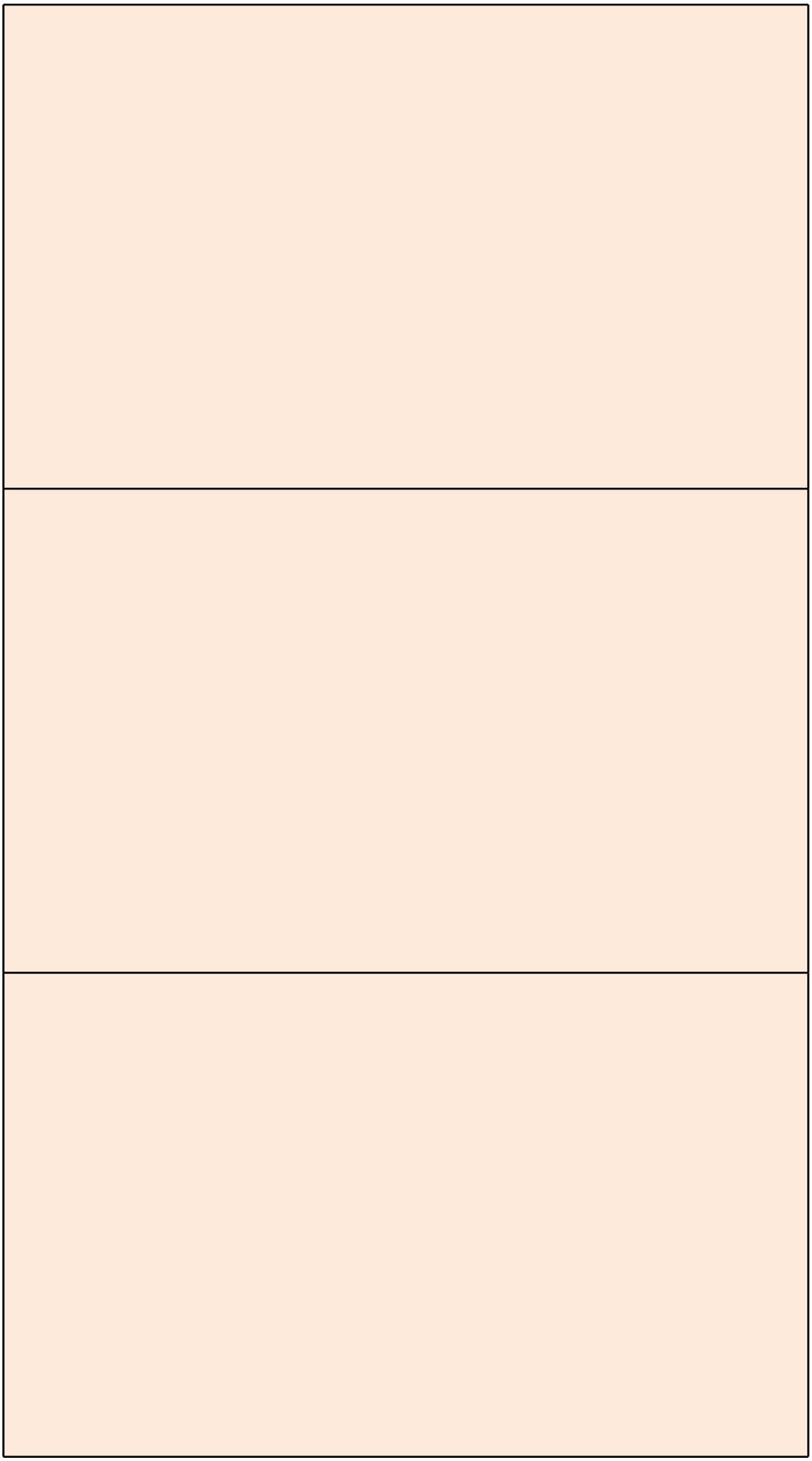


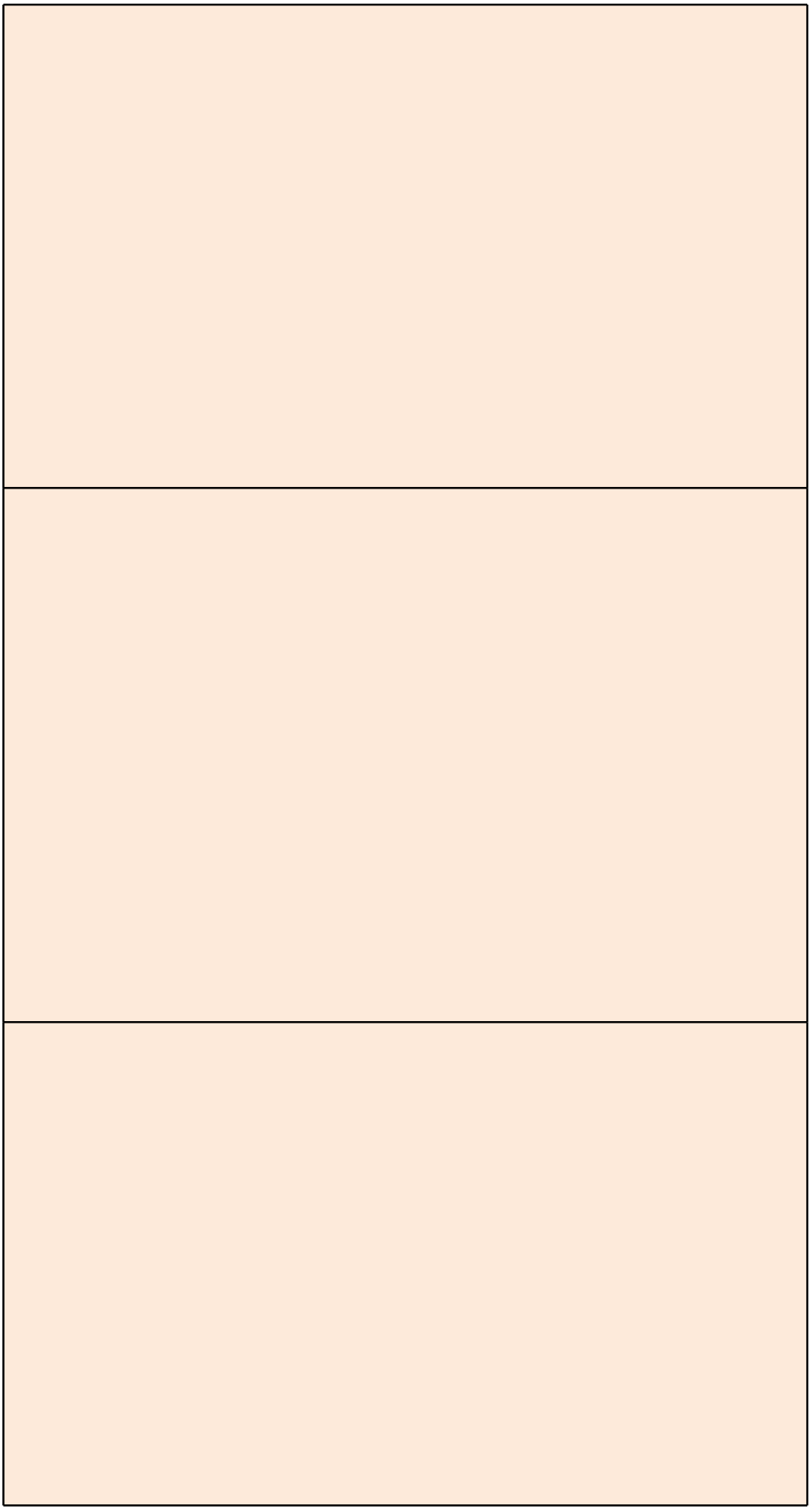


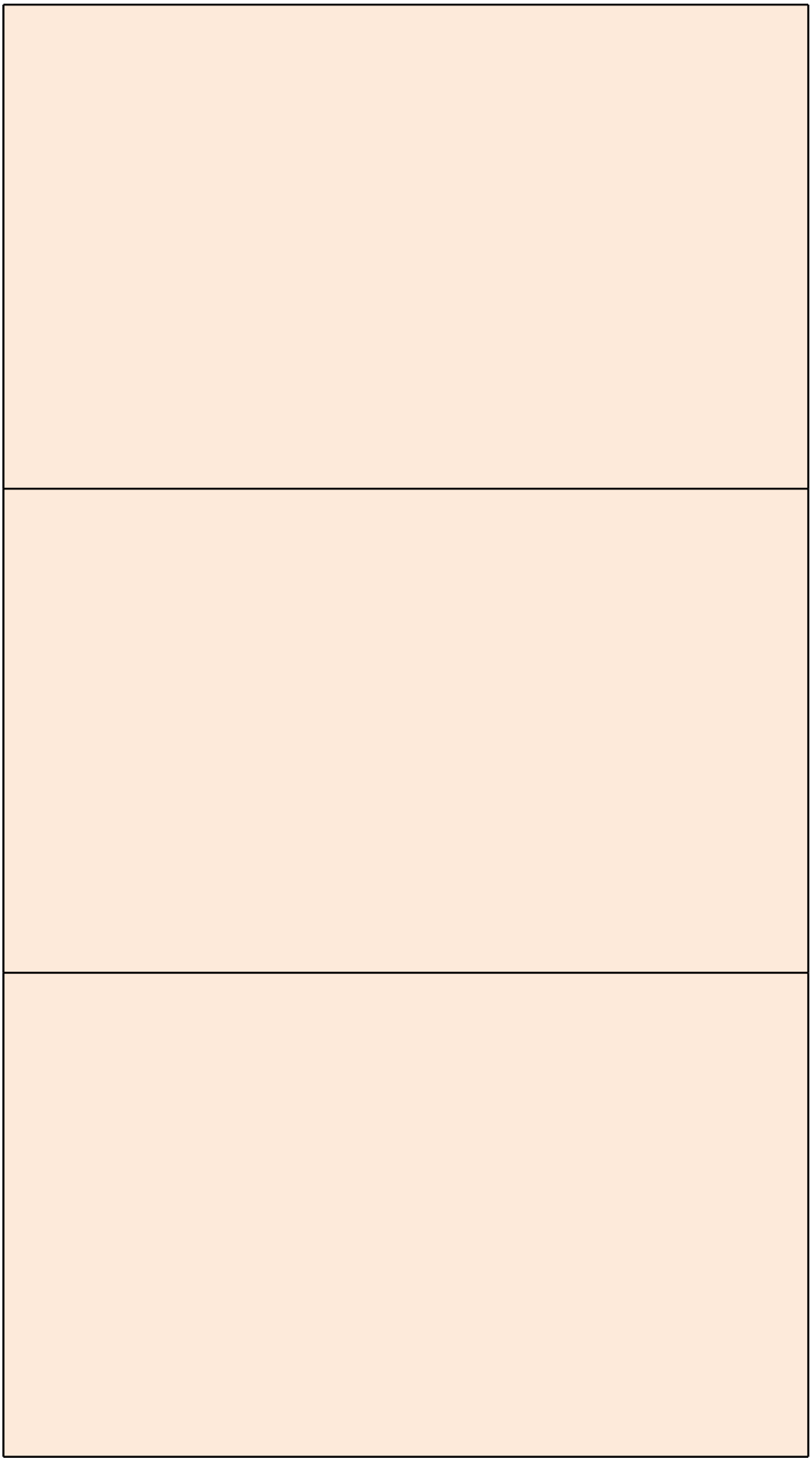


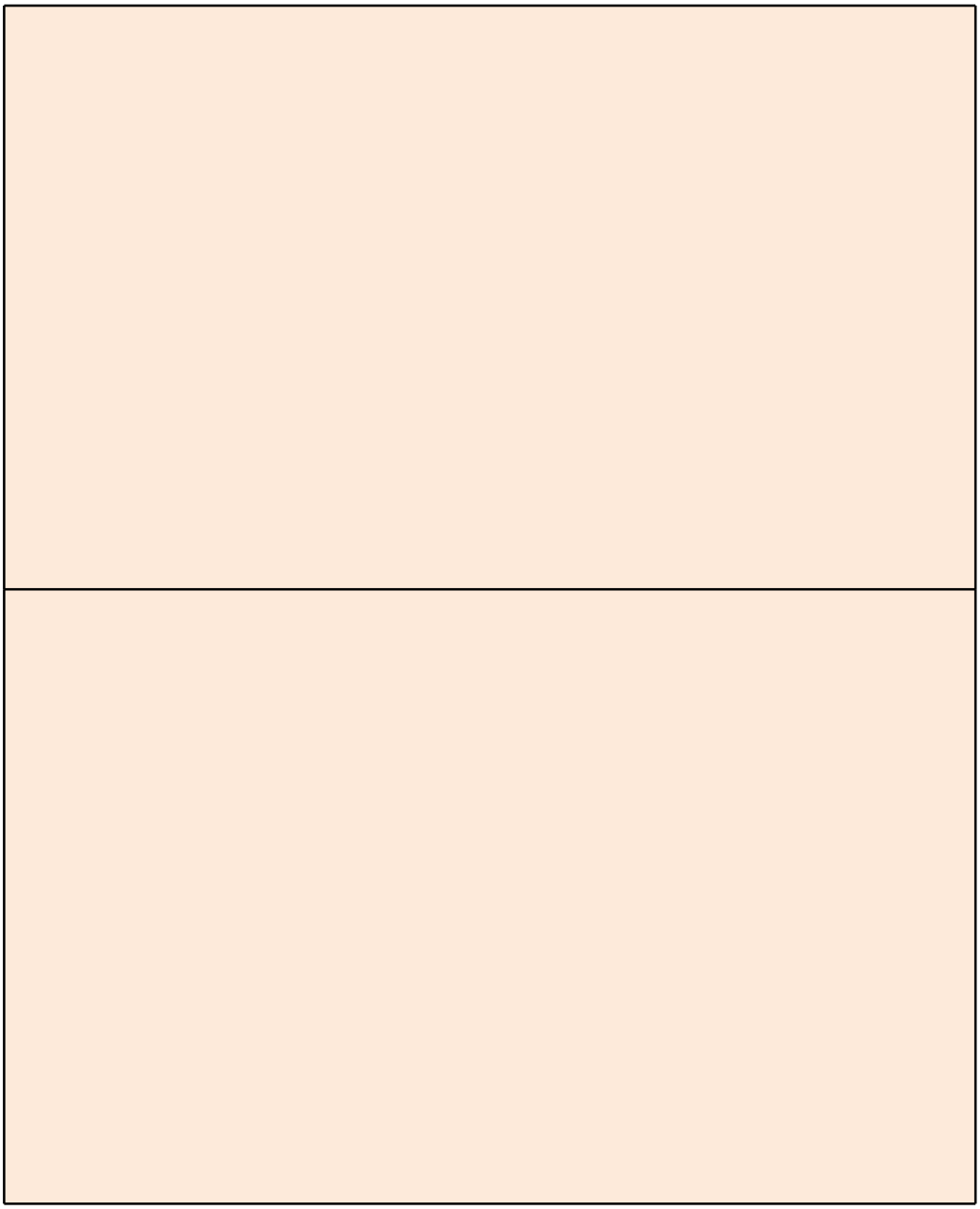


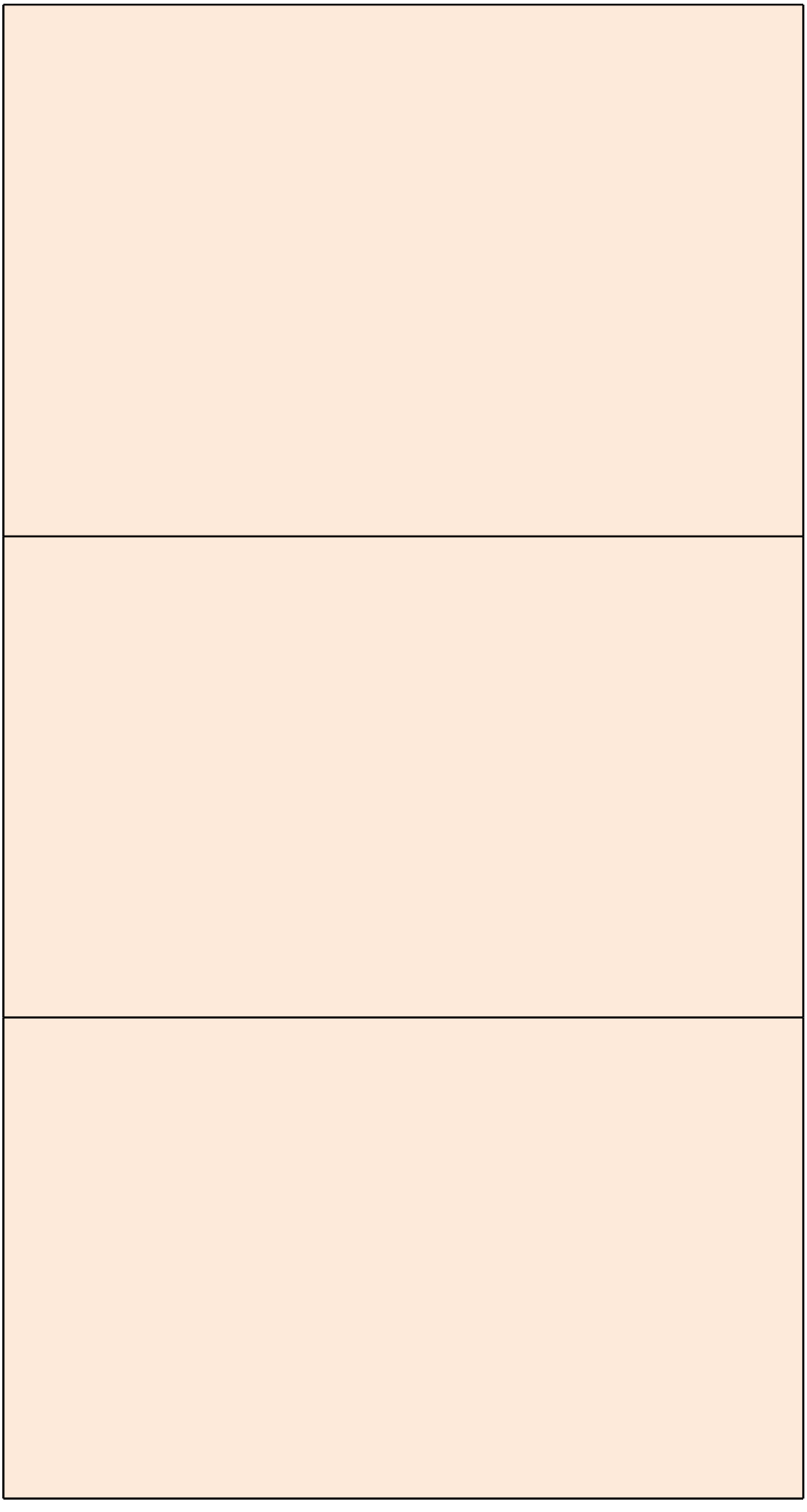


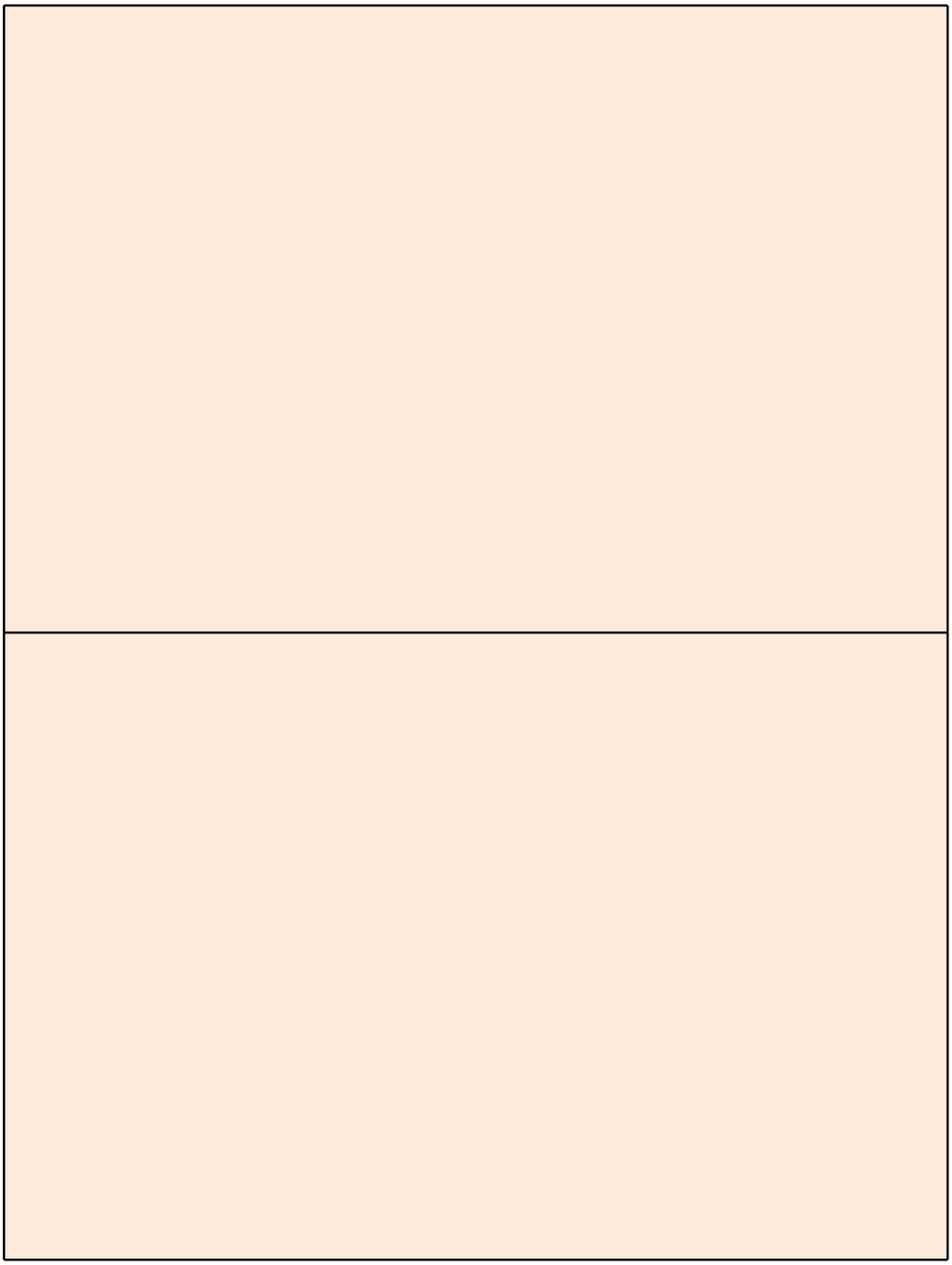


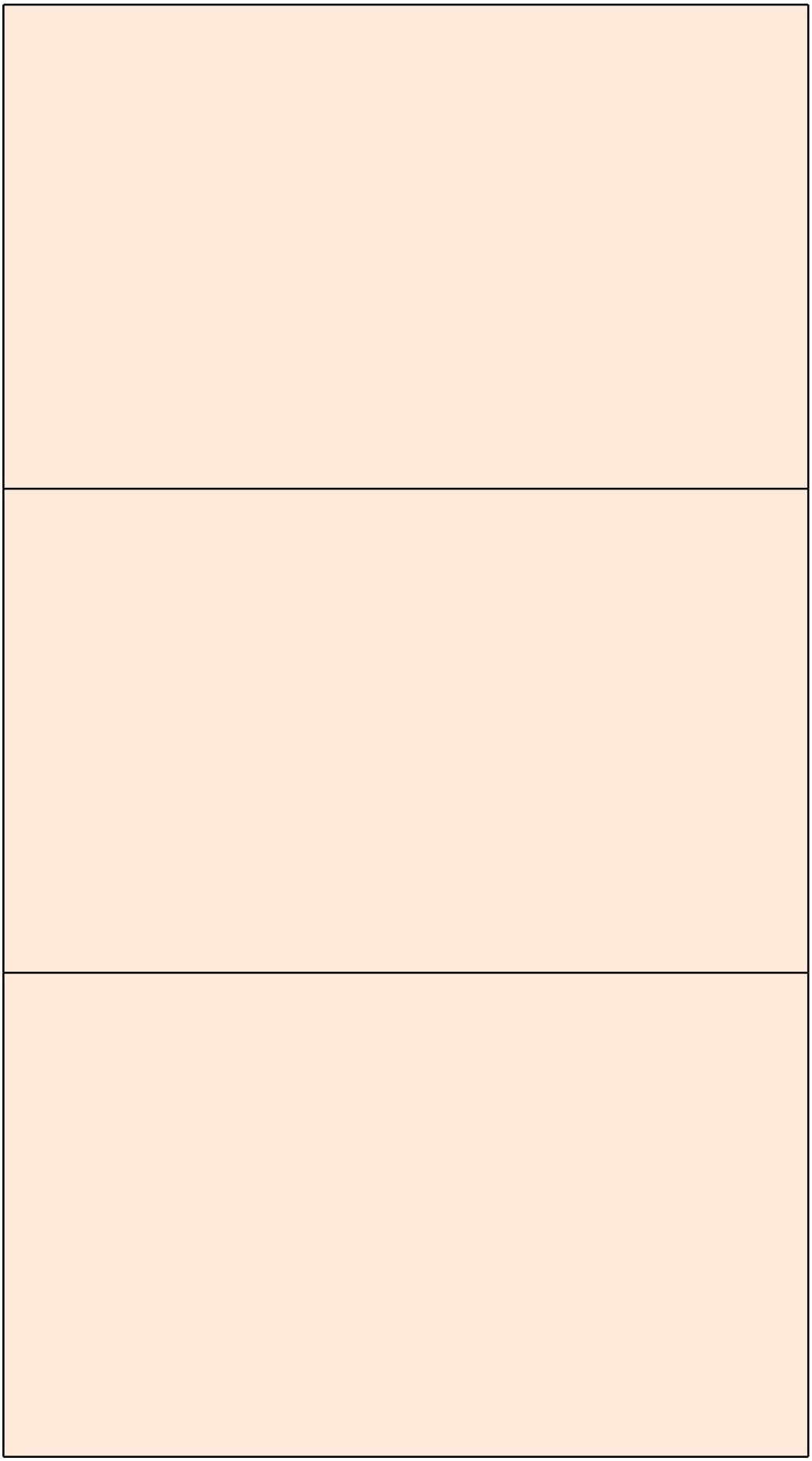


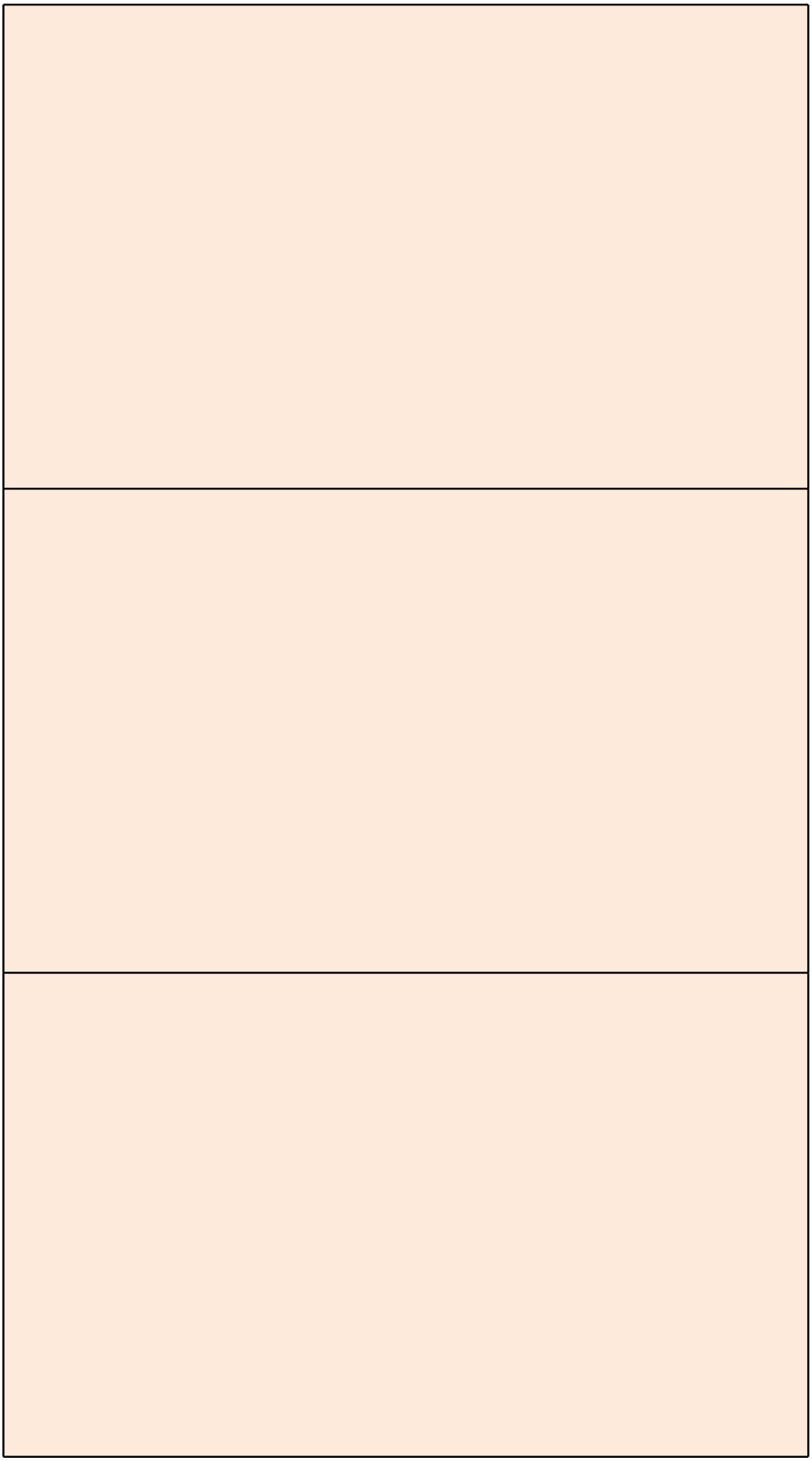


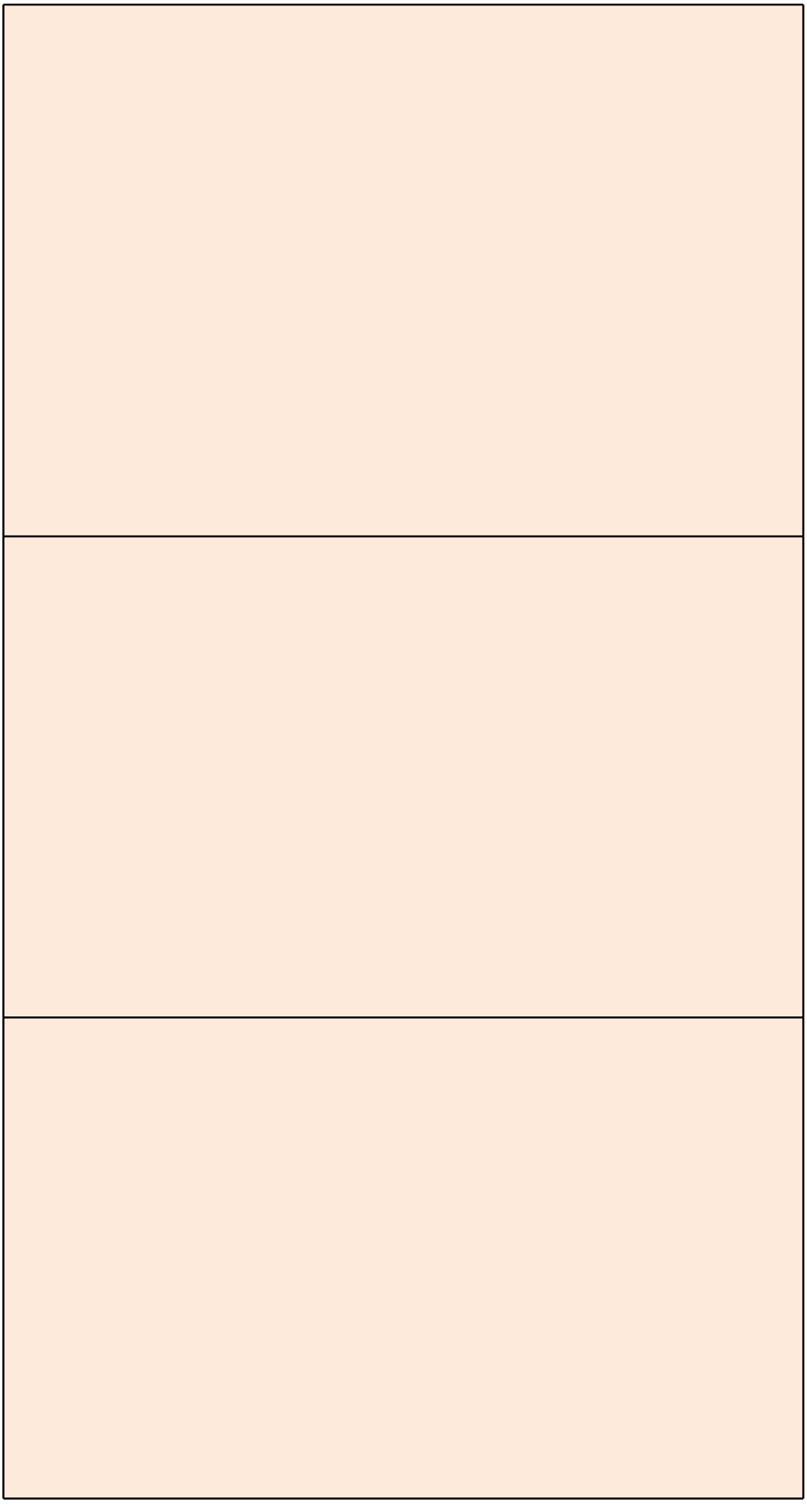


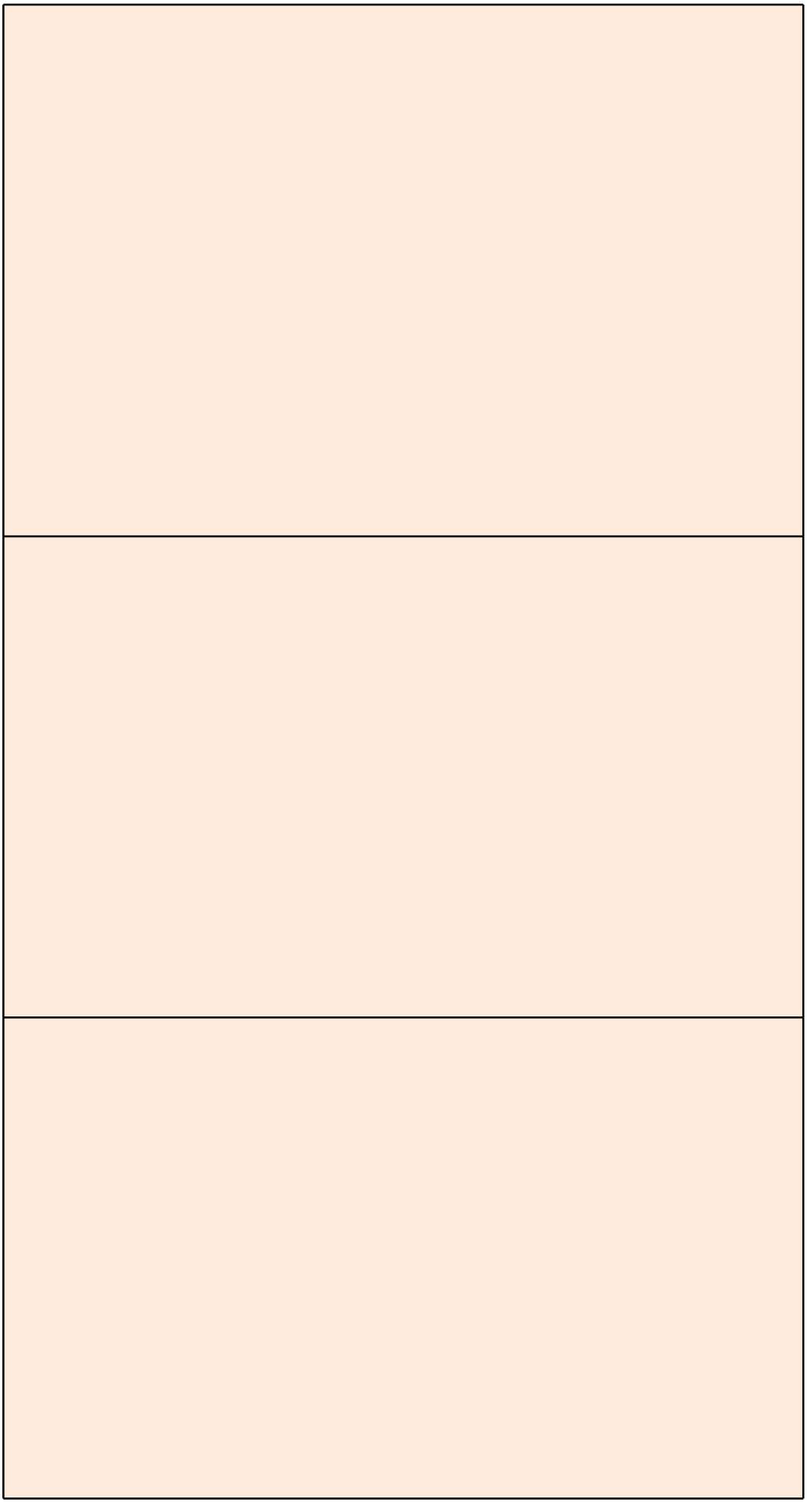


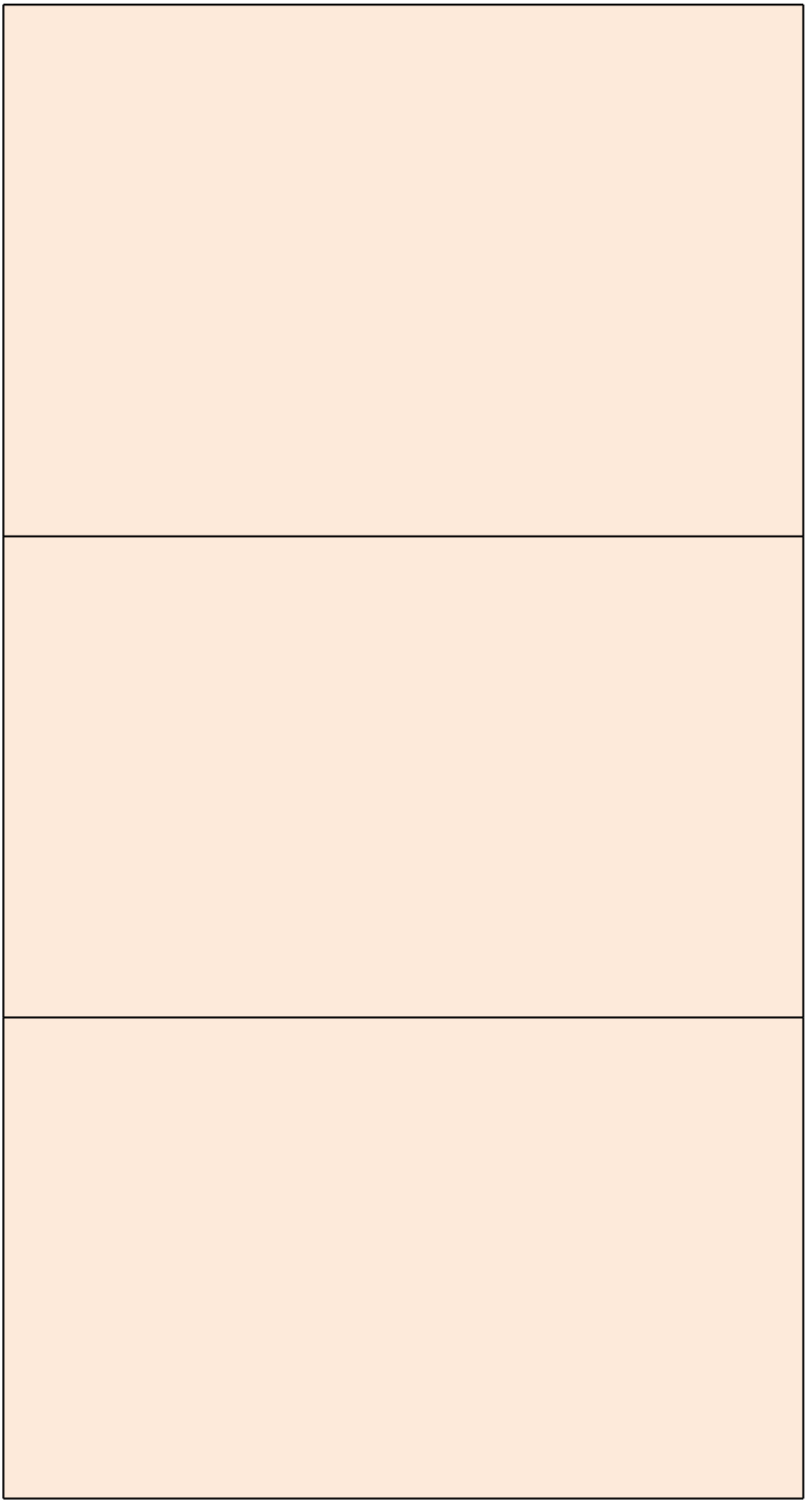


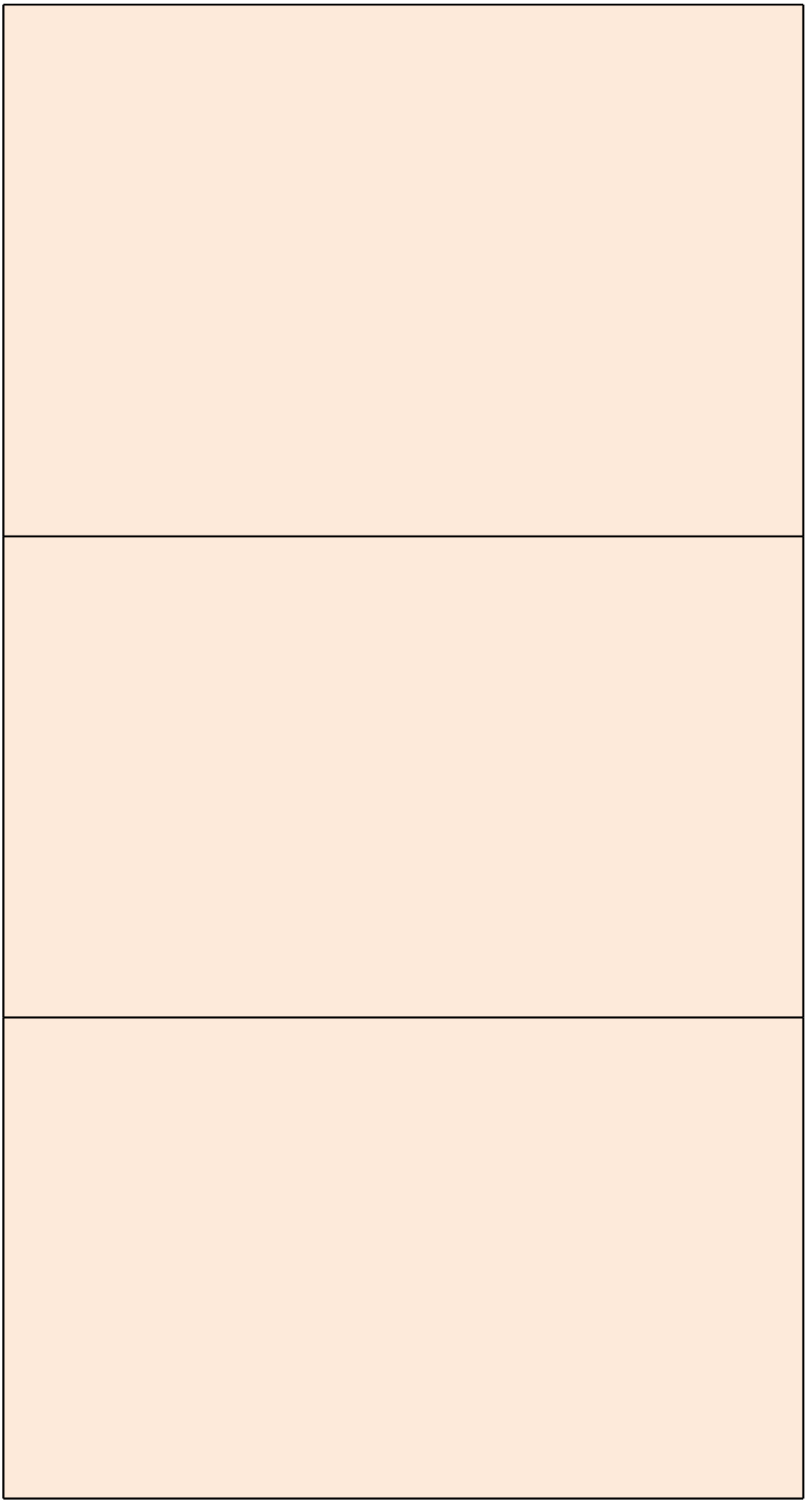


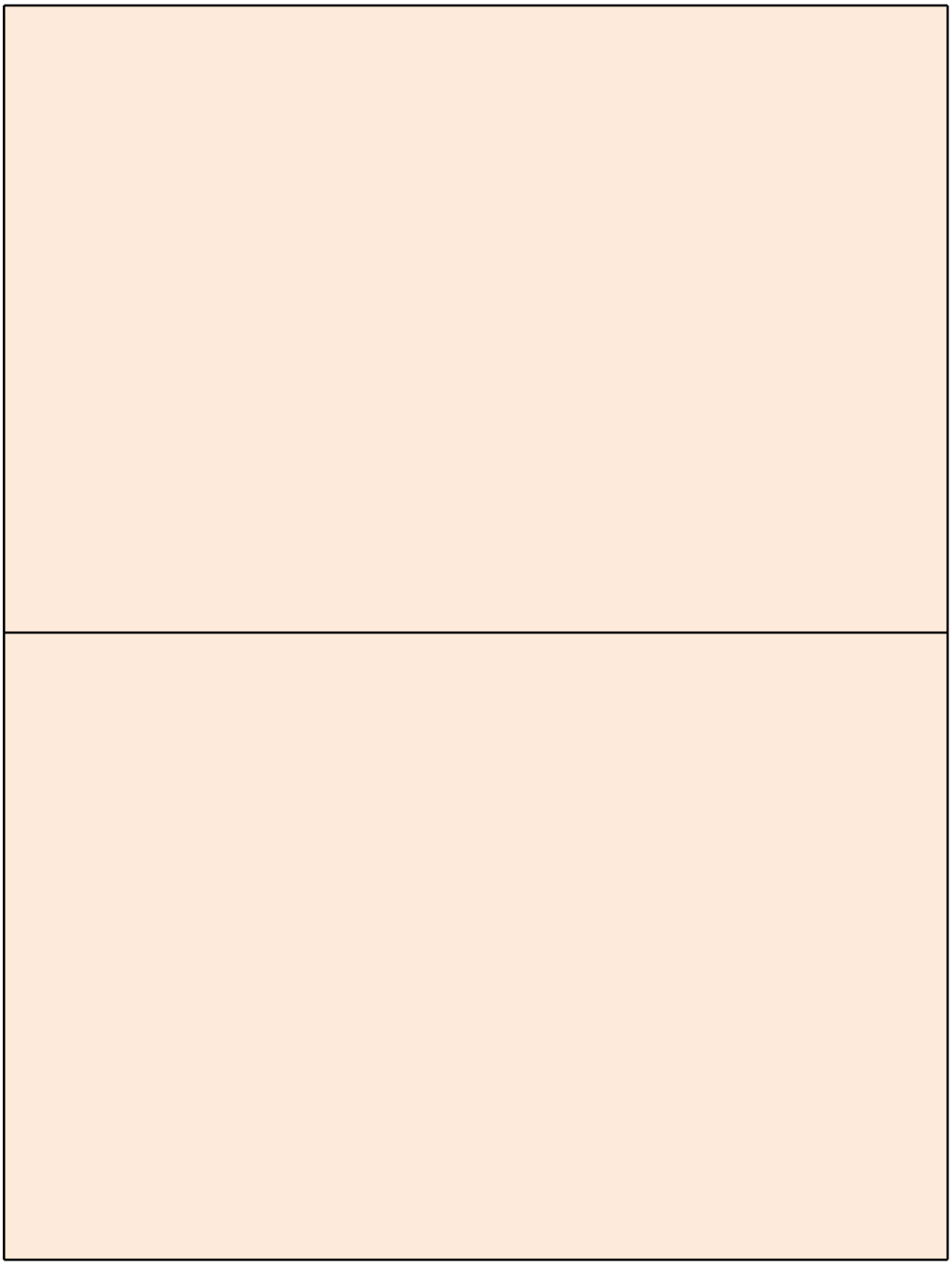


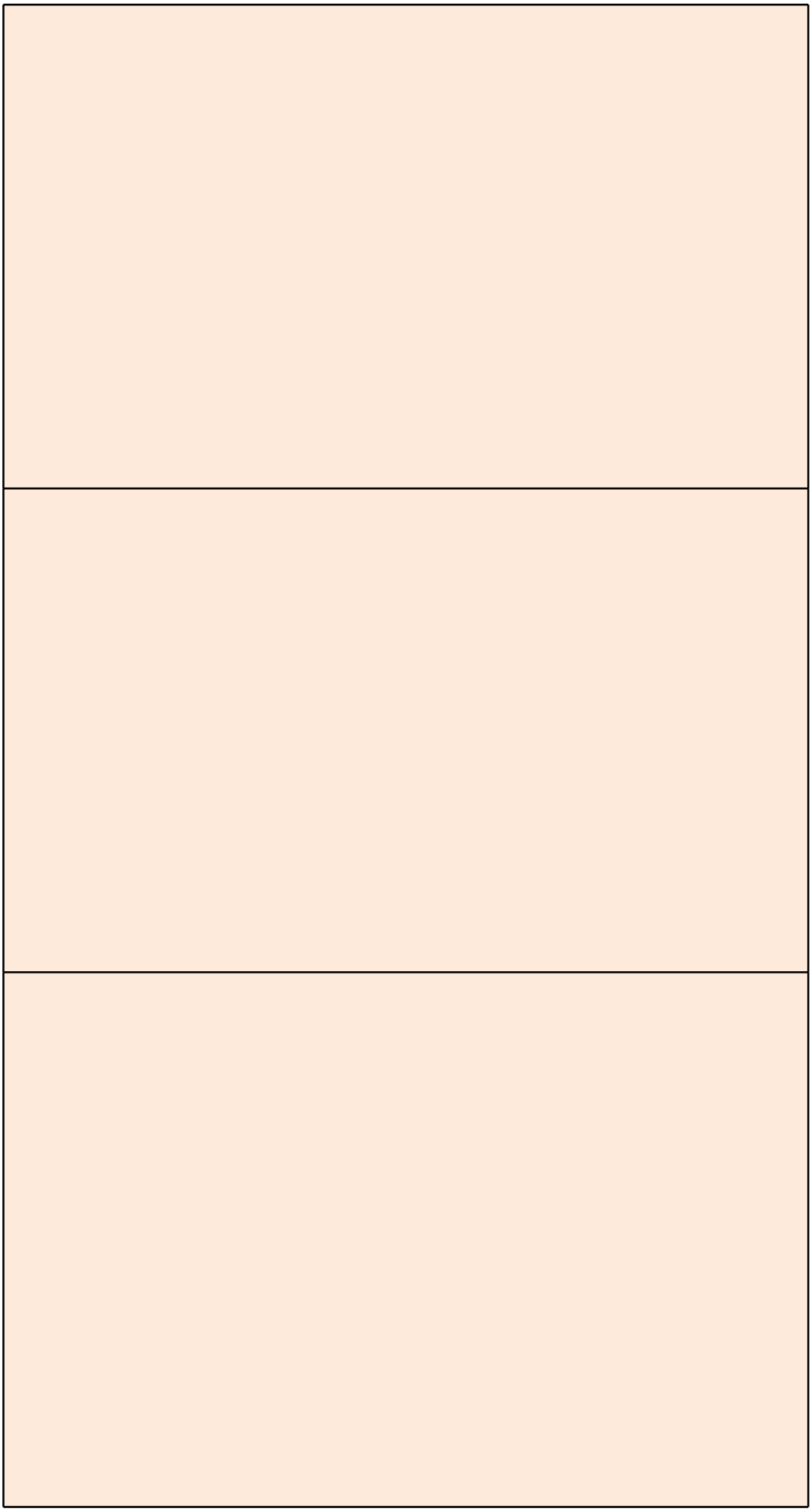


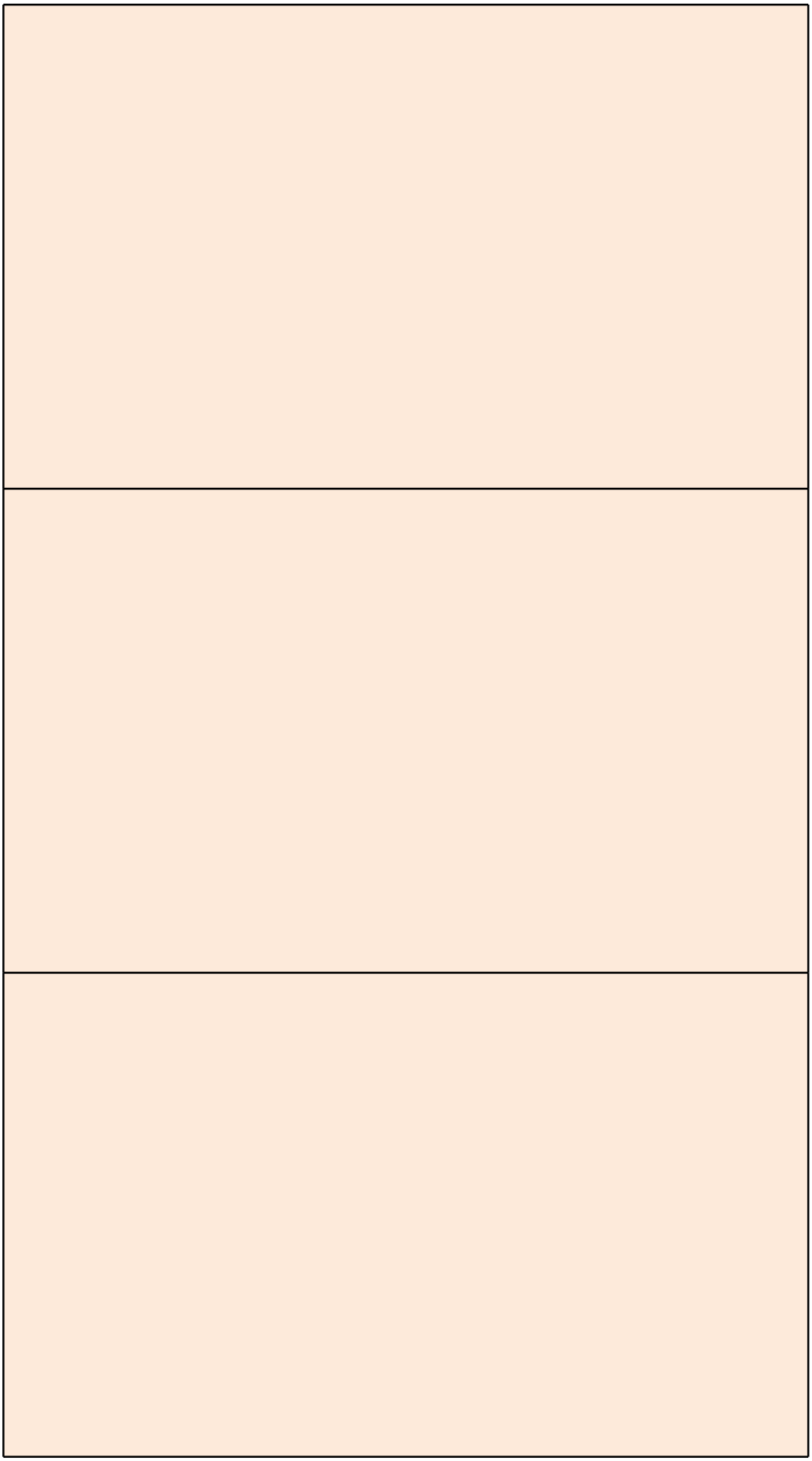


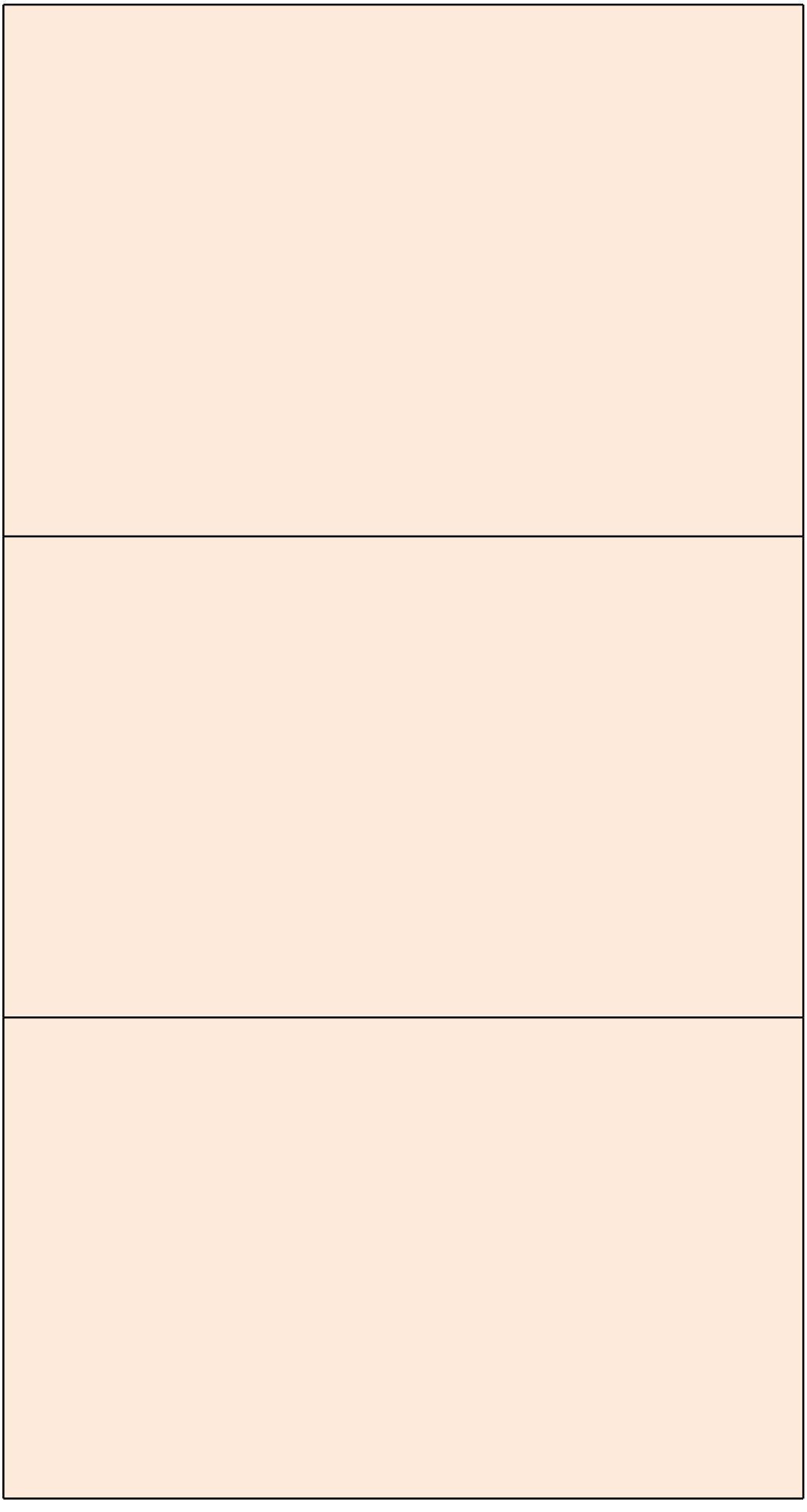


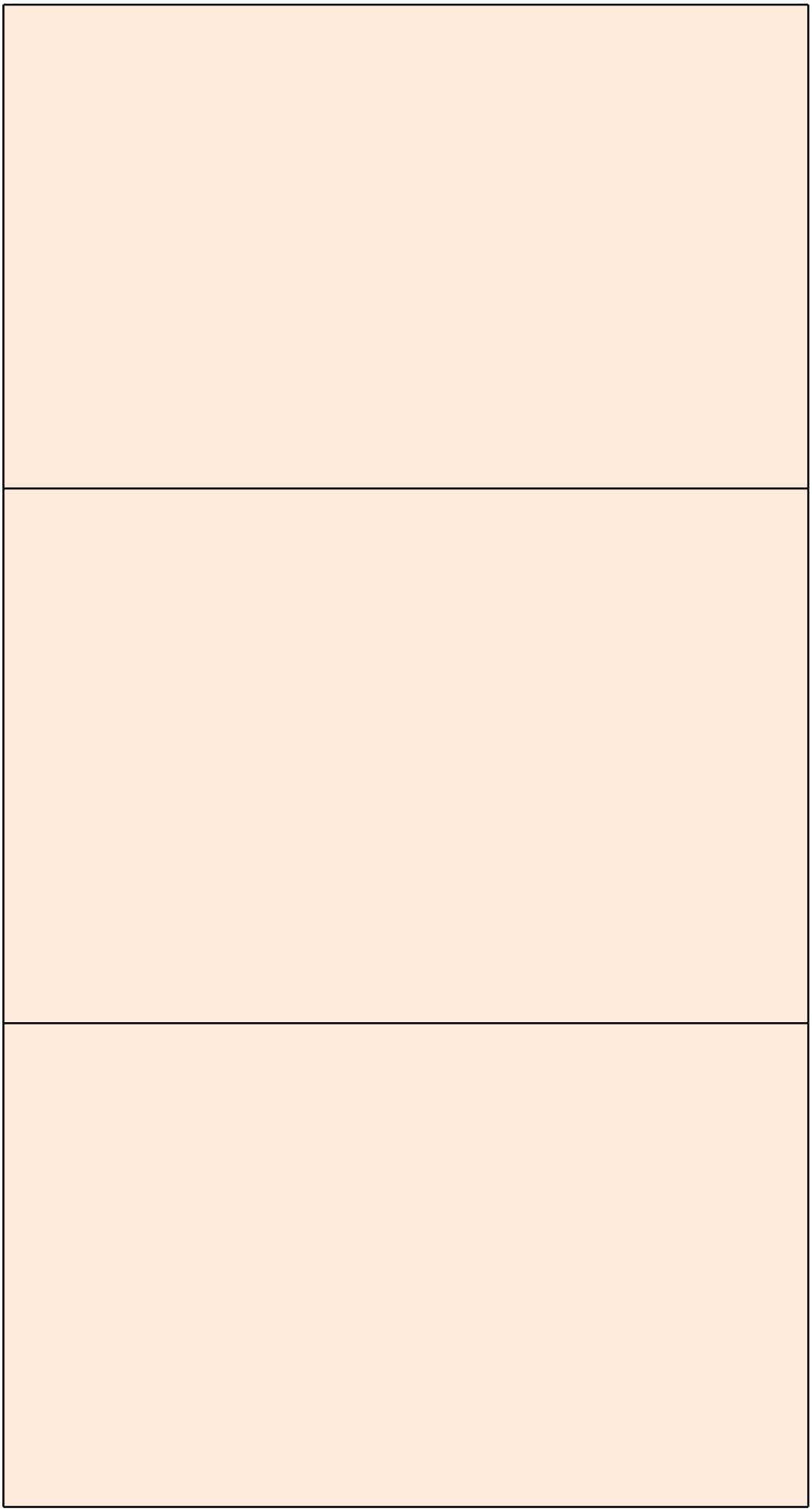


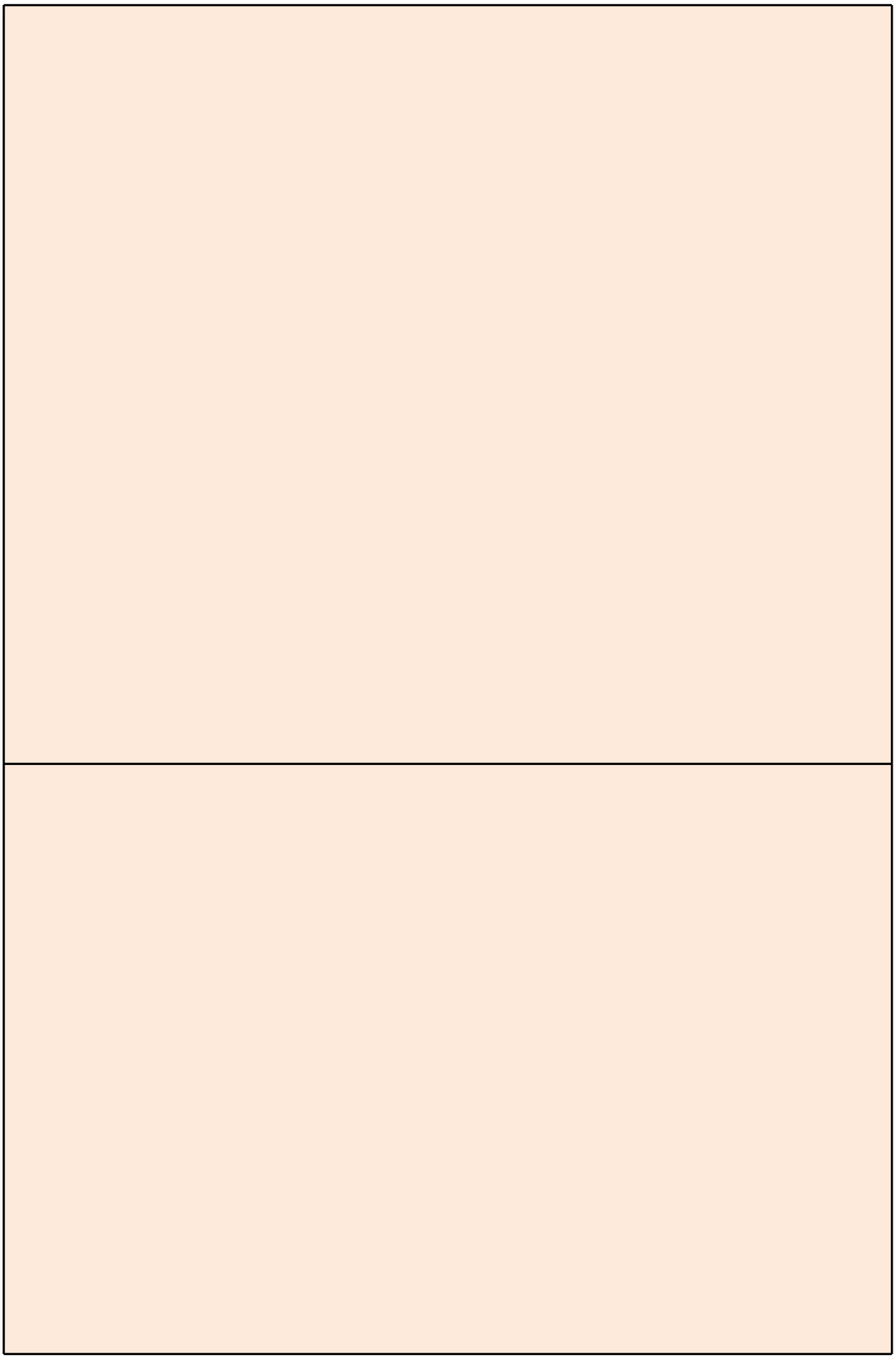


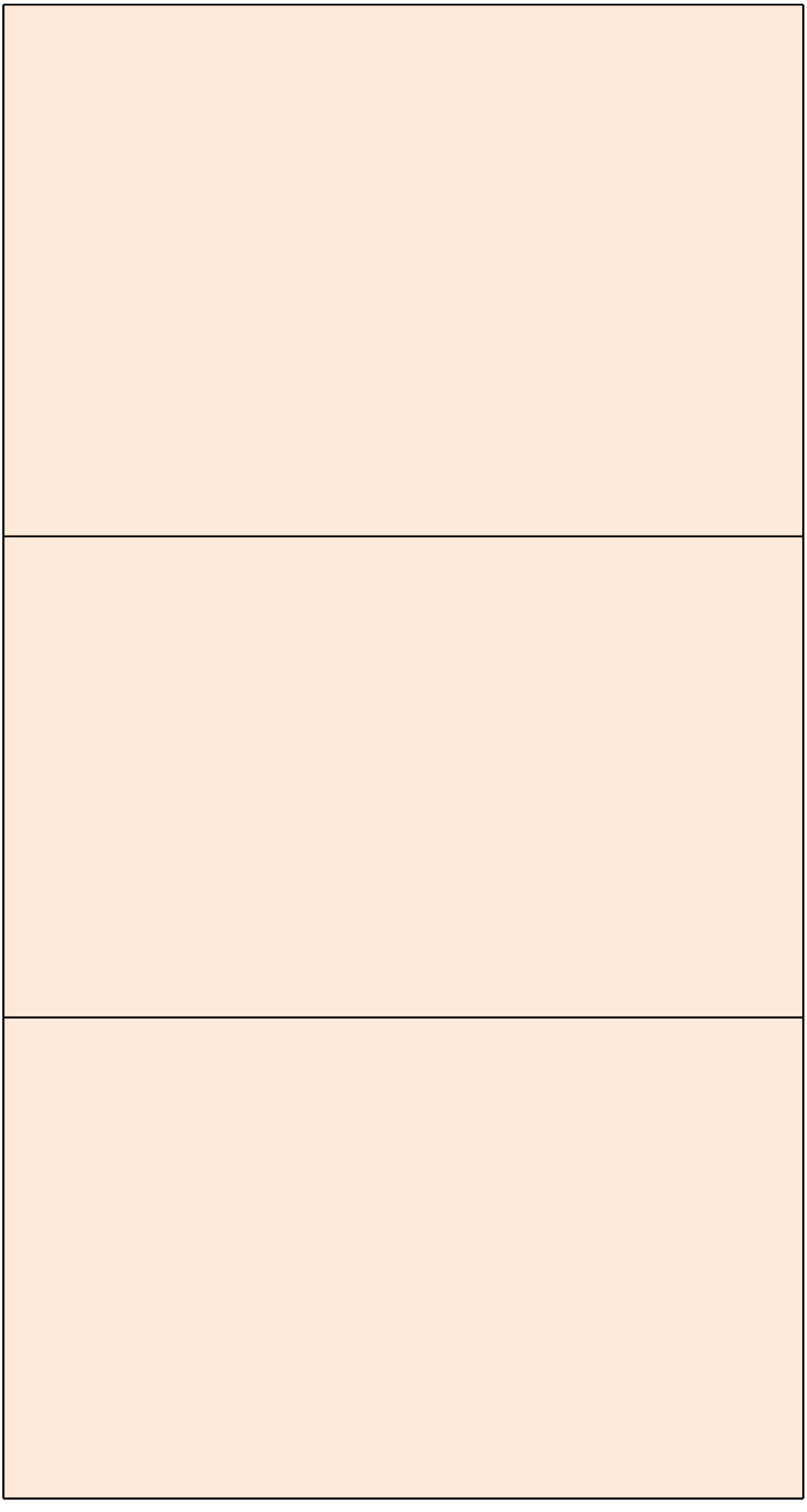


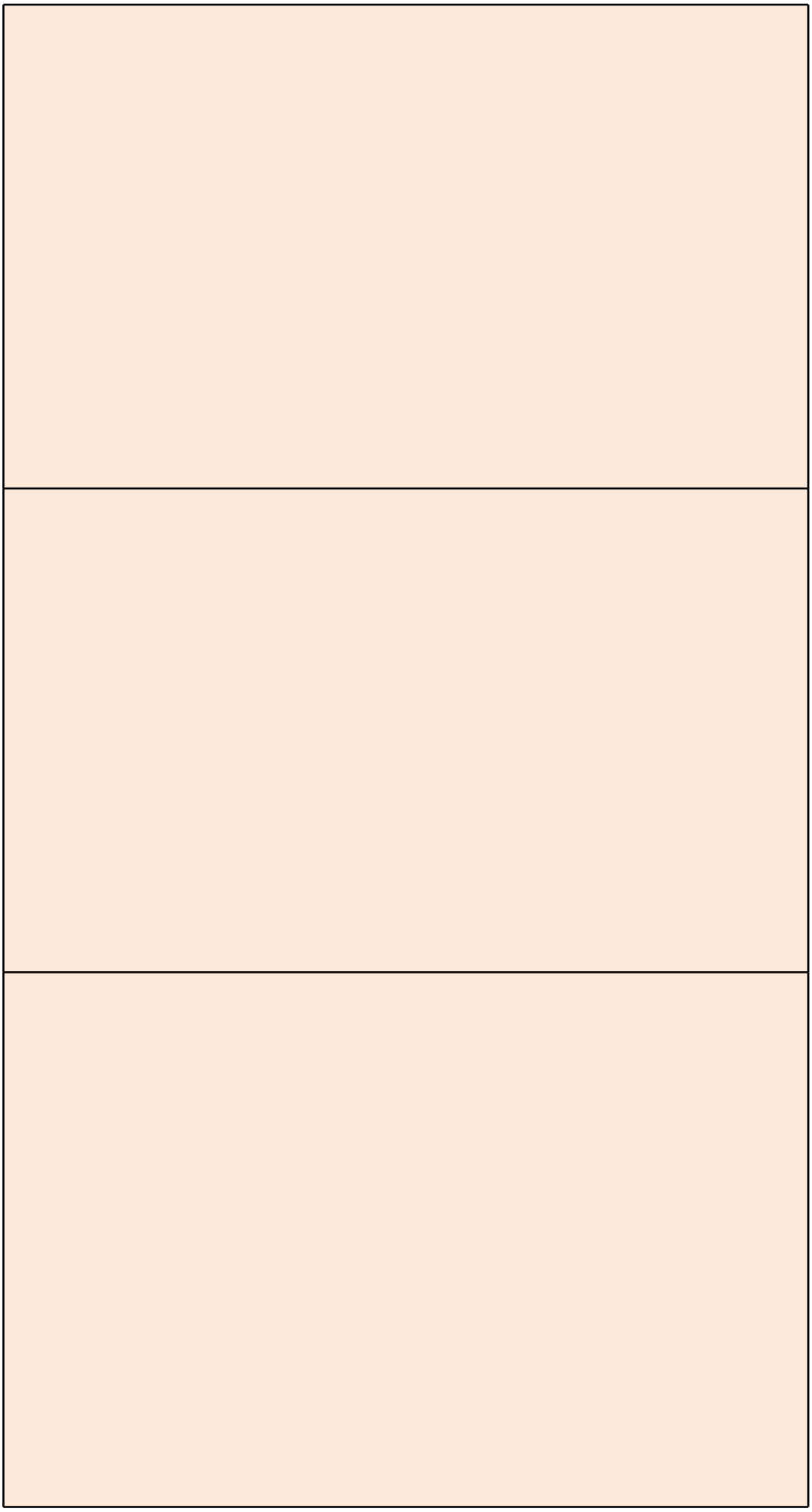


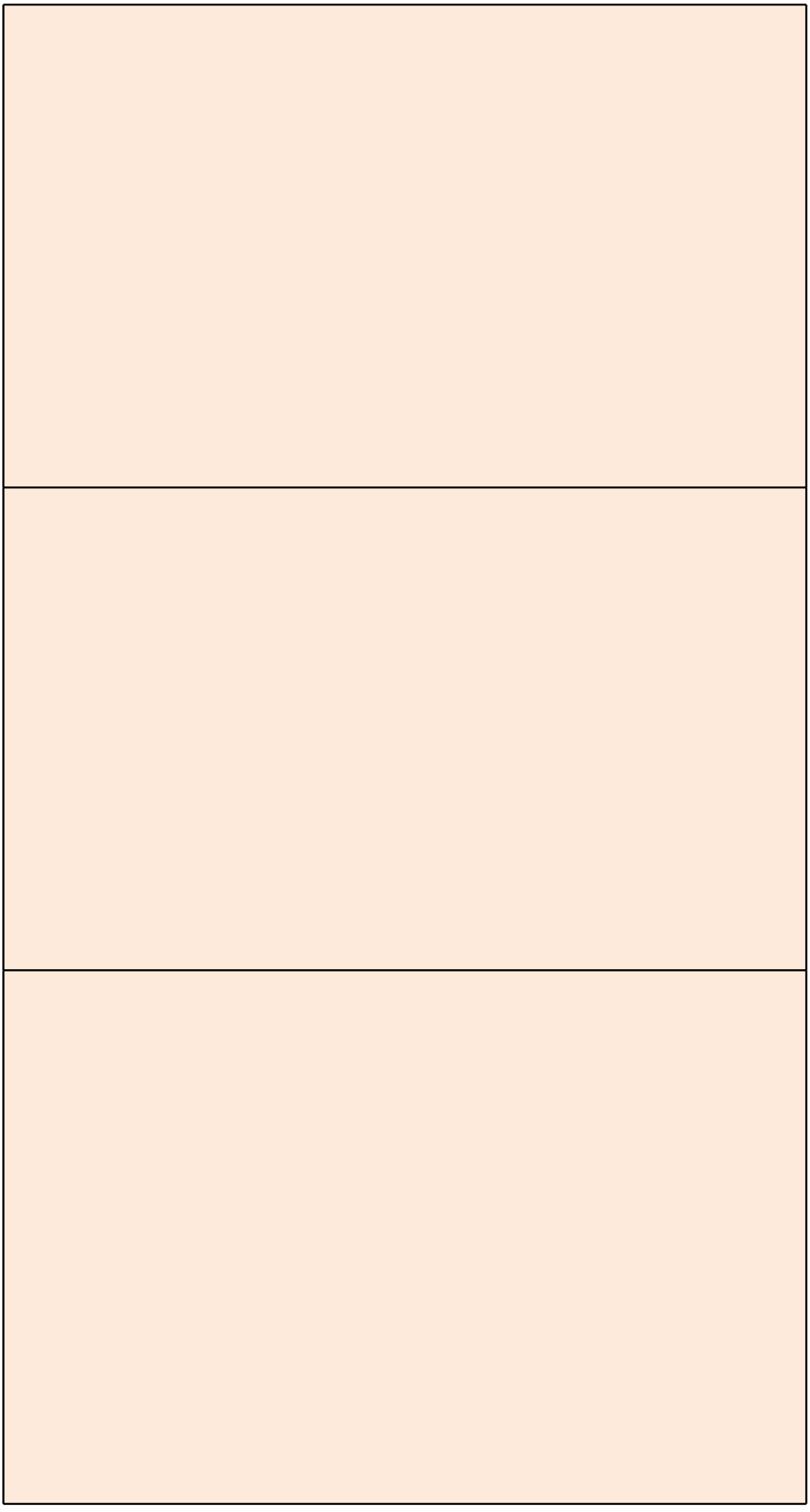


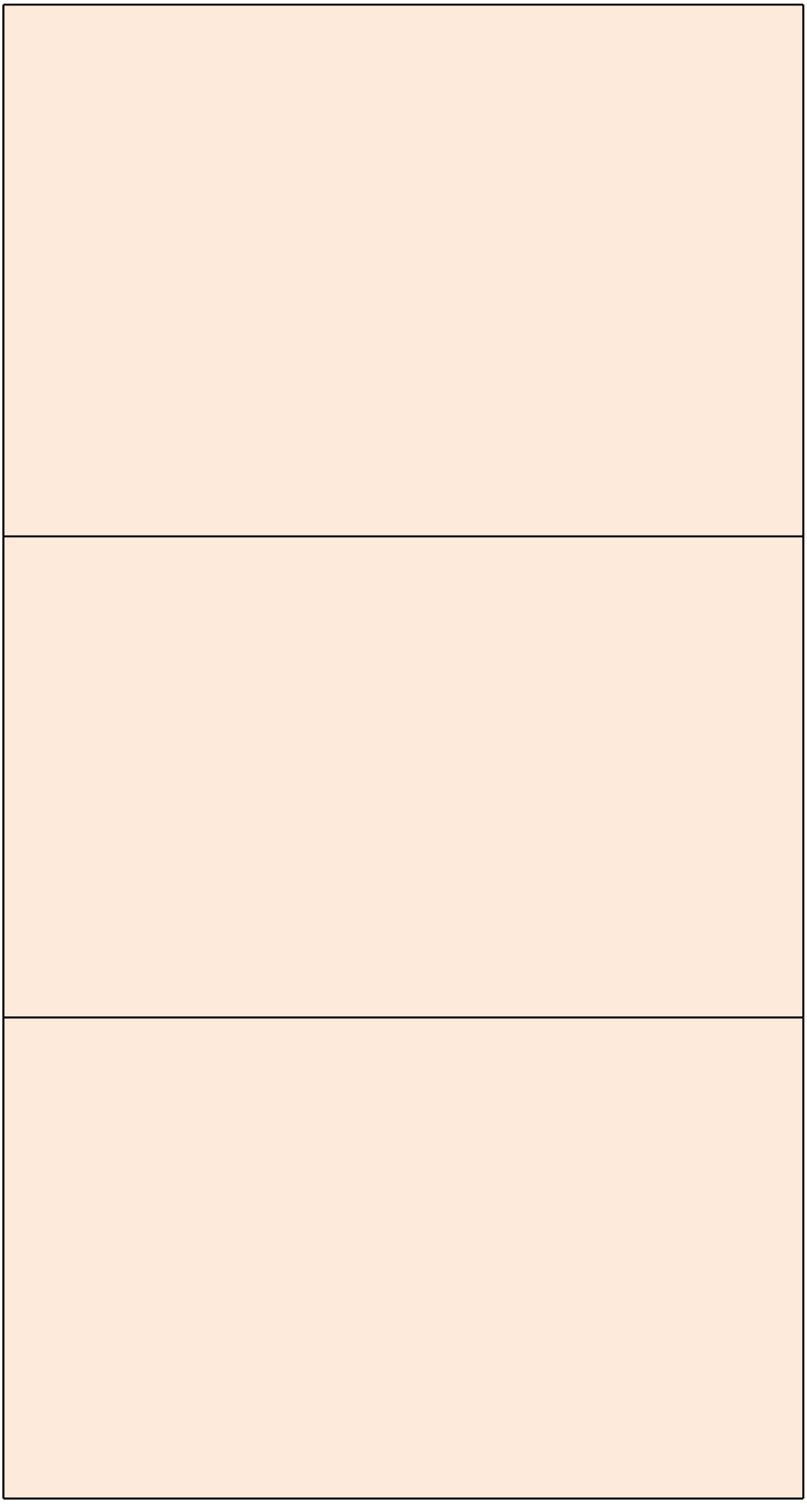


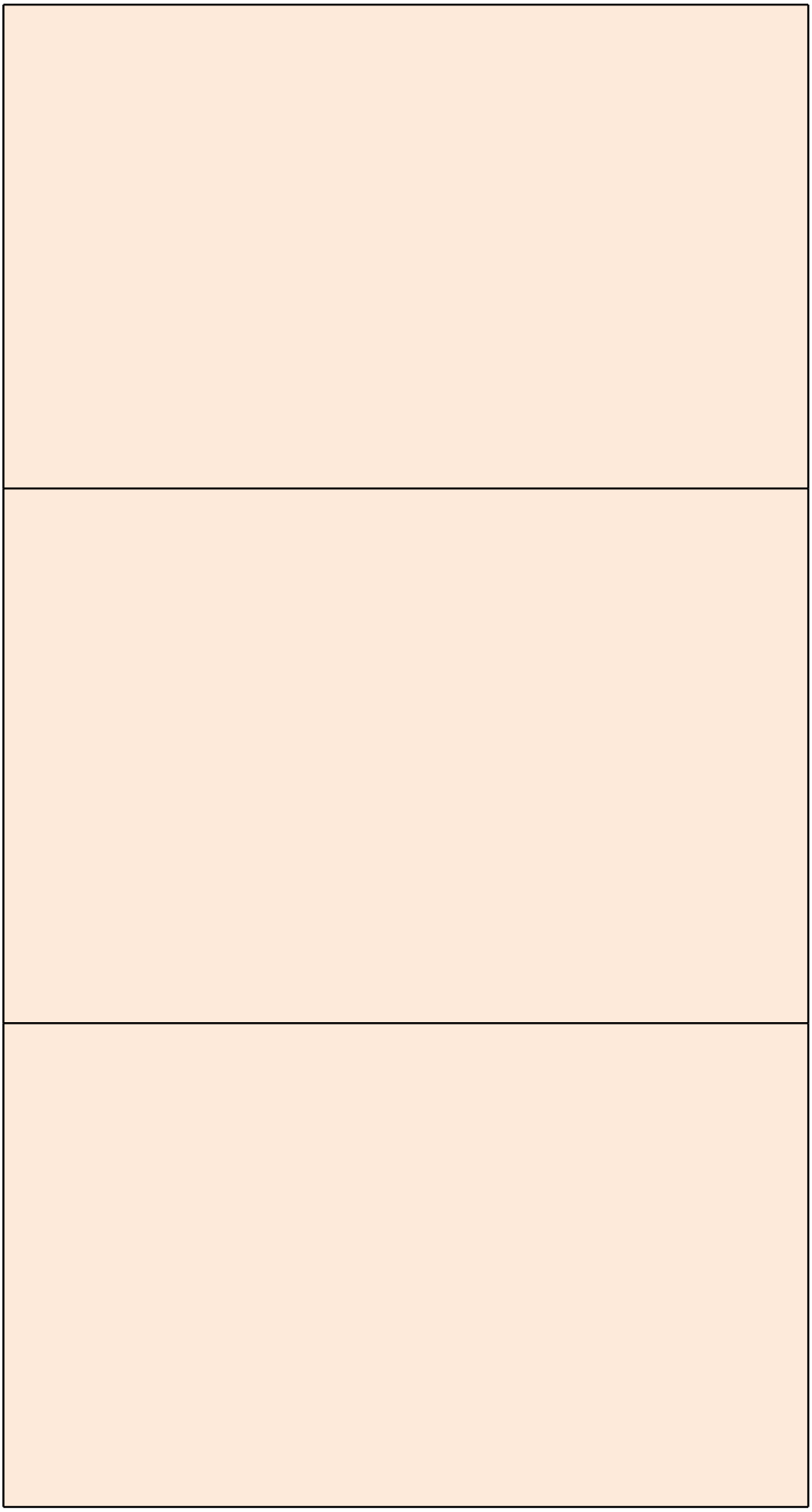


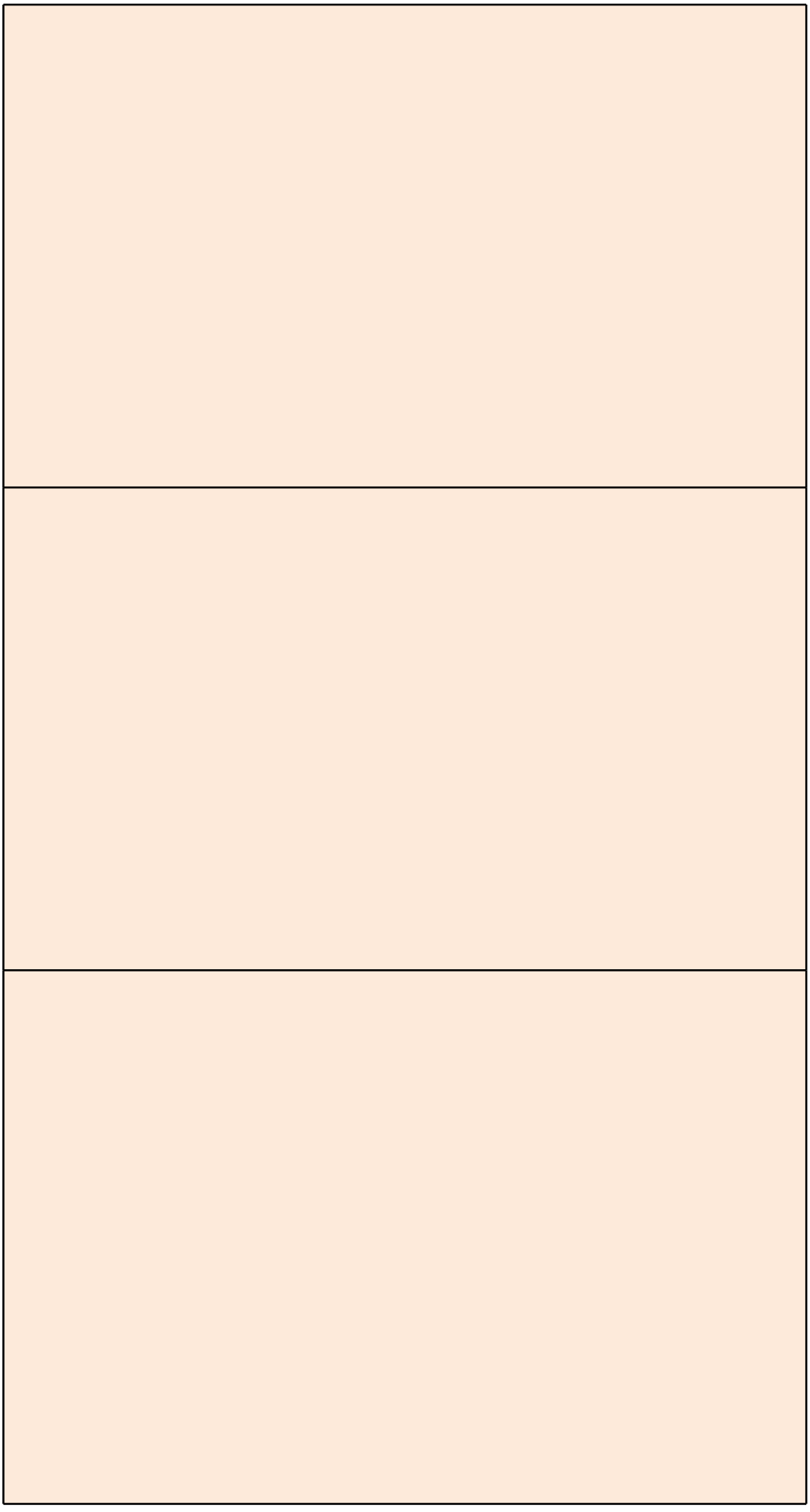


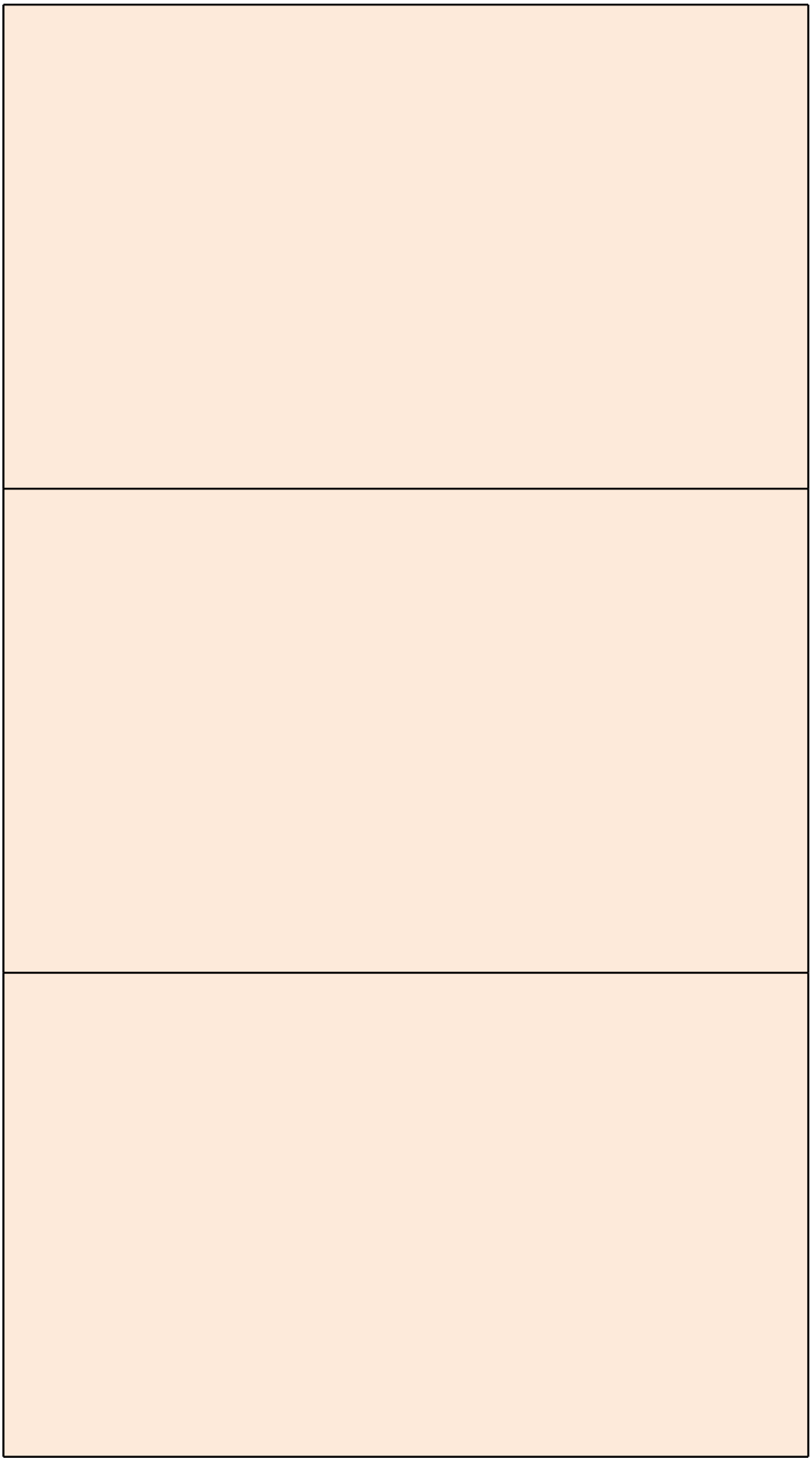


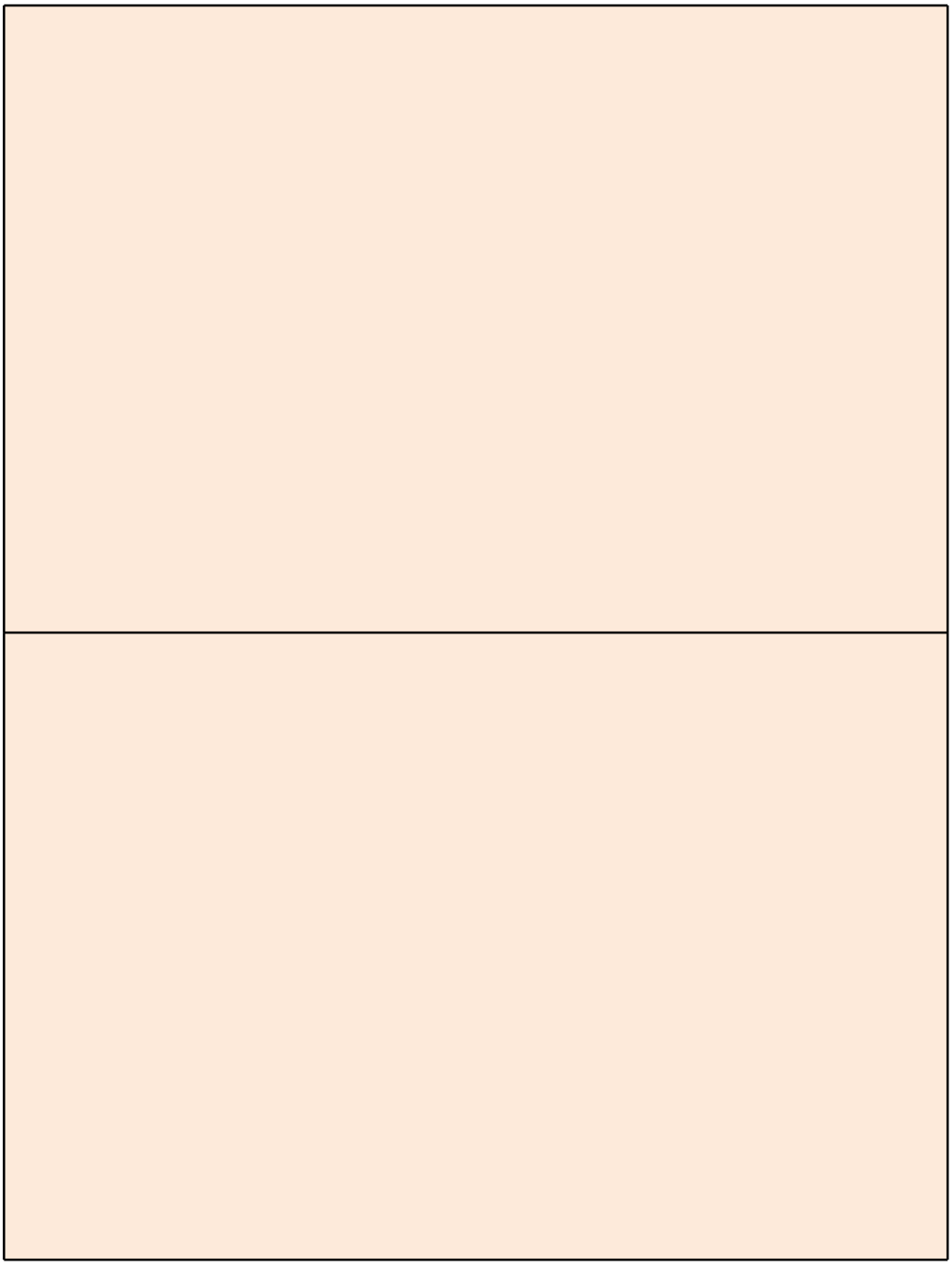


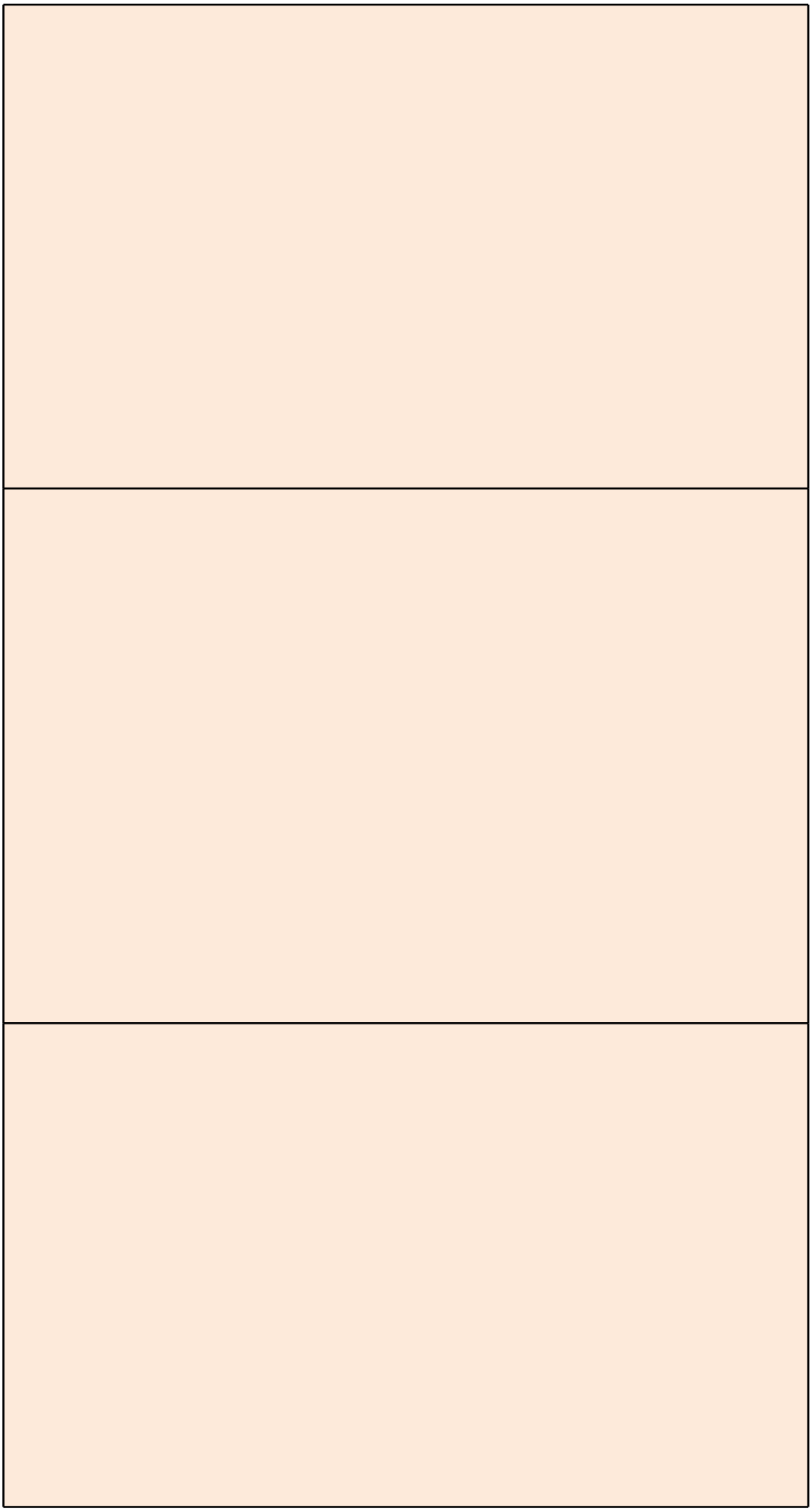


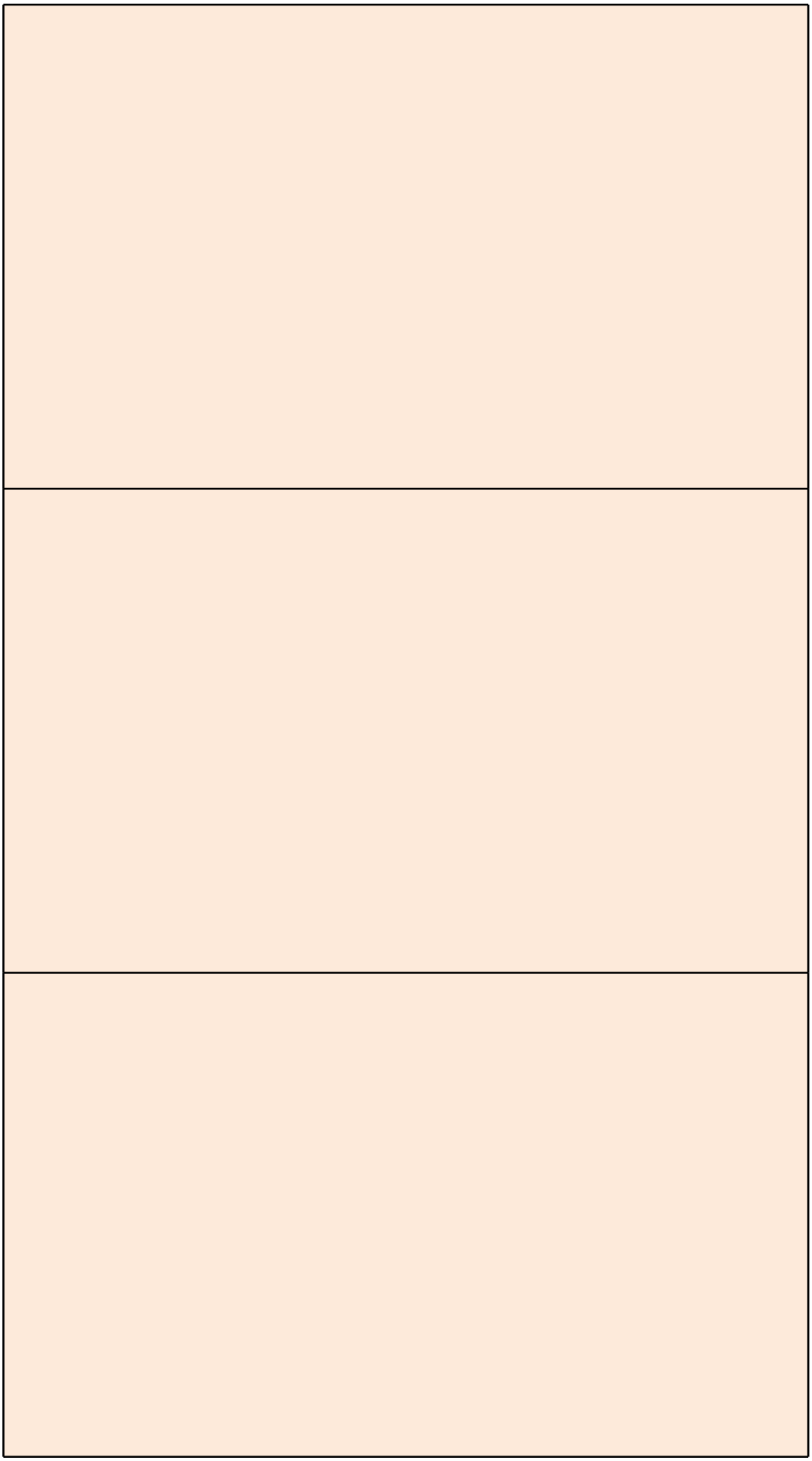


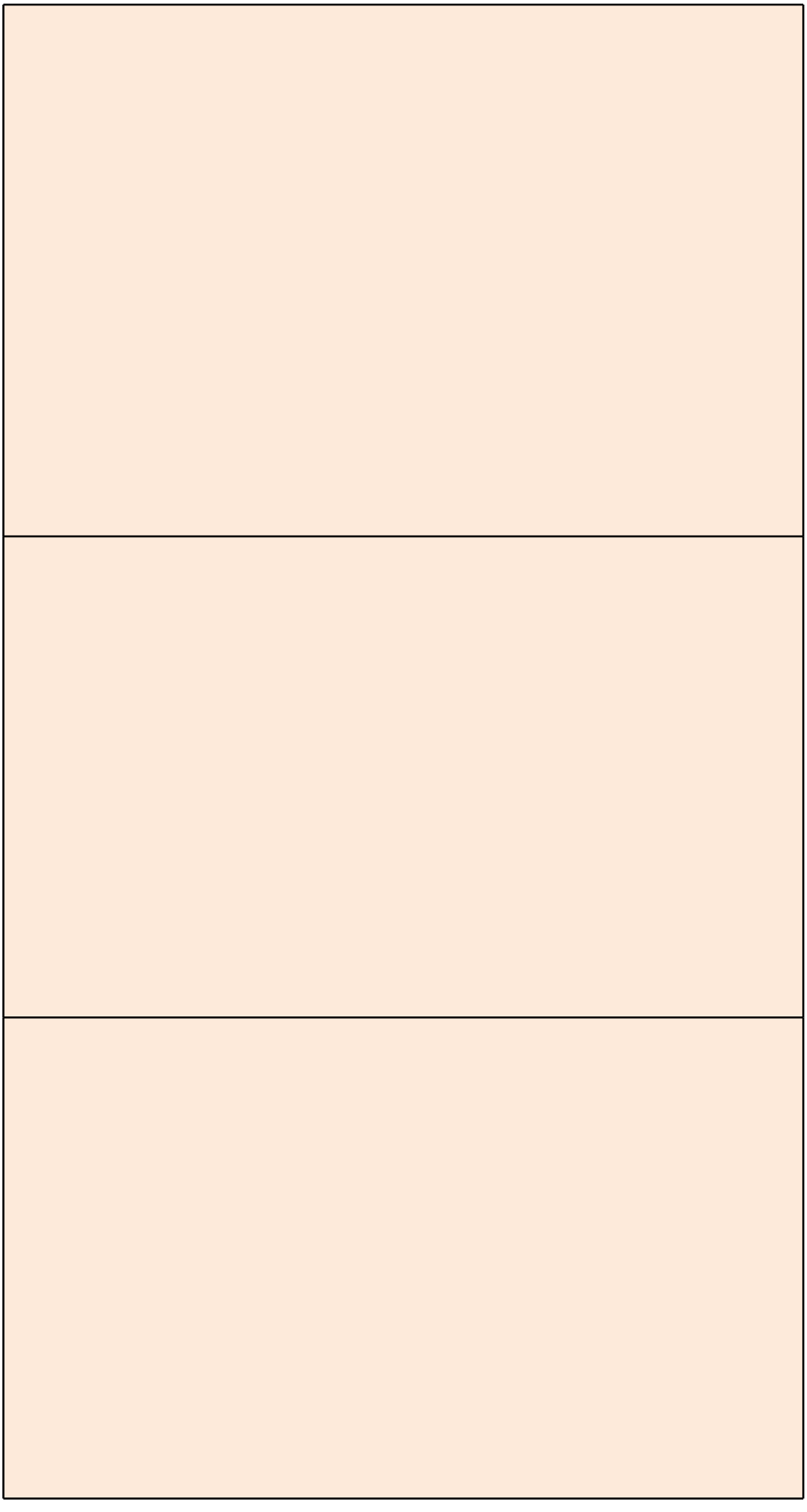


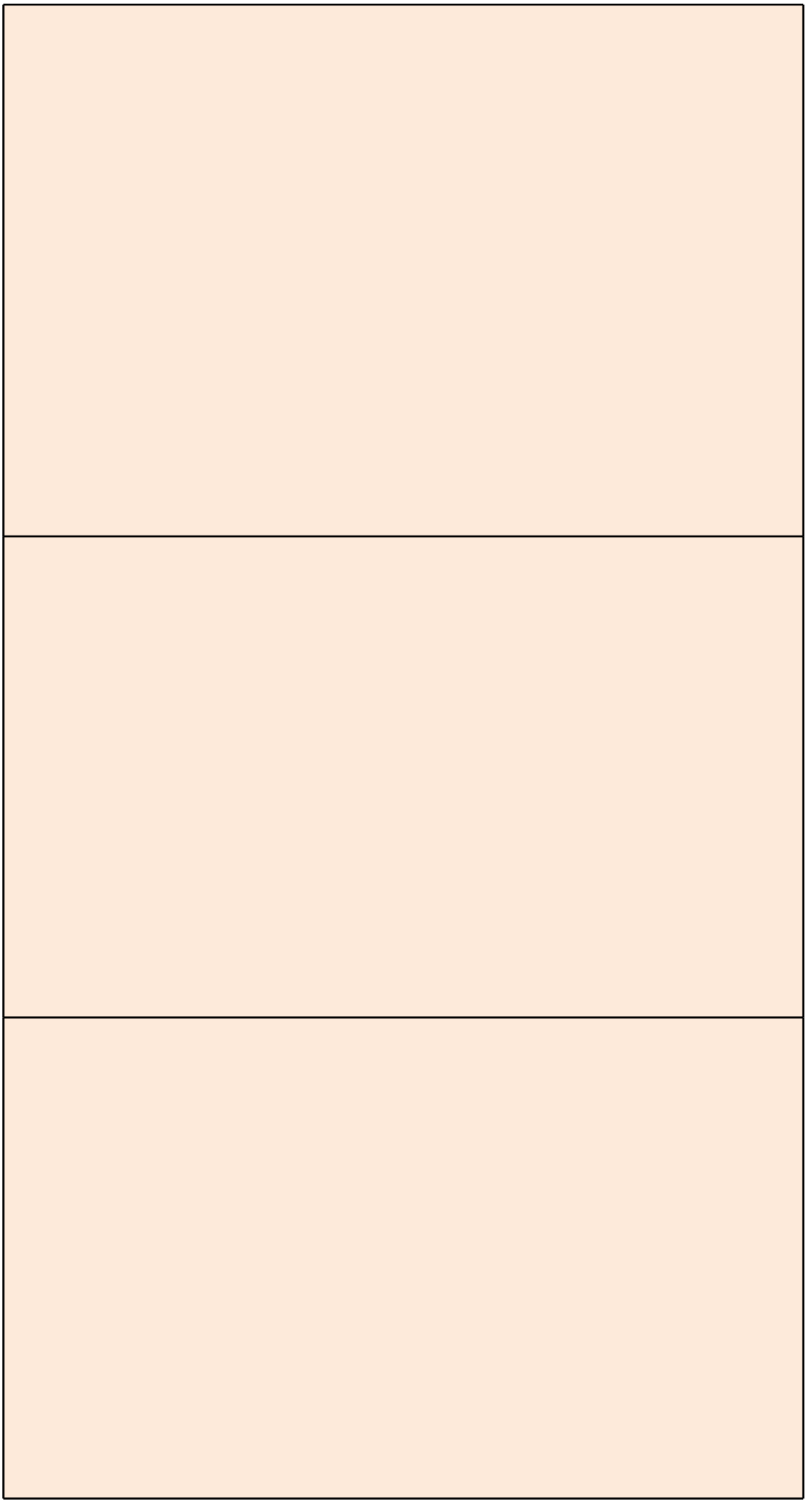


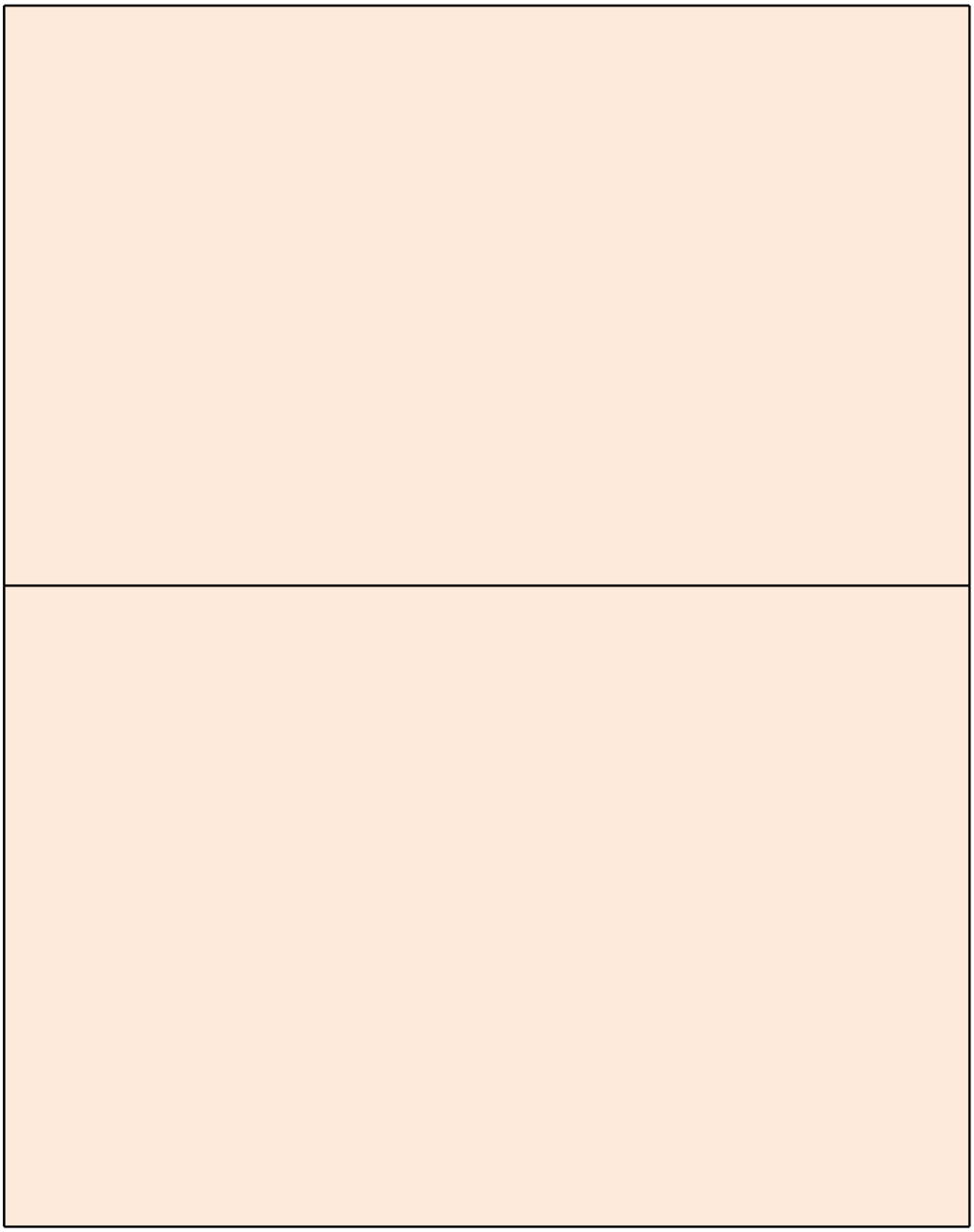


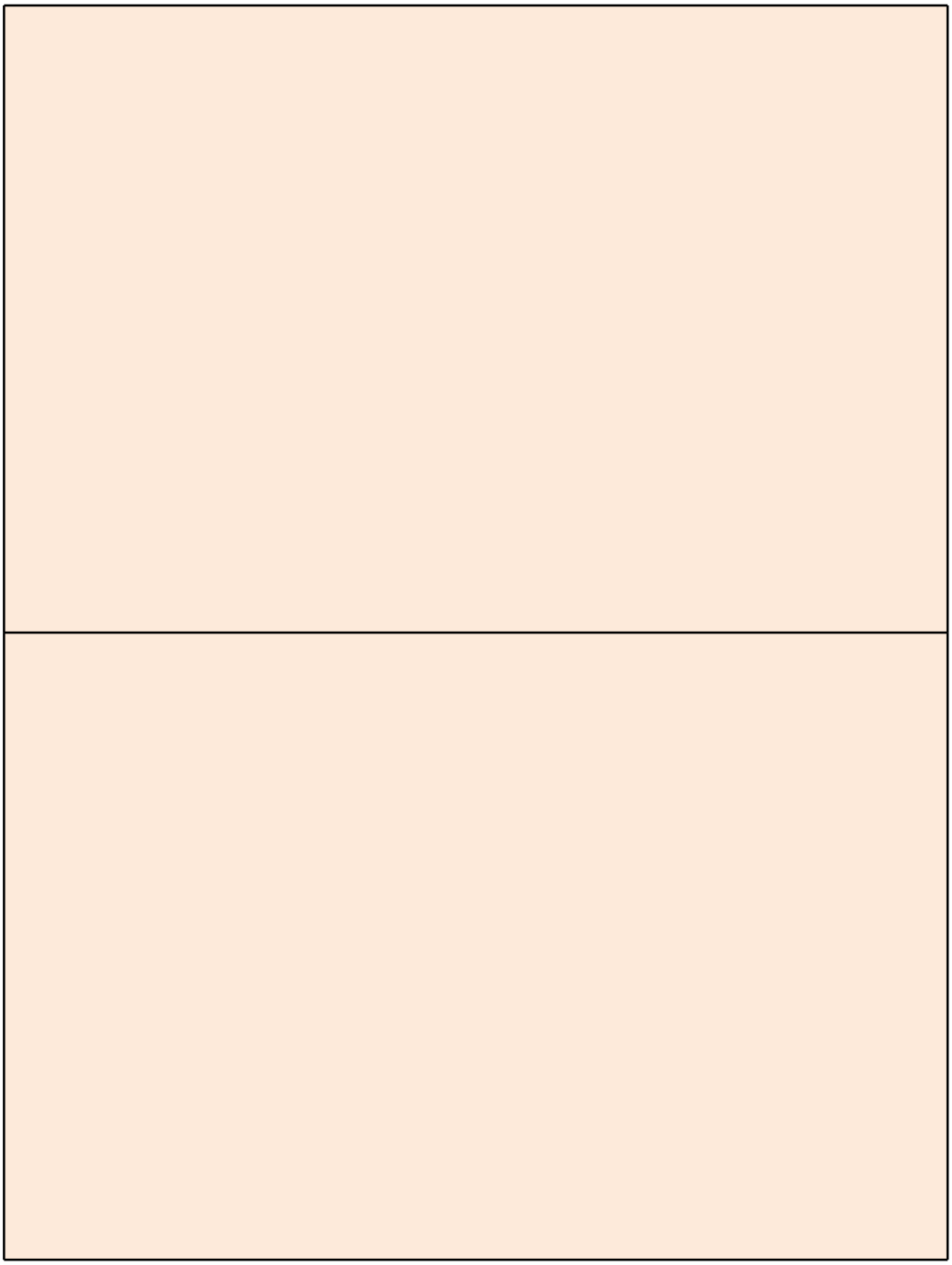




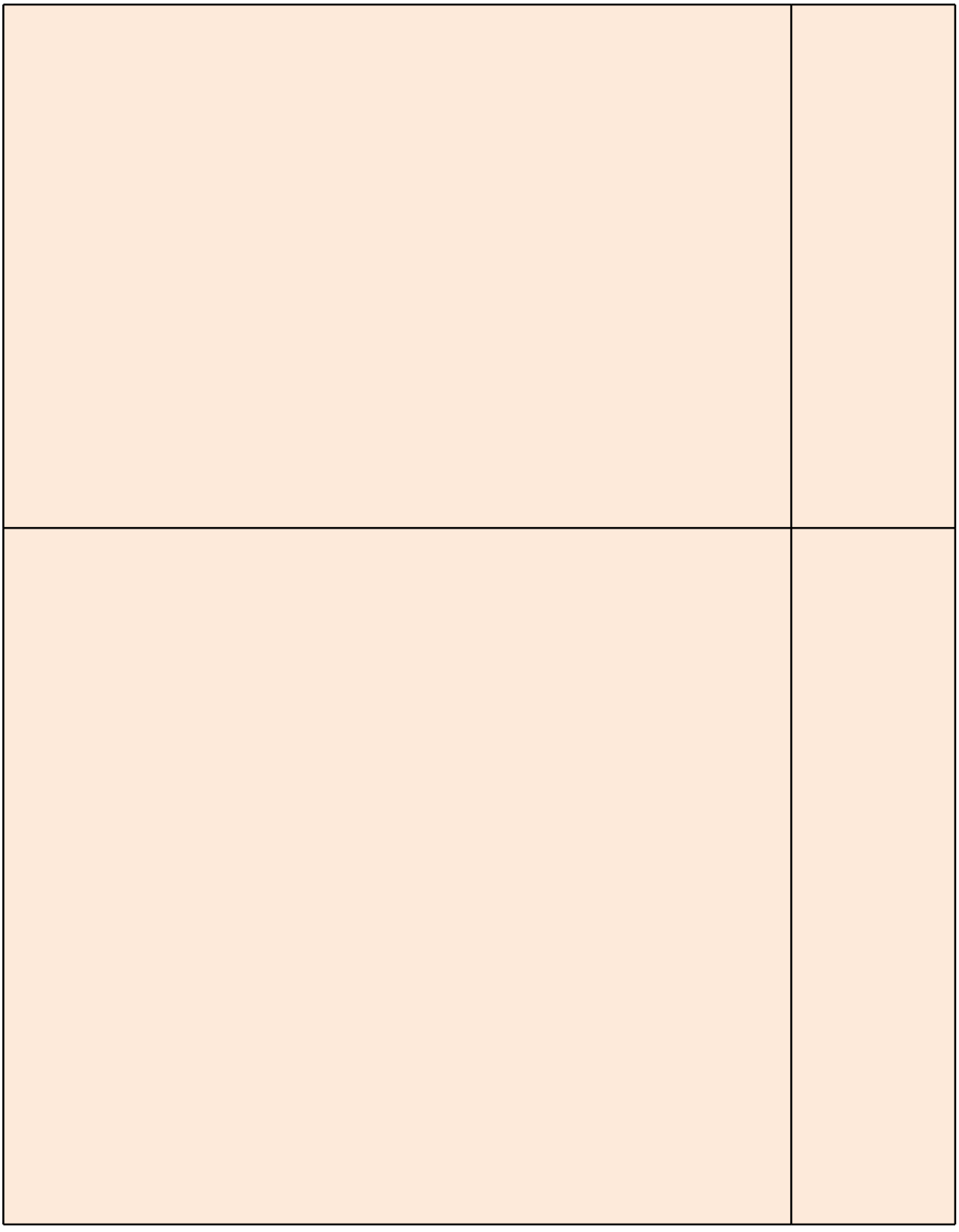


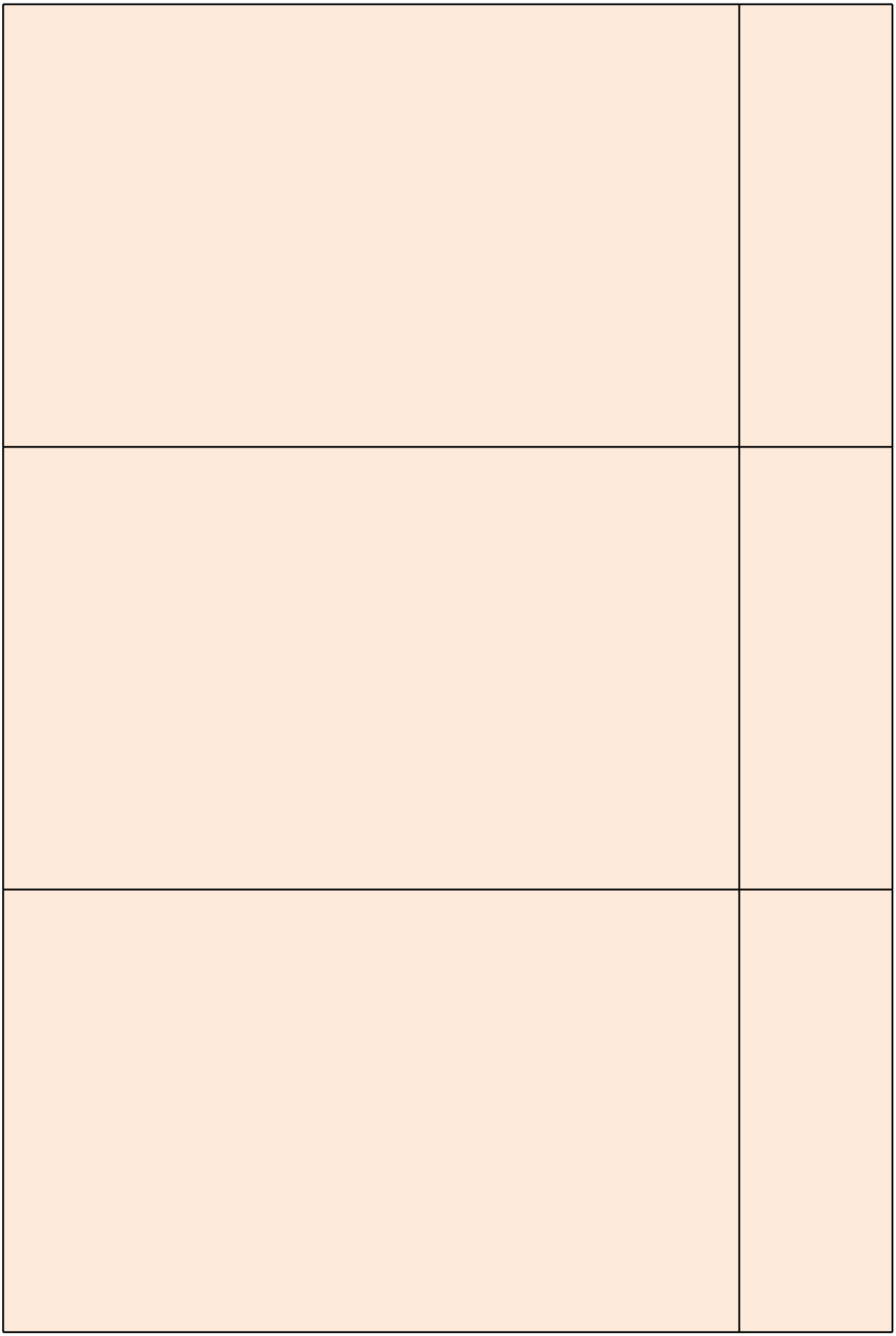


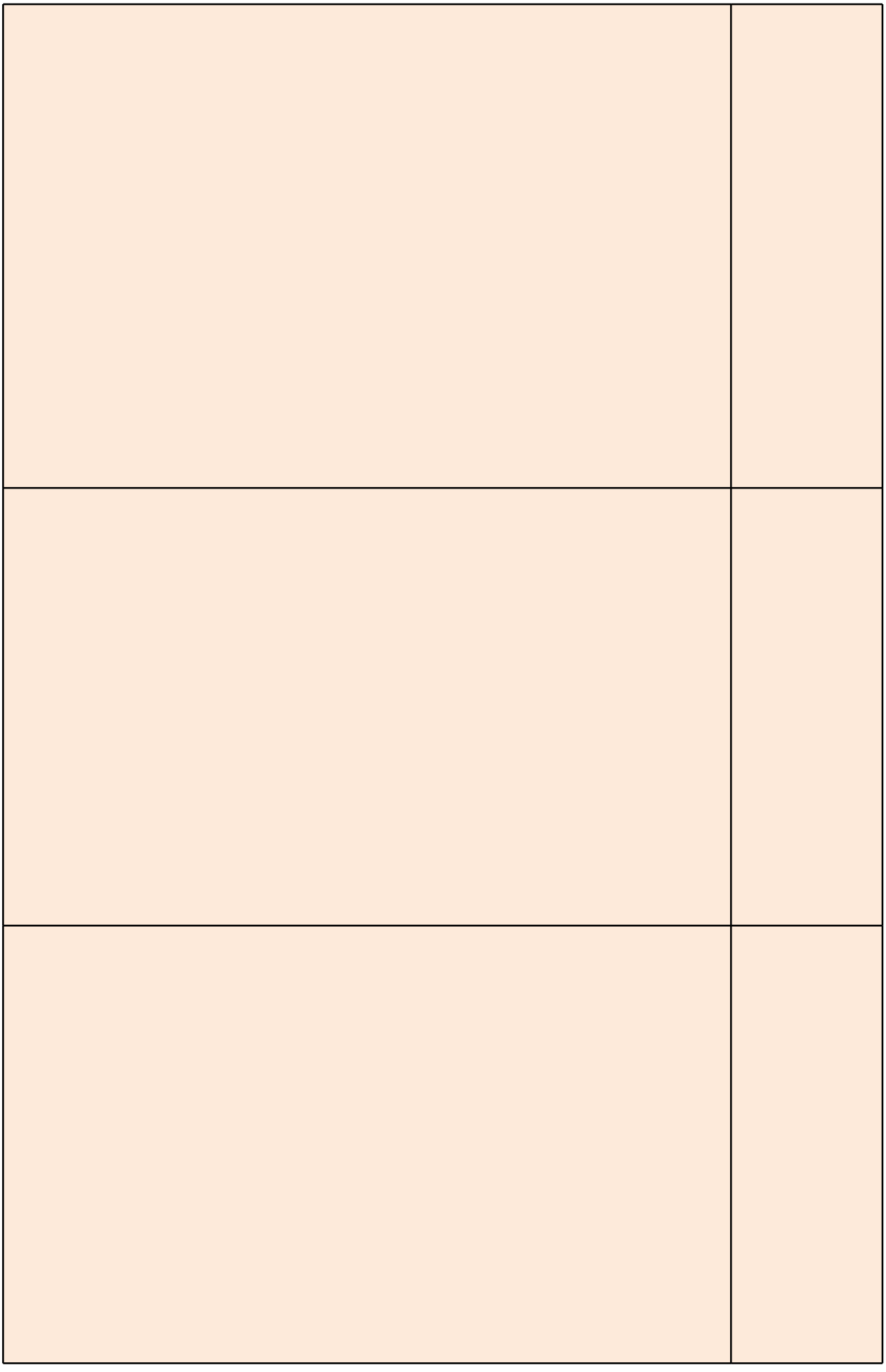


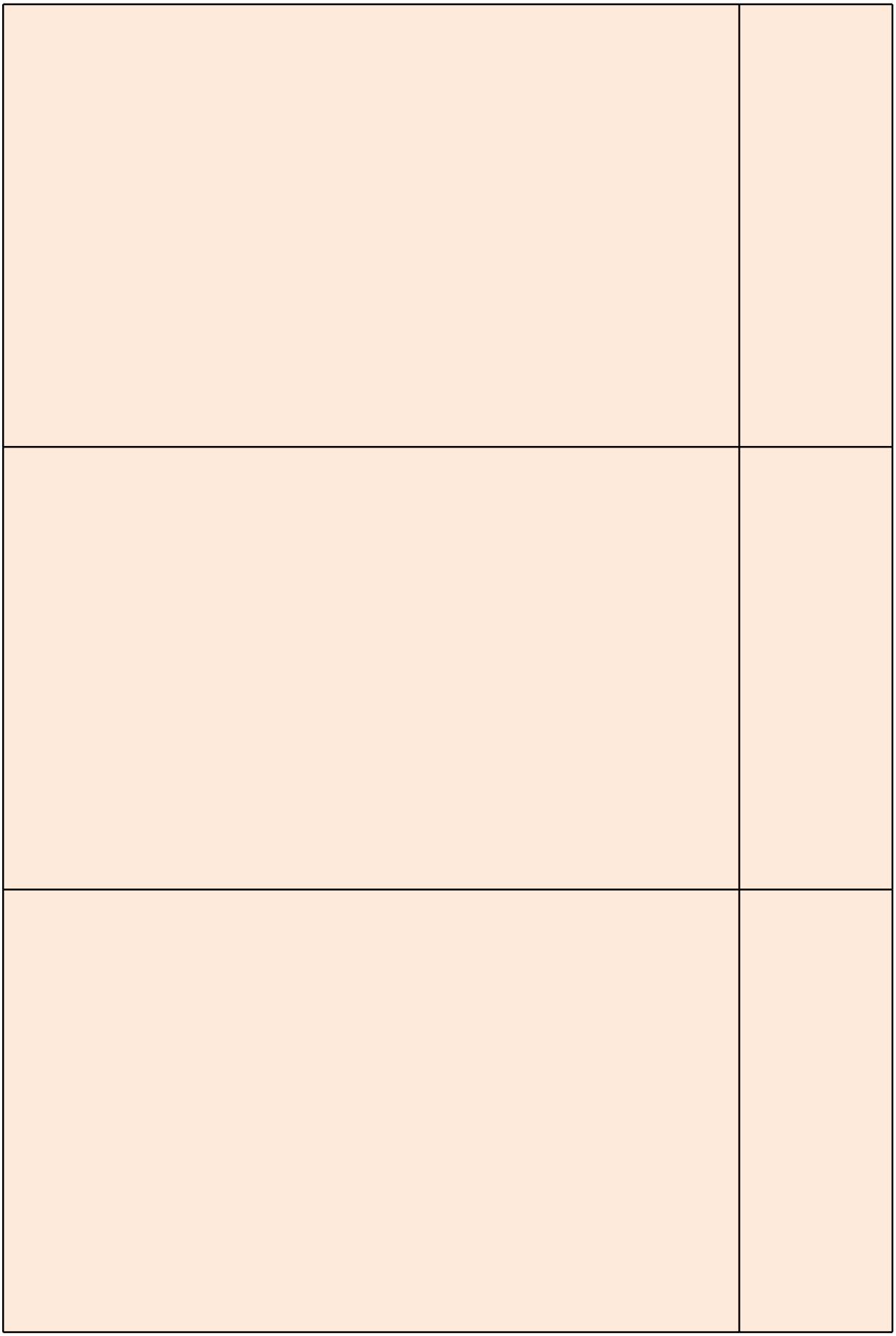


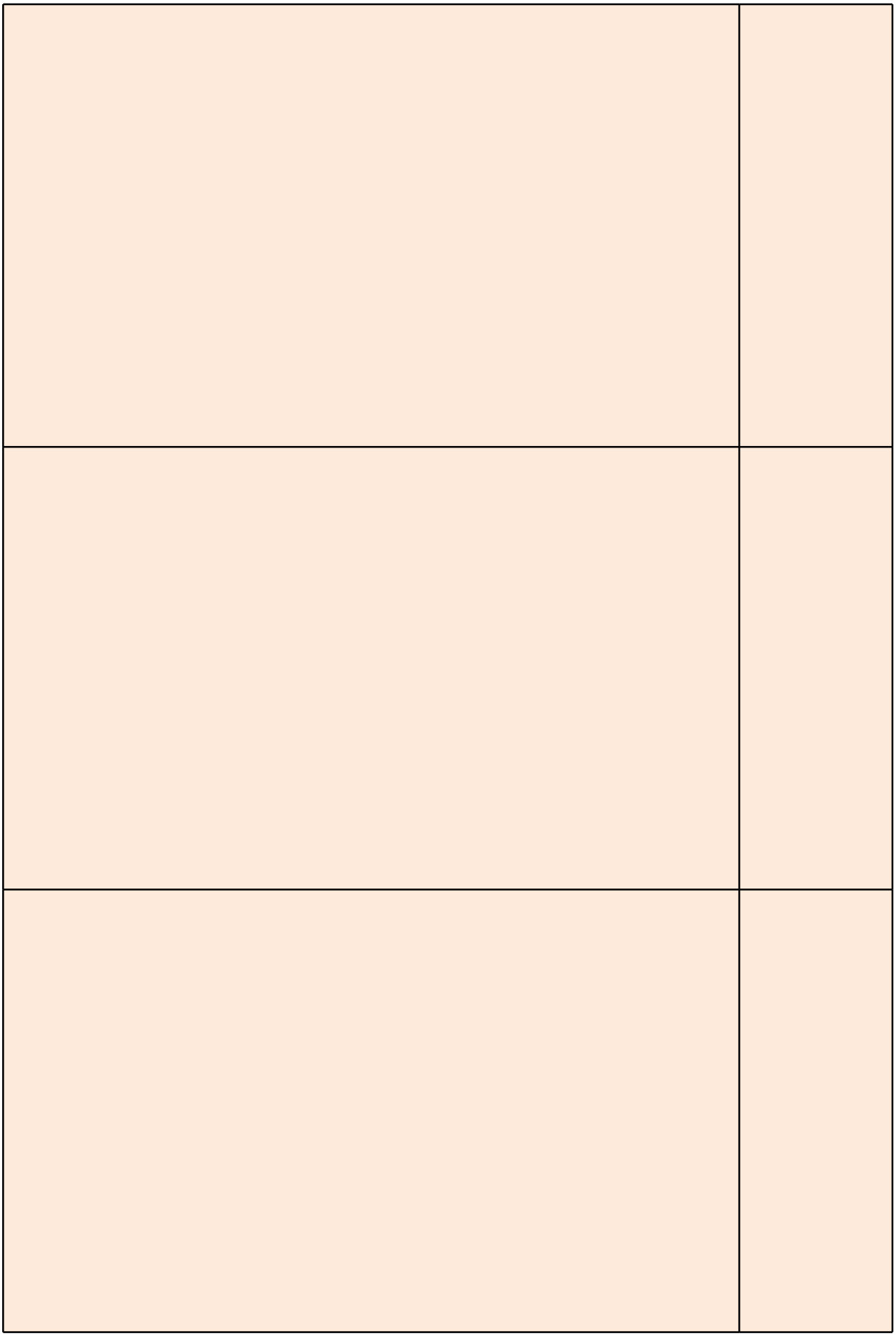
Siirtymäsäännöstarve (ext)	Organisaatio

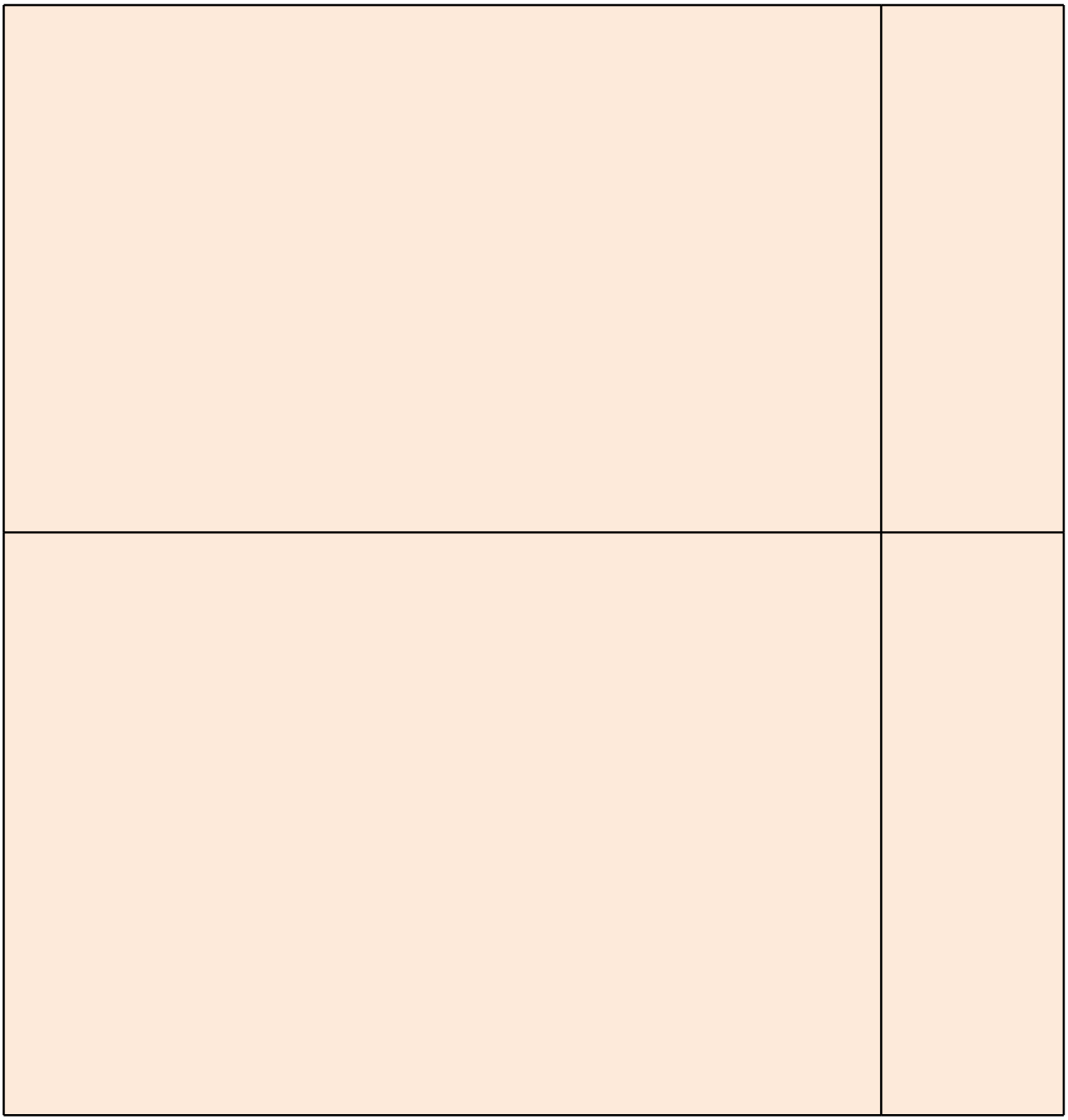


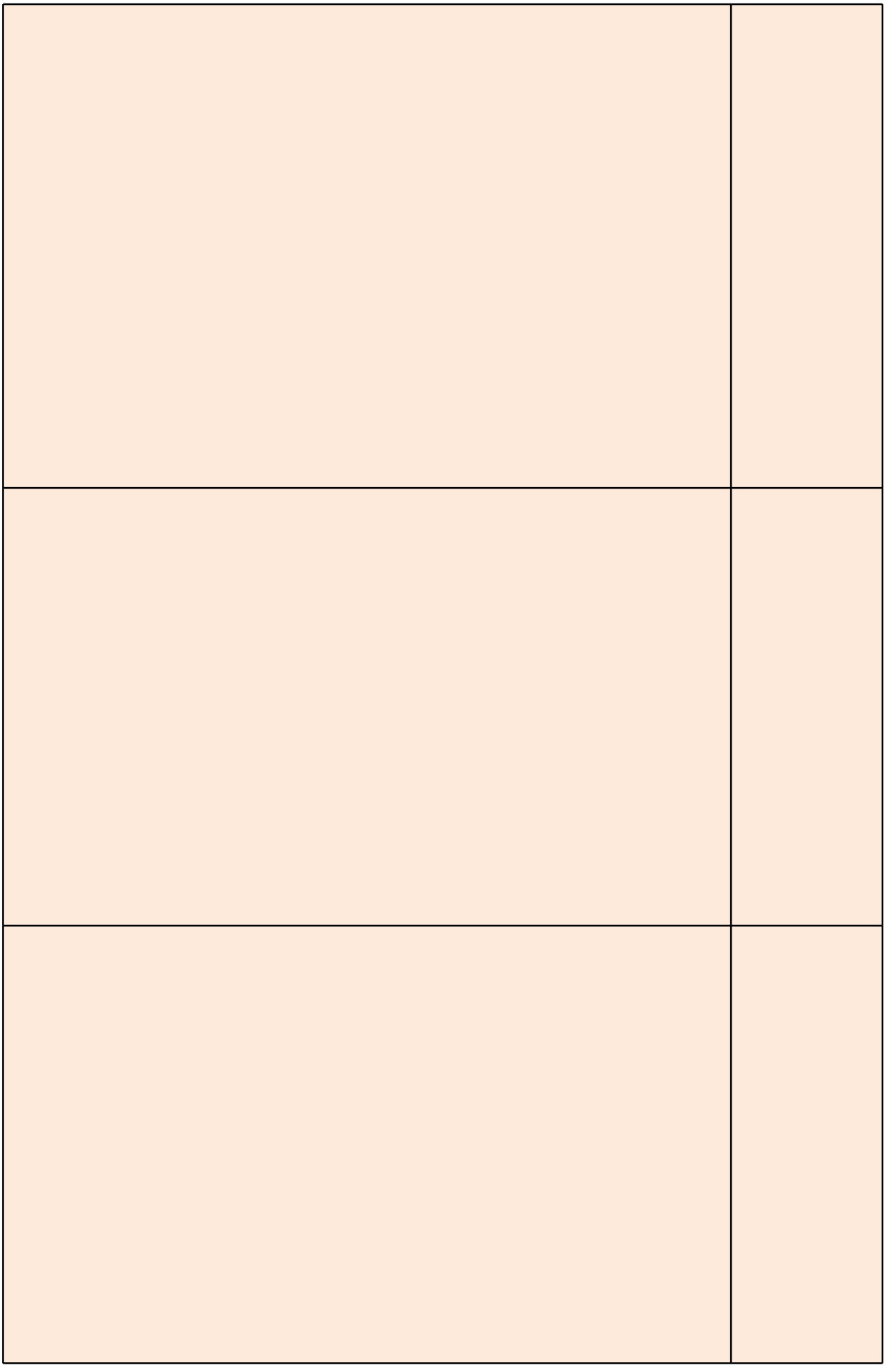


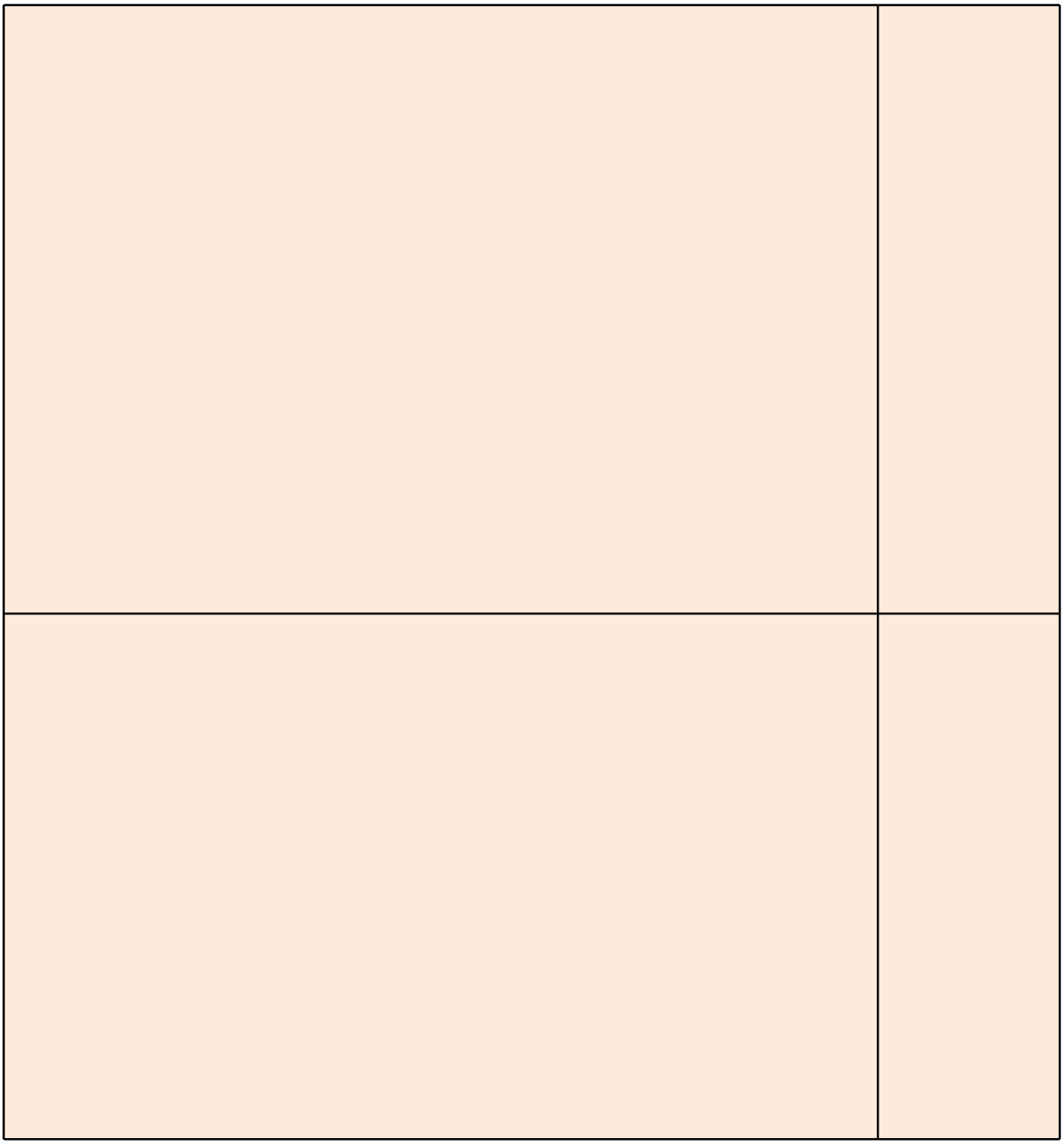


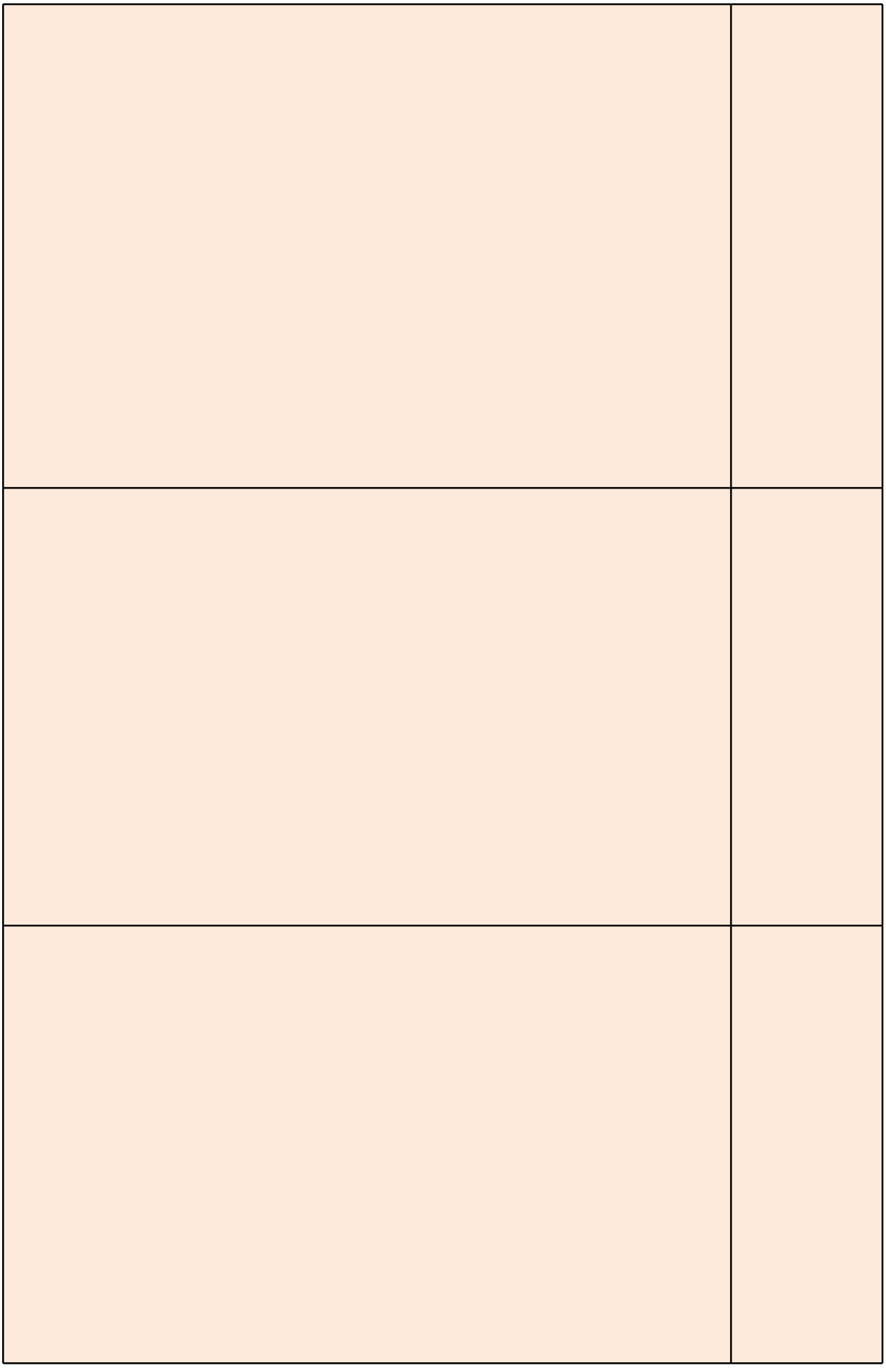


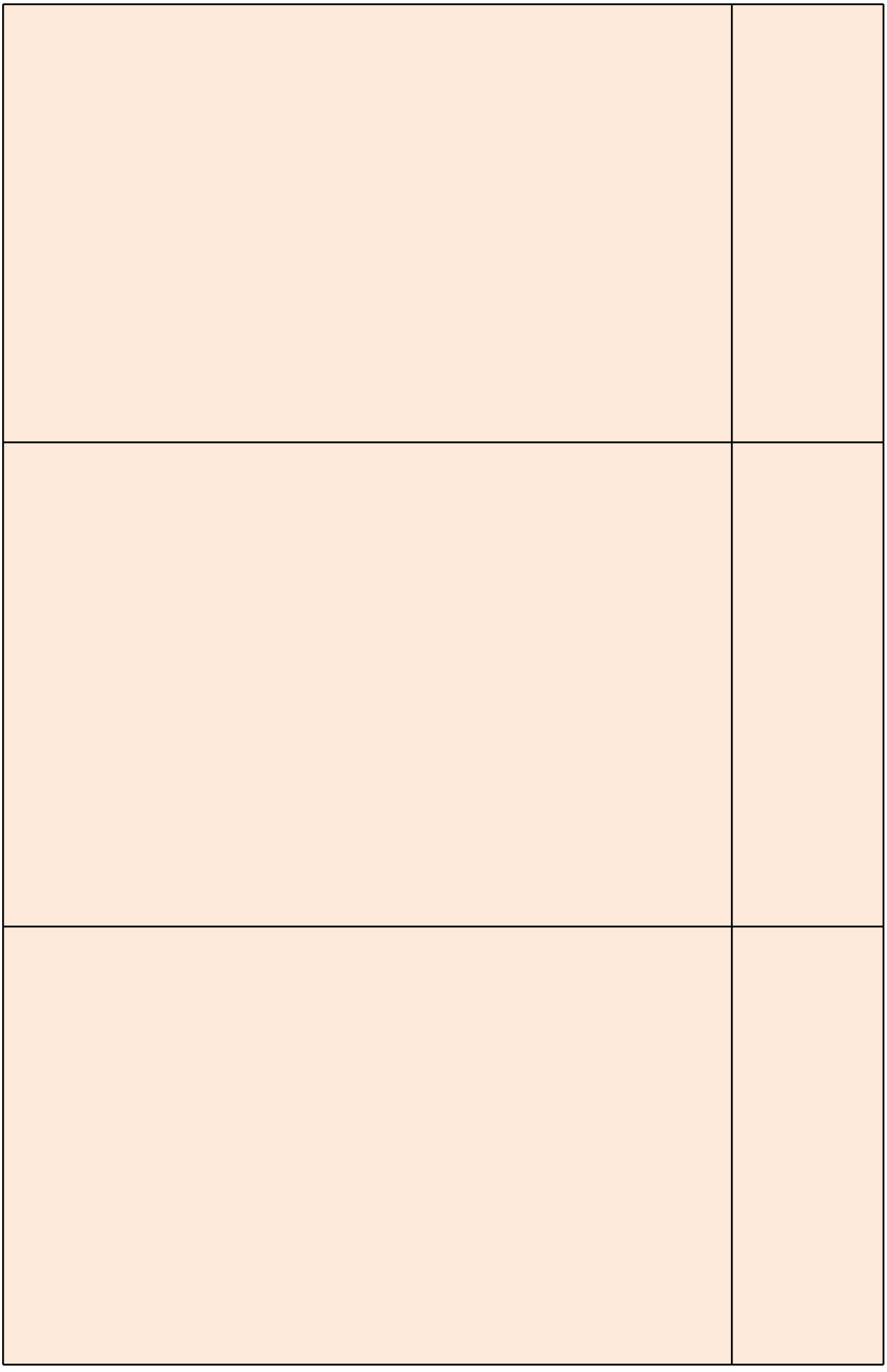


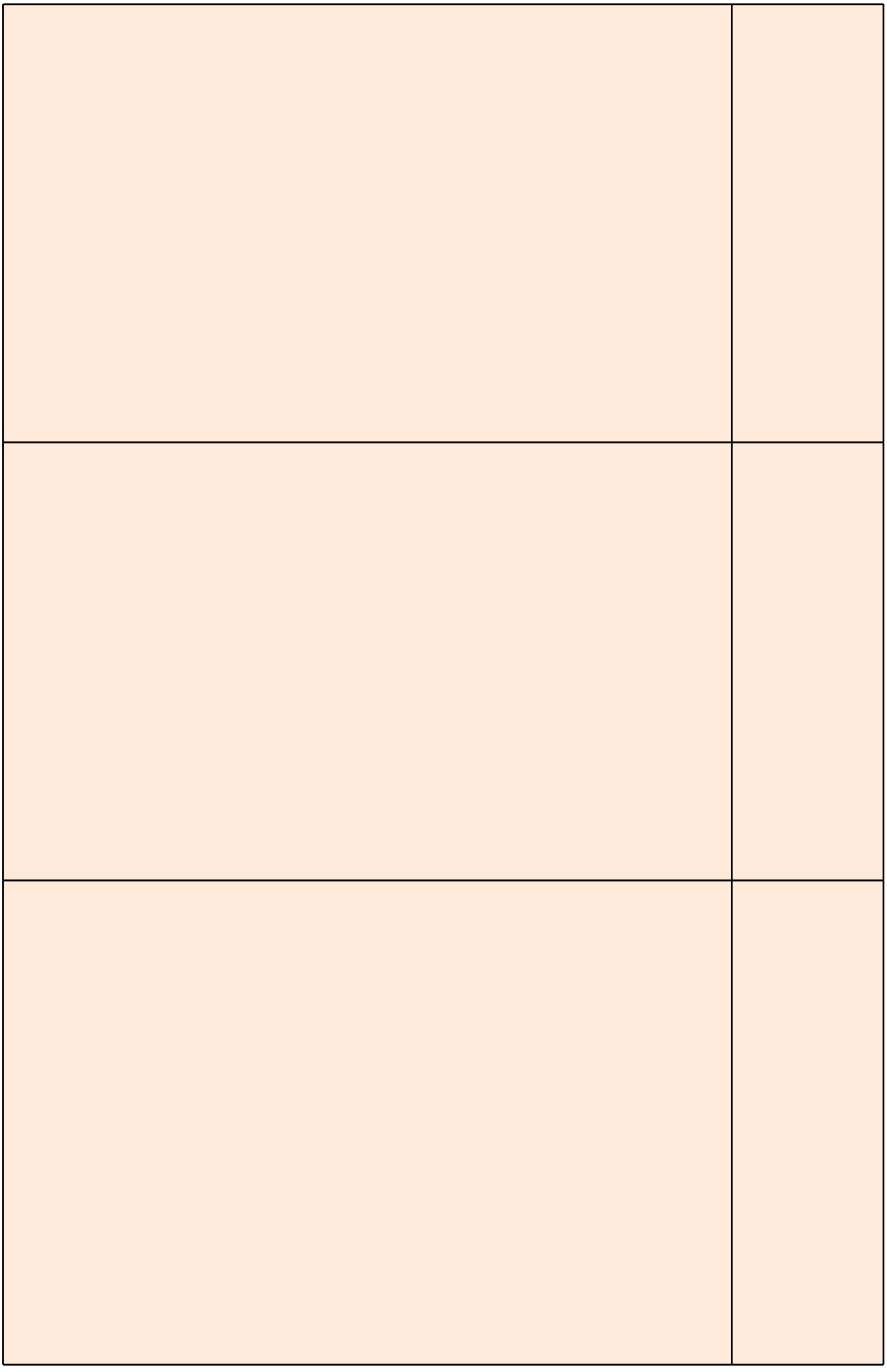


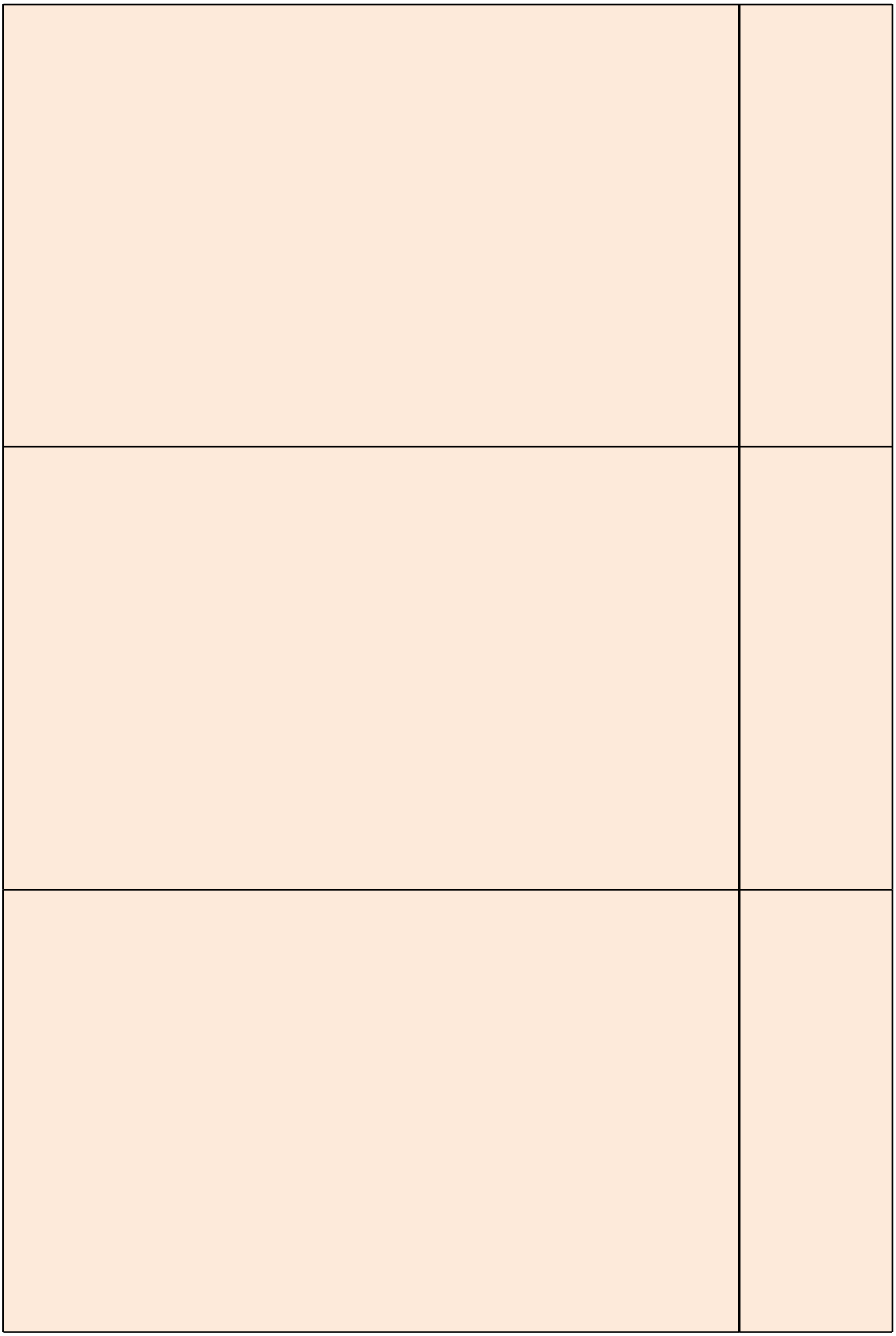


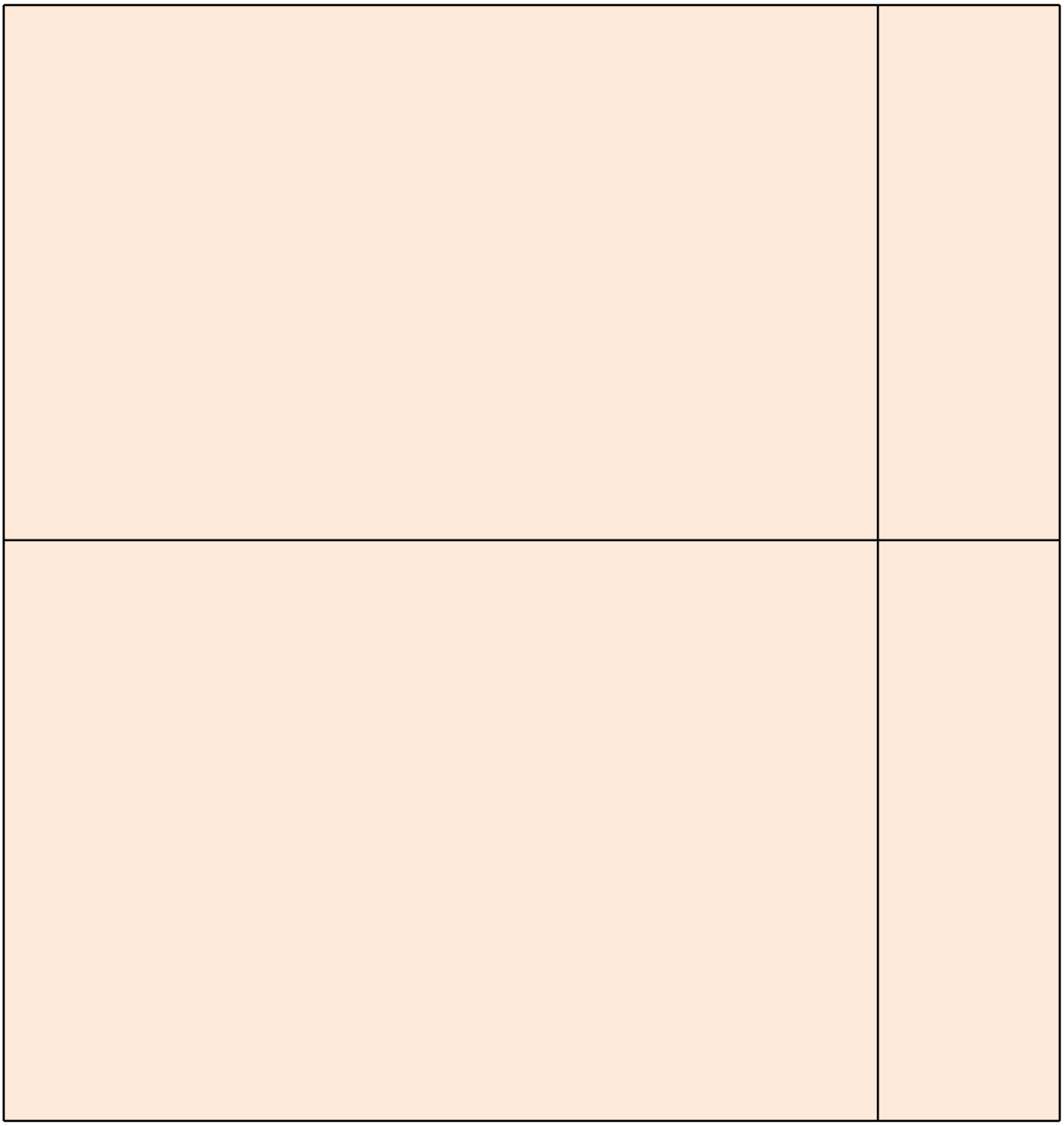


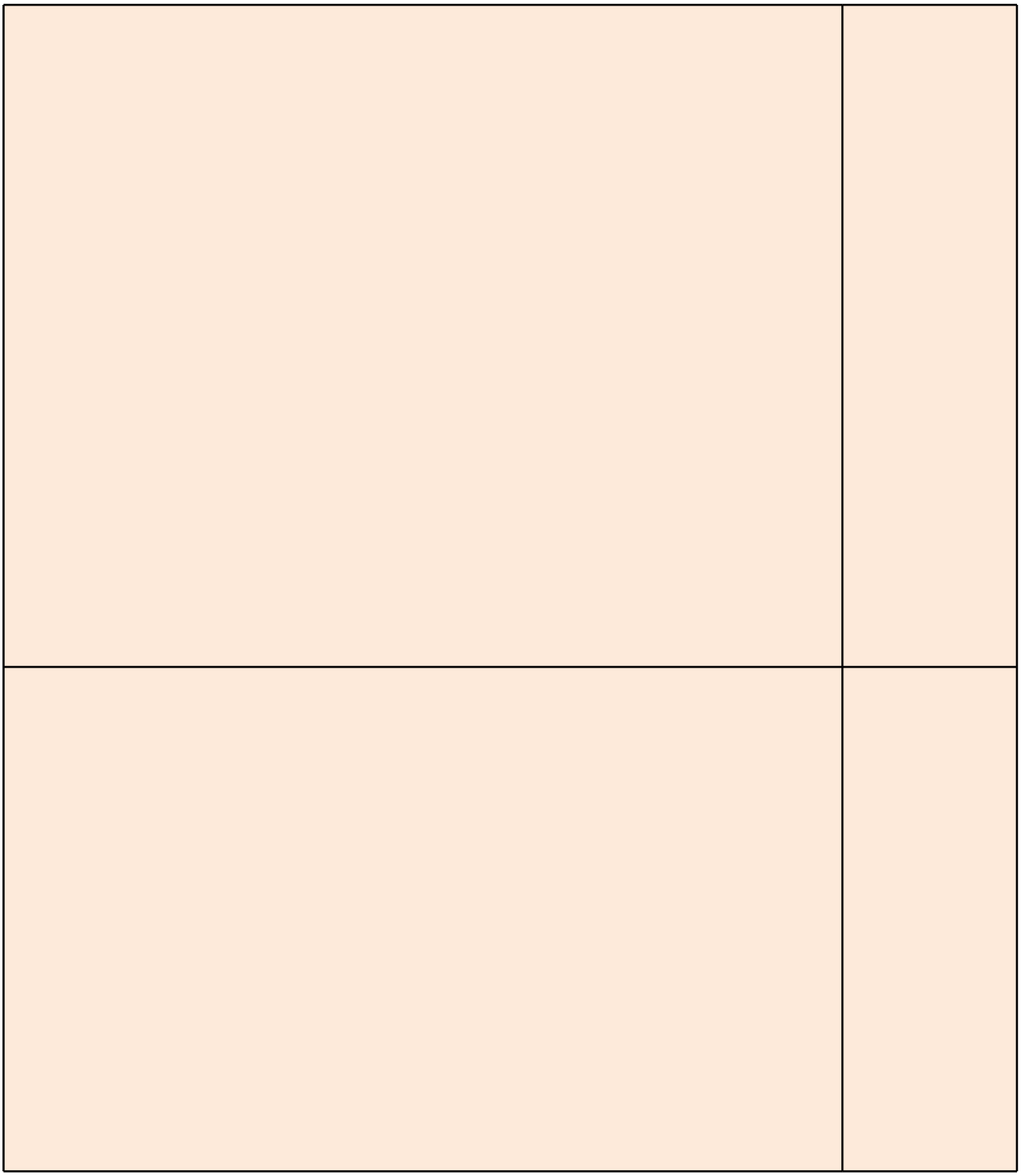


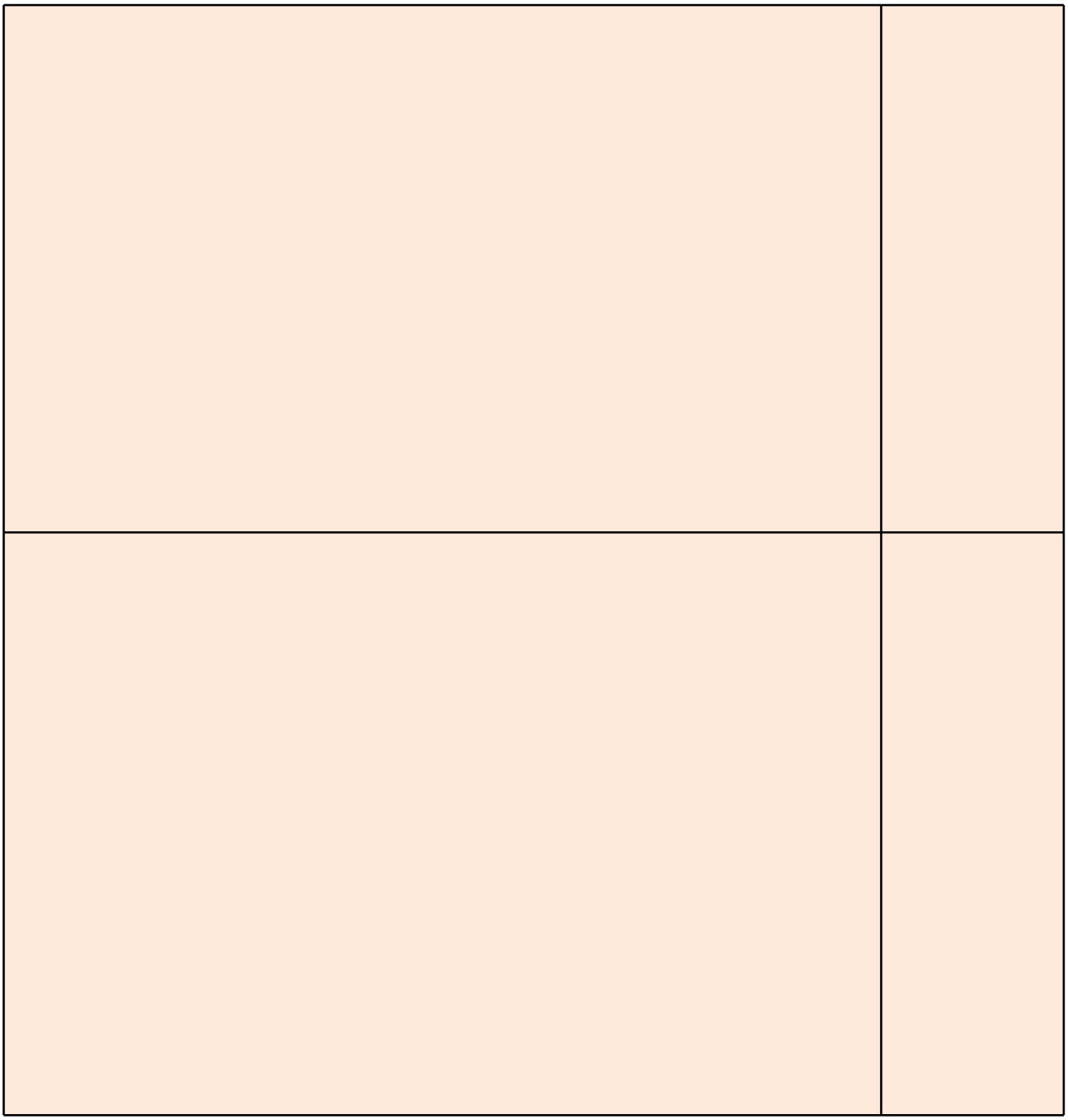


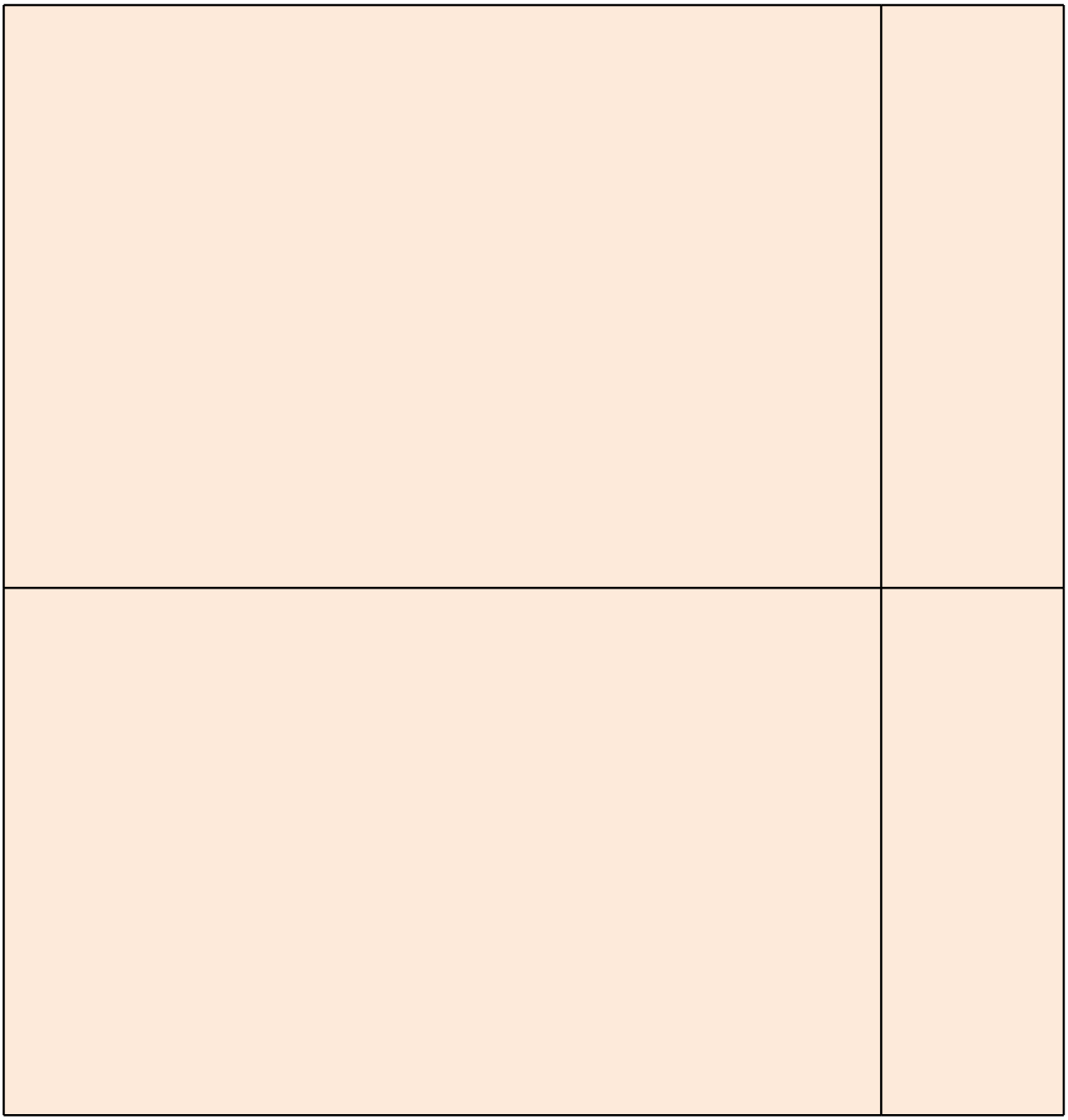


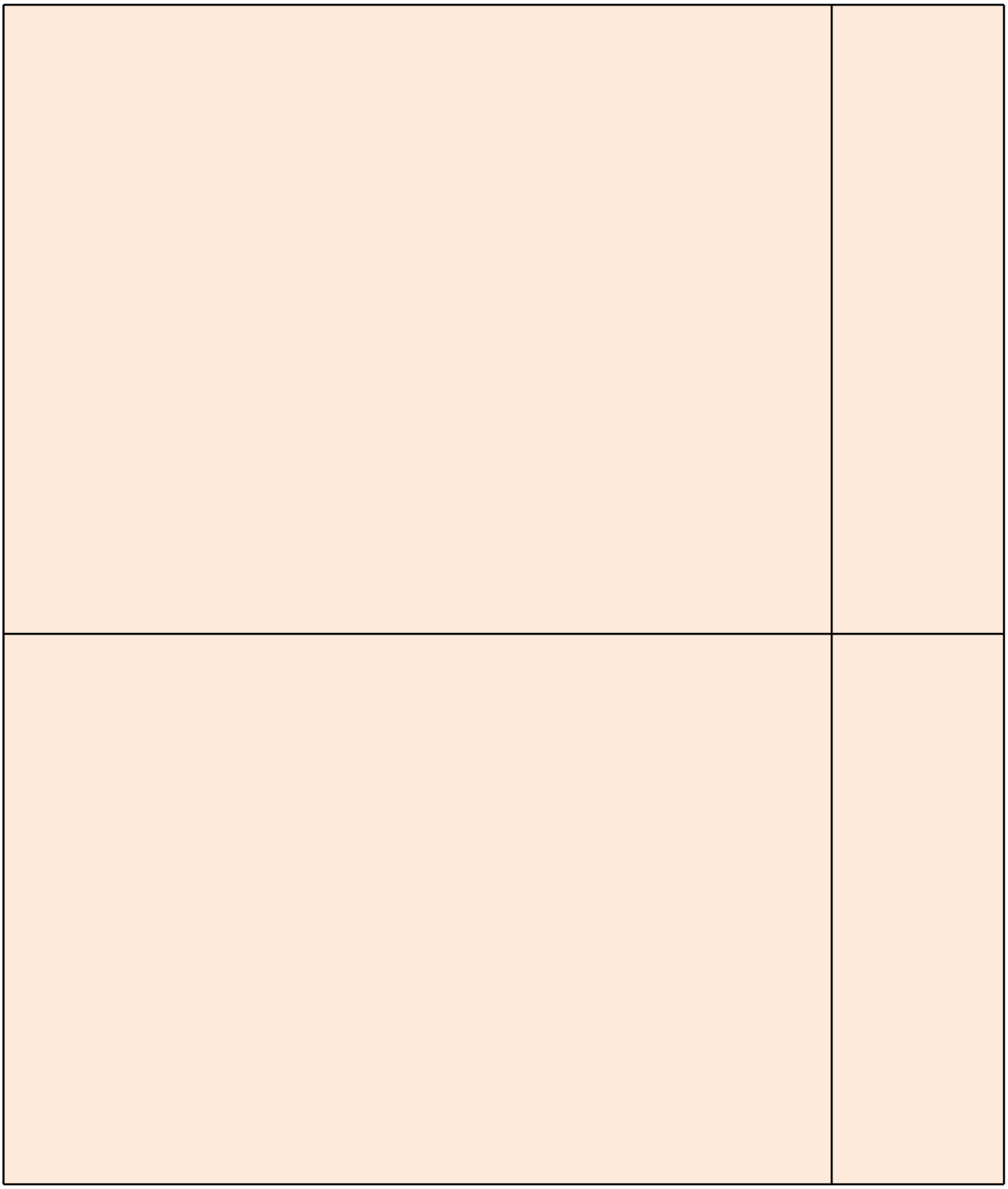


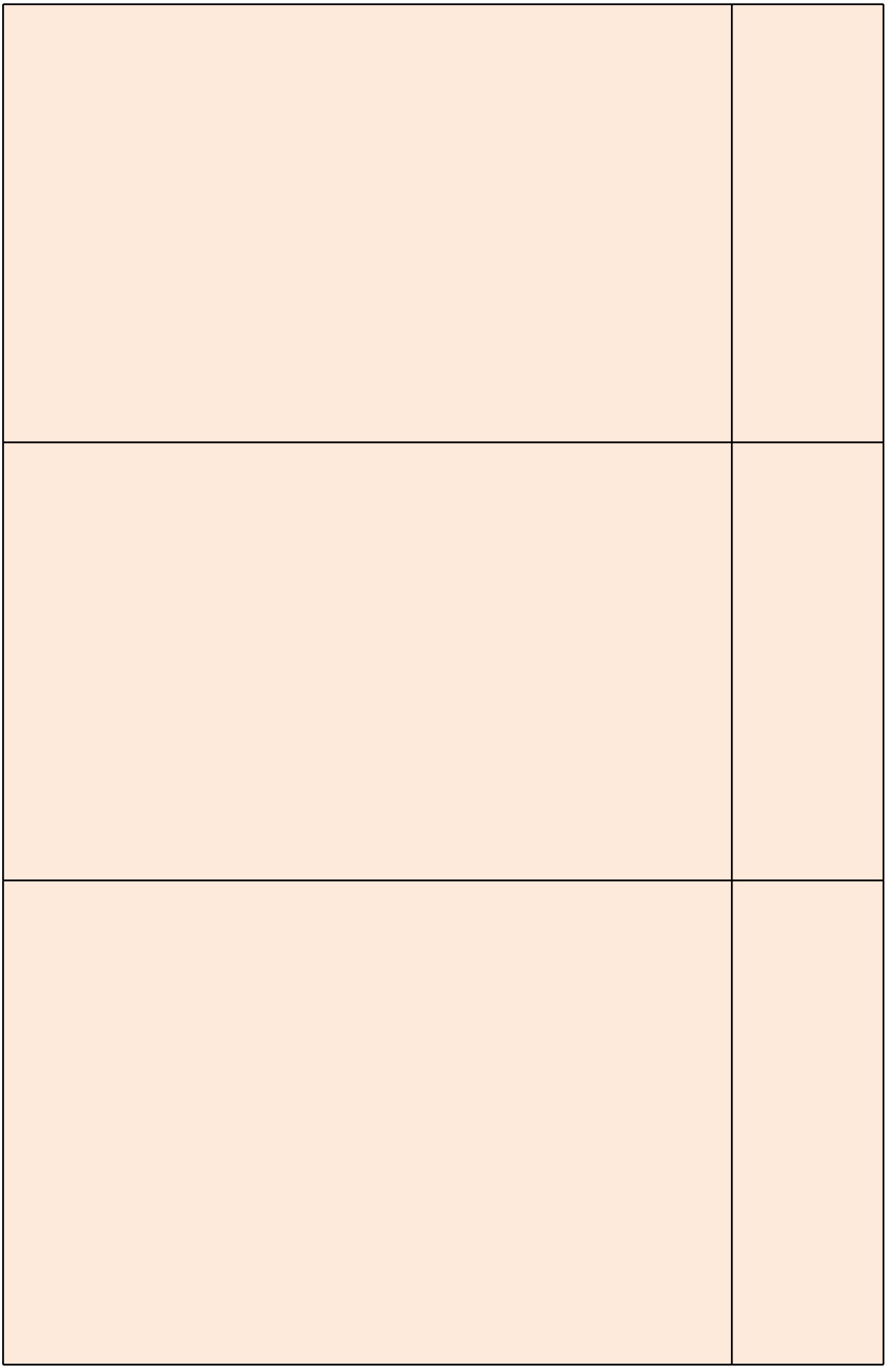


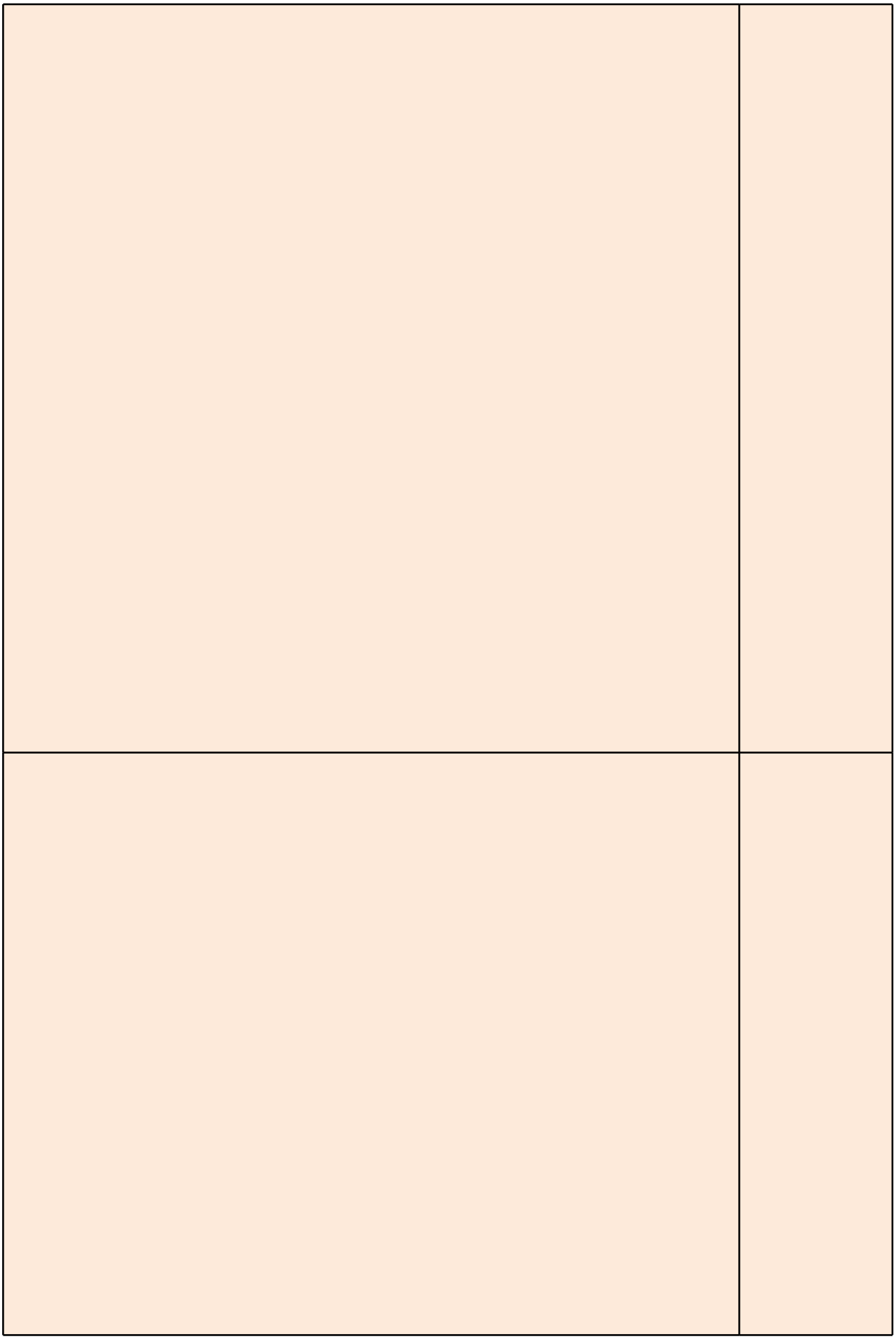


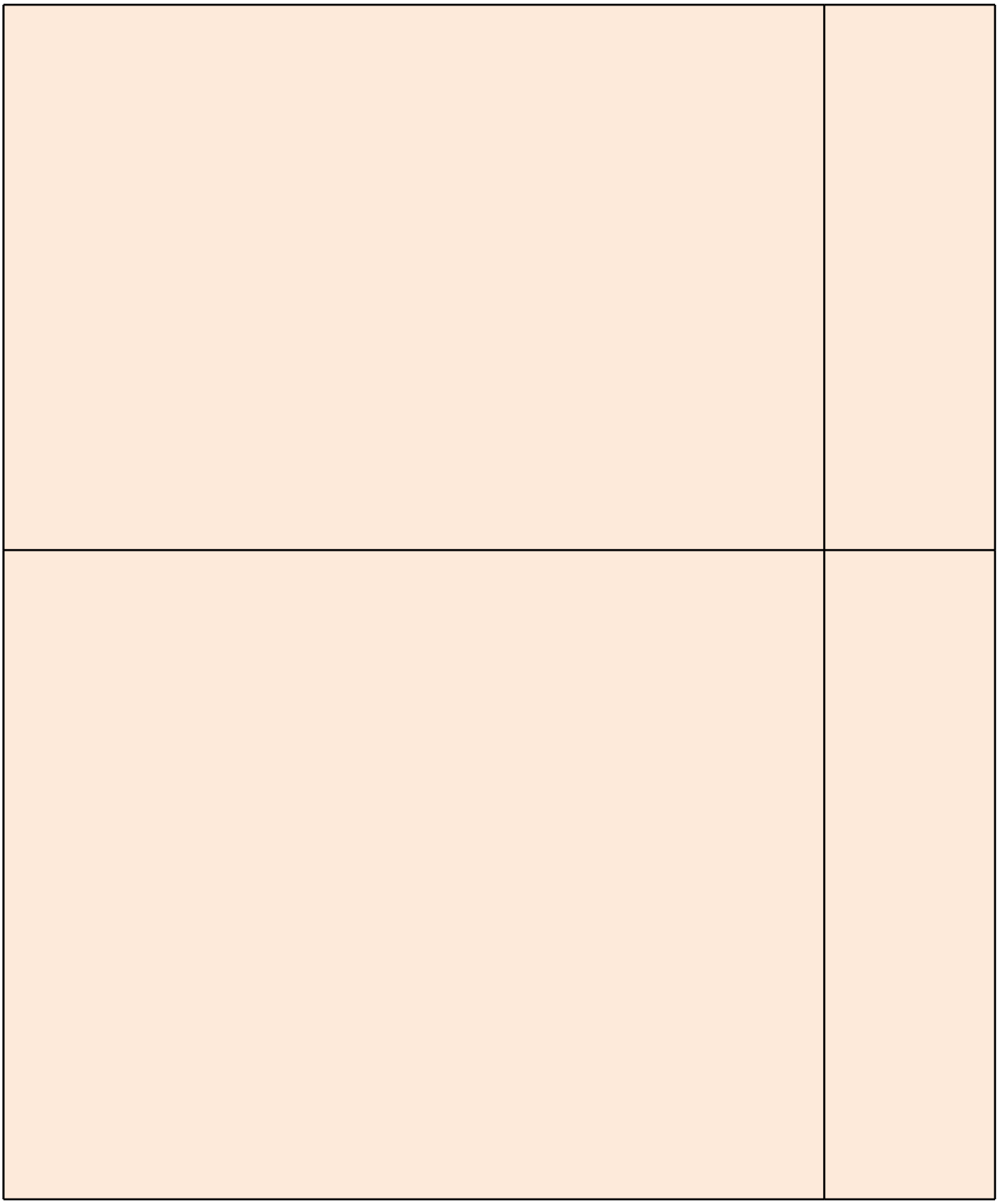


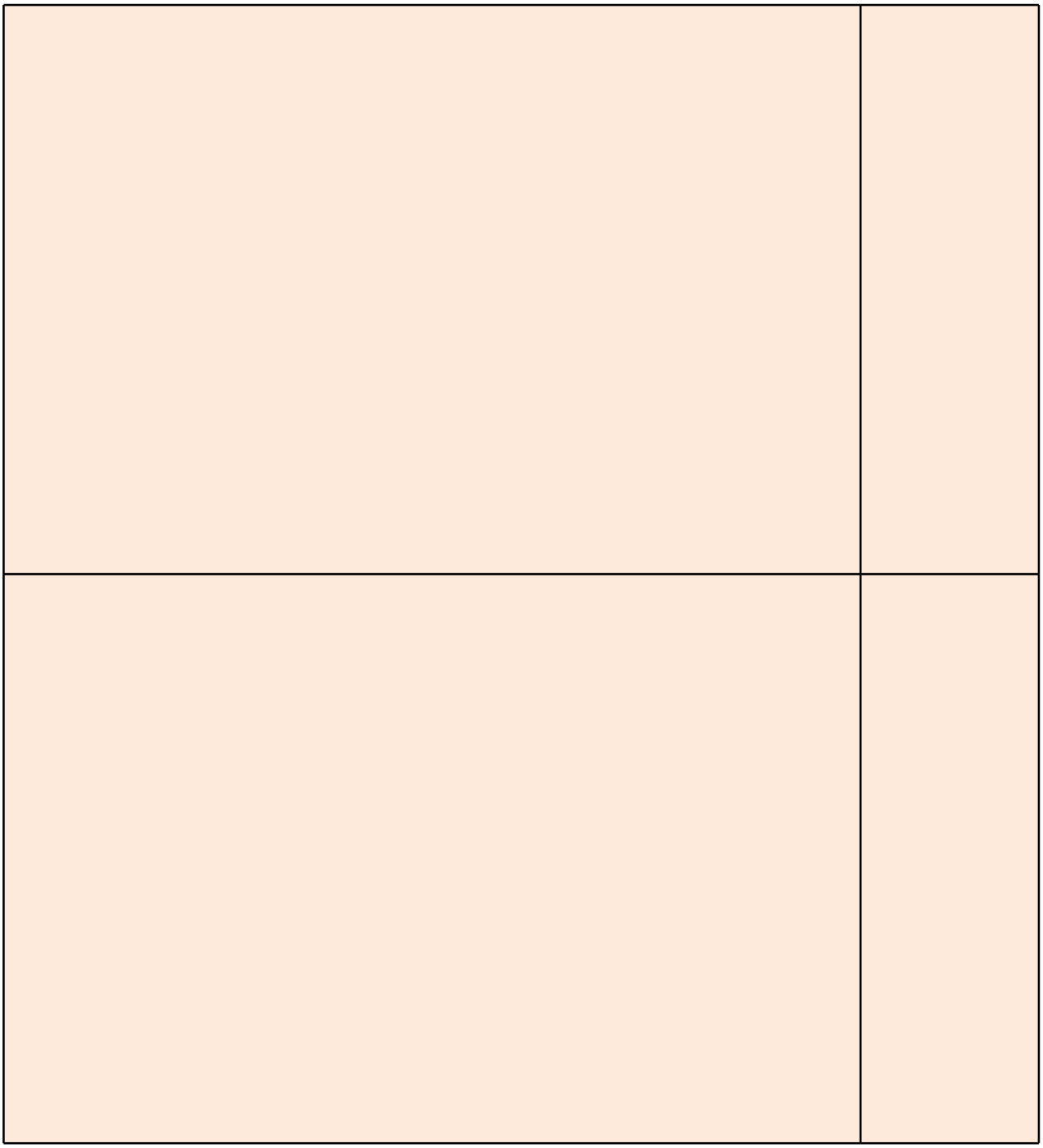


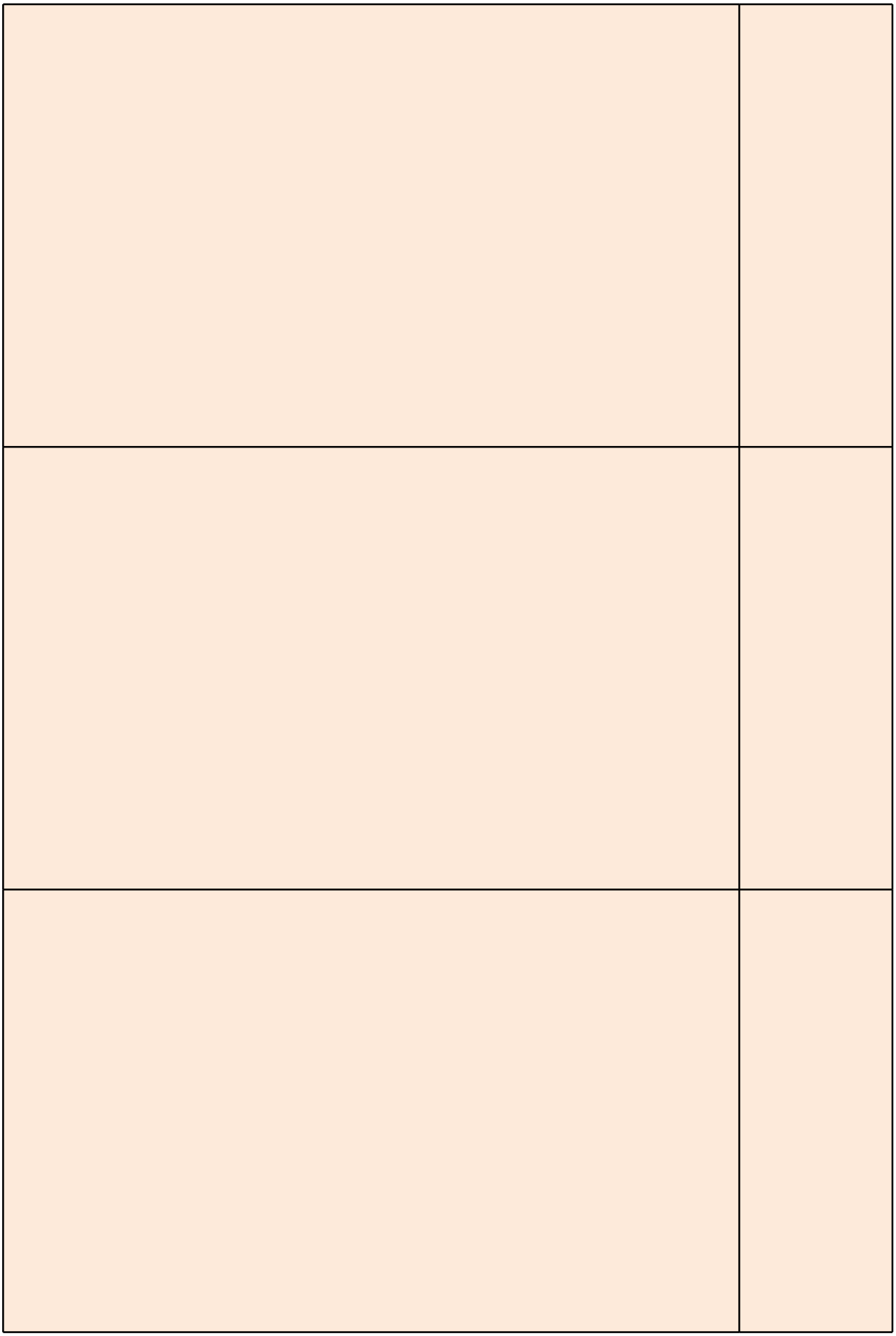


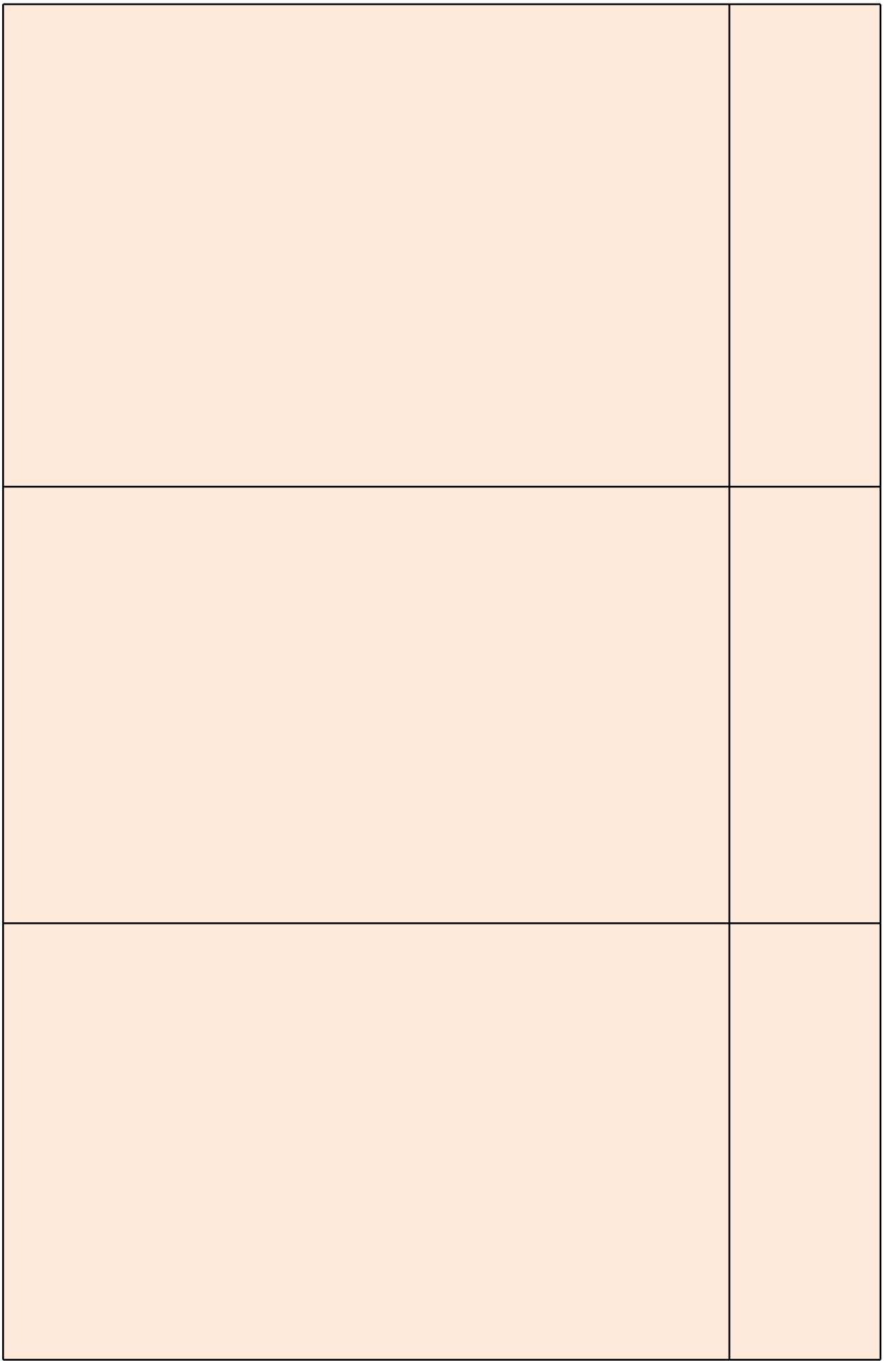


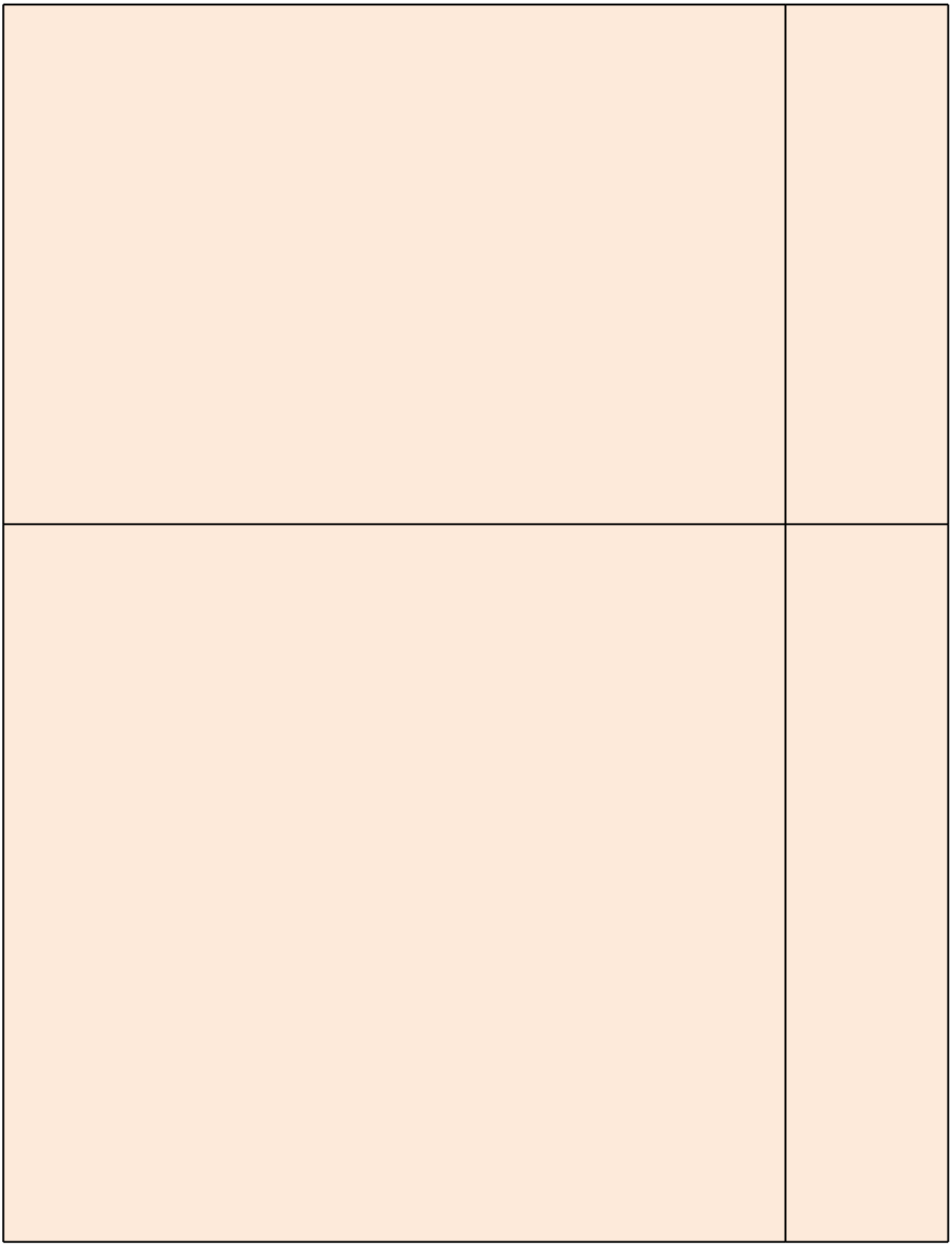


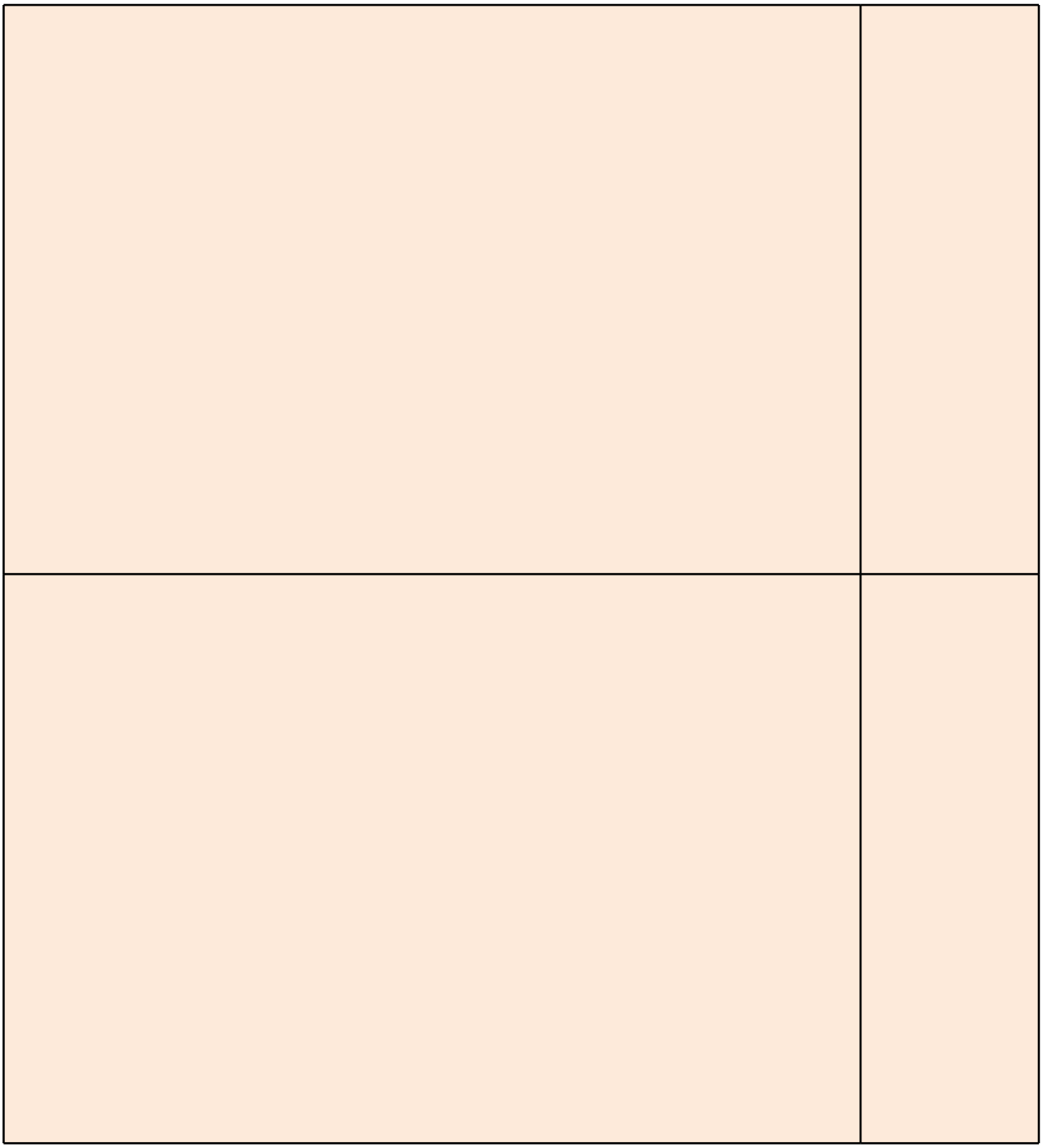


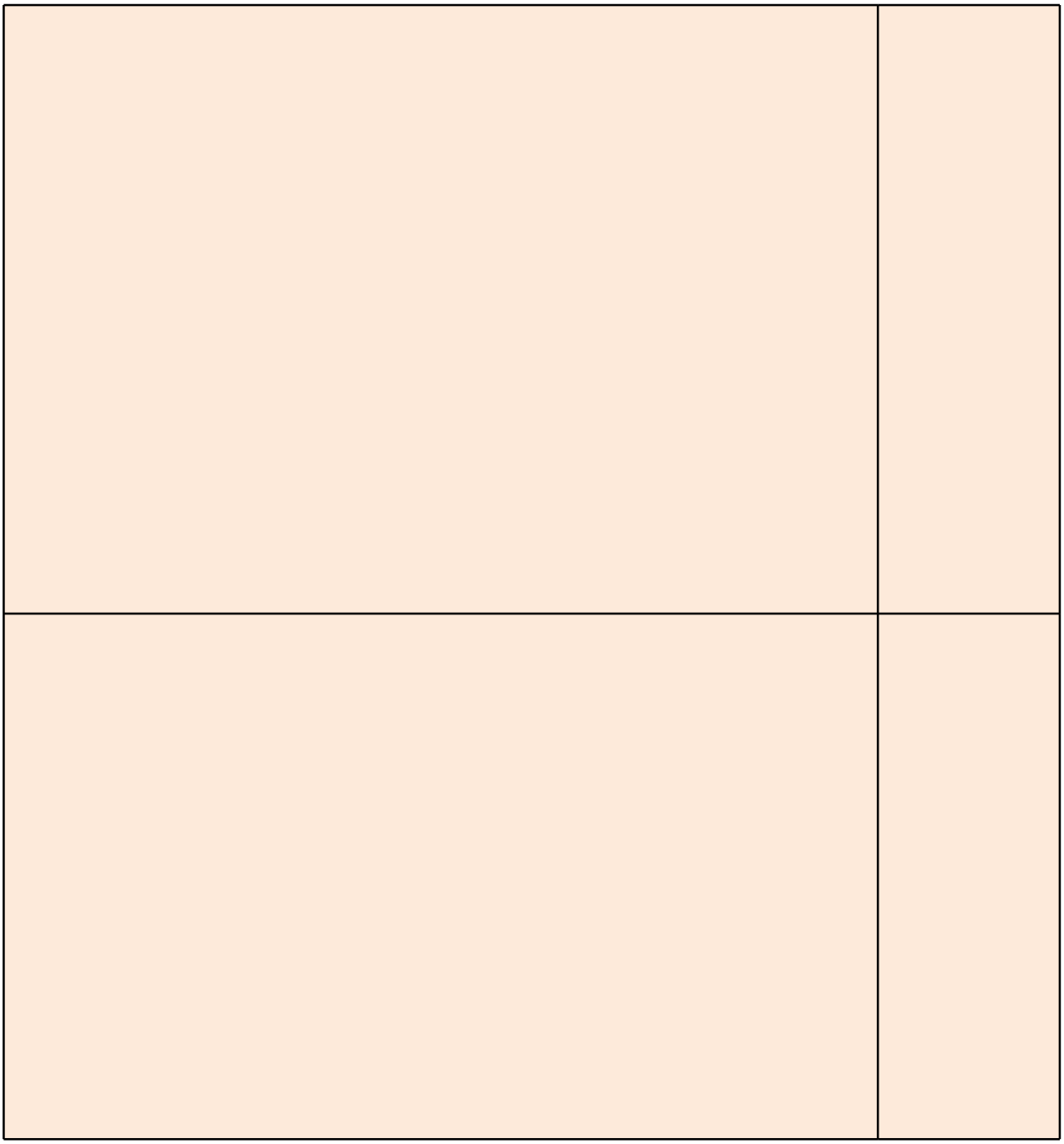


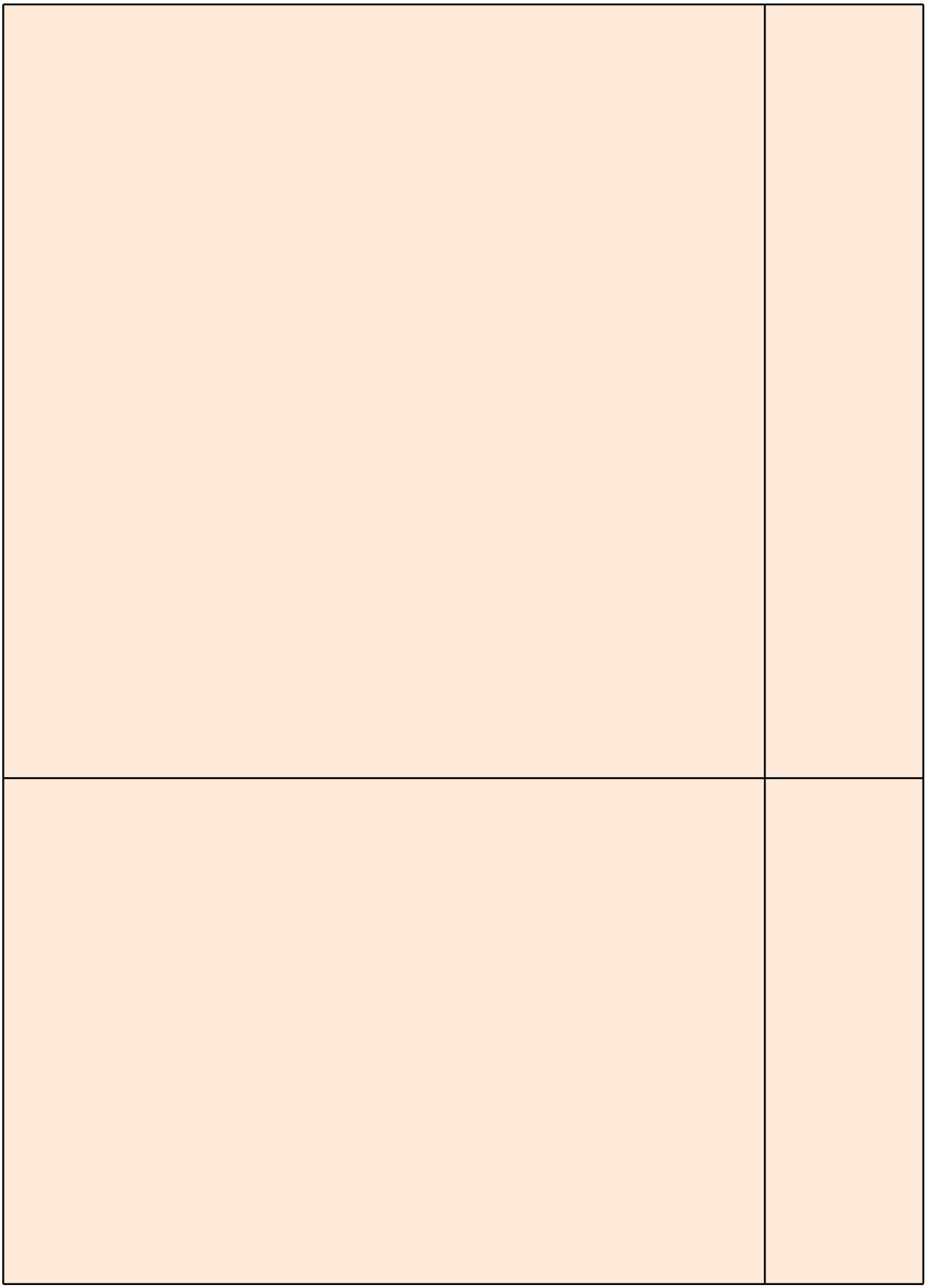


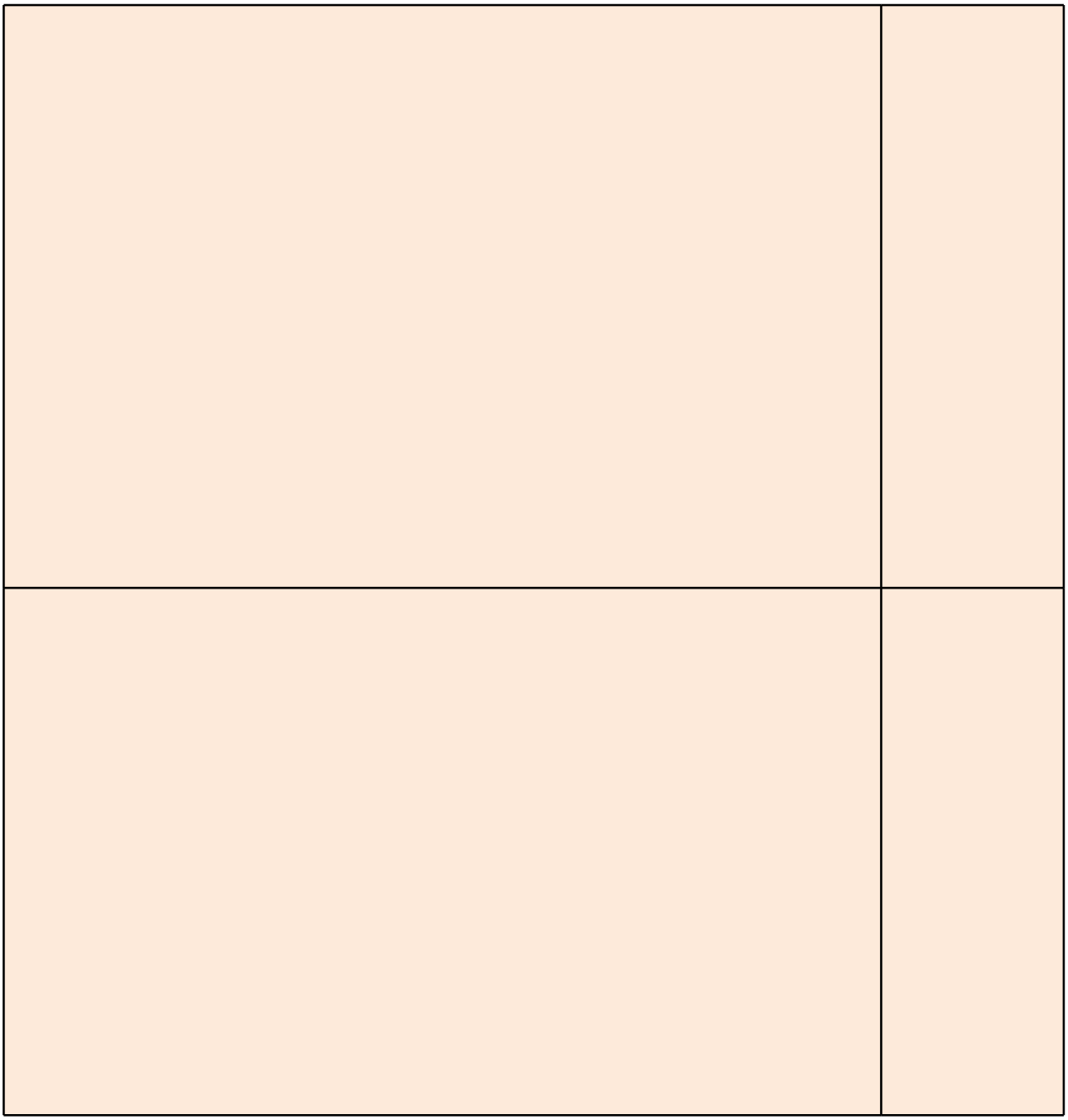


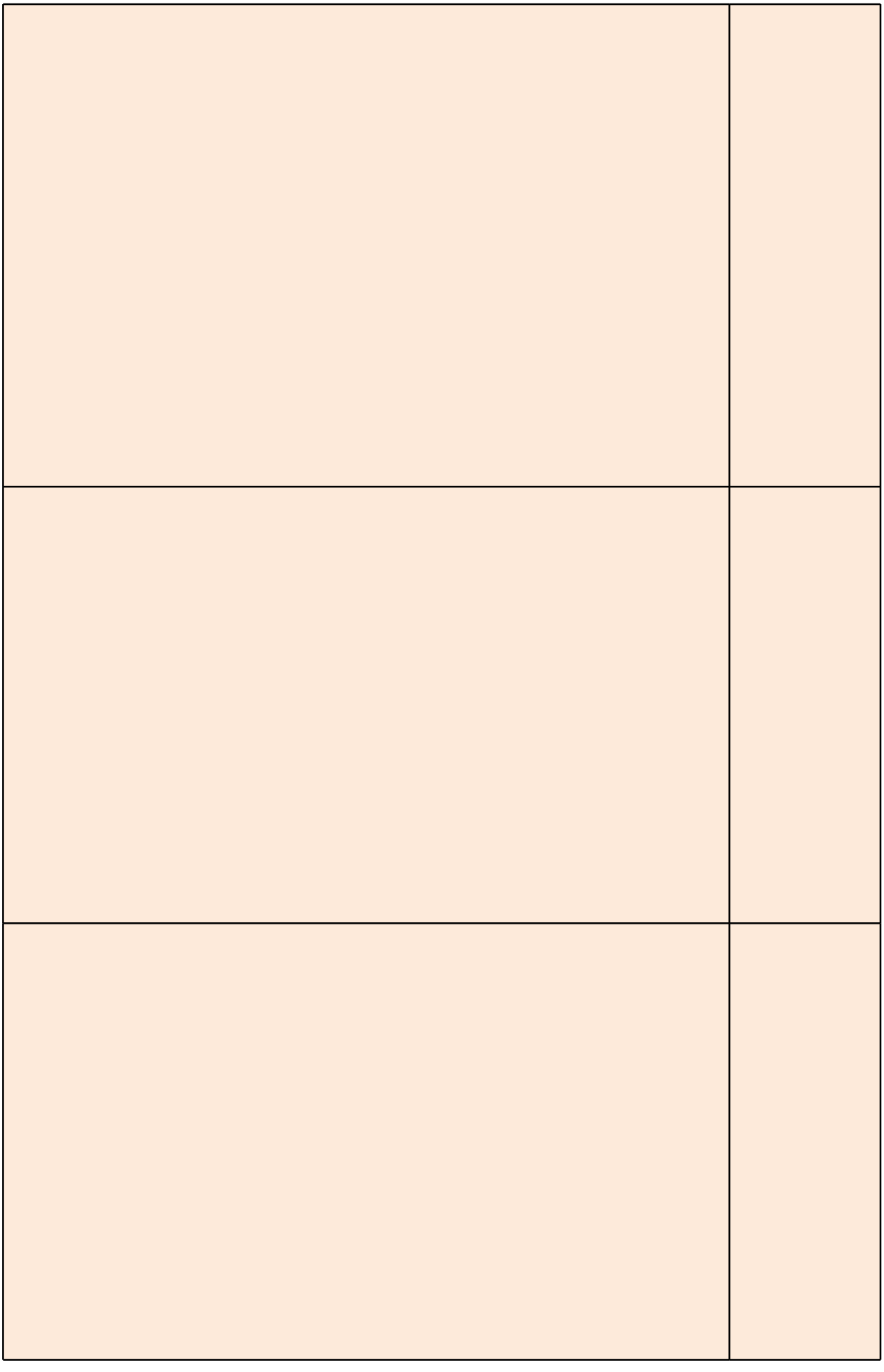


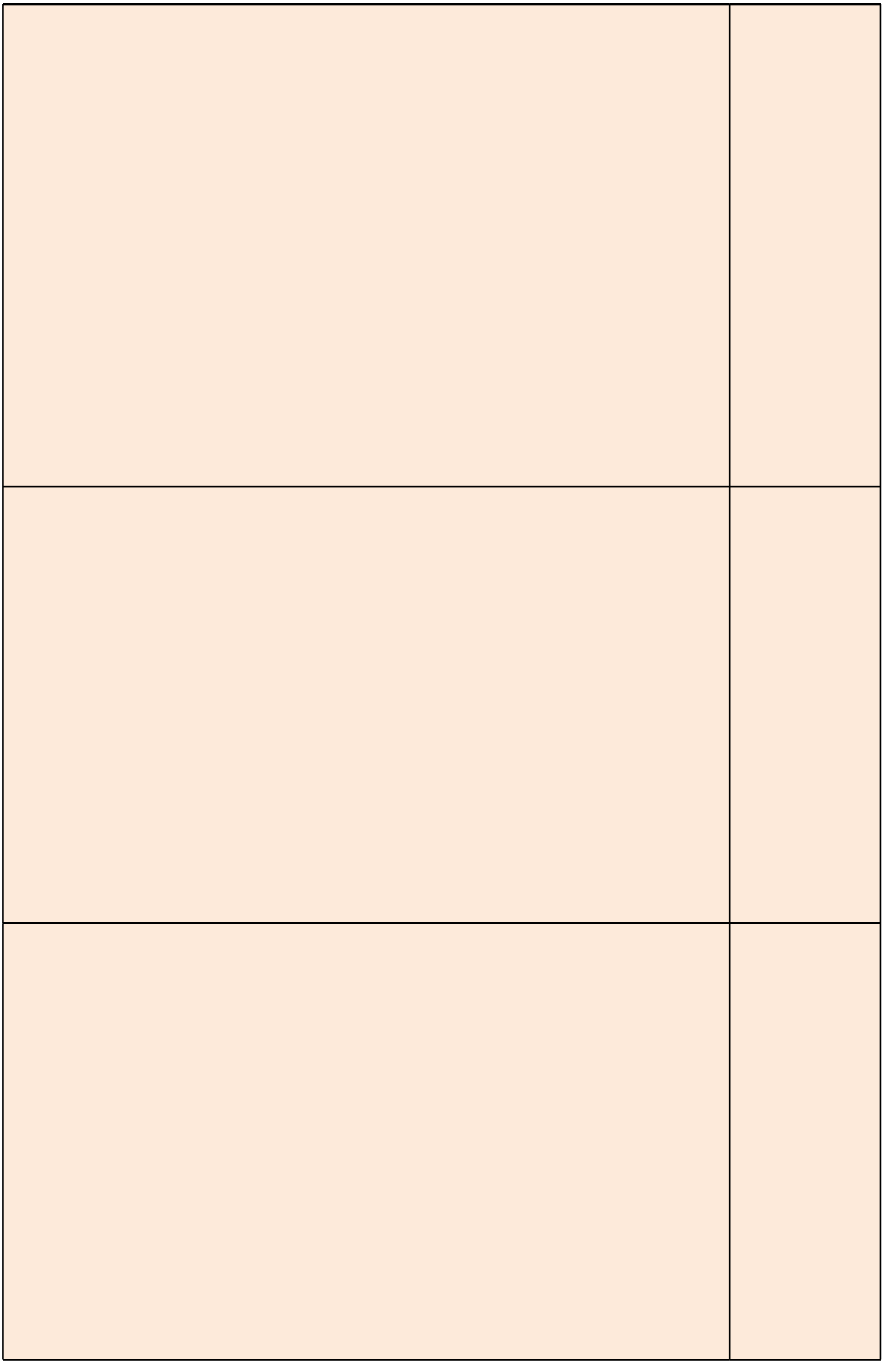


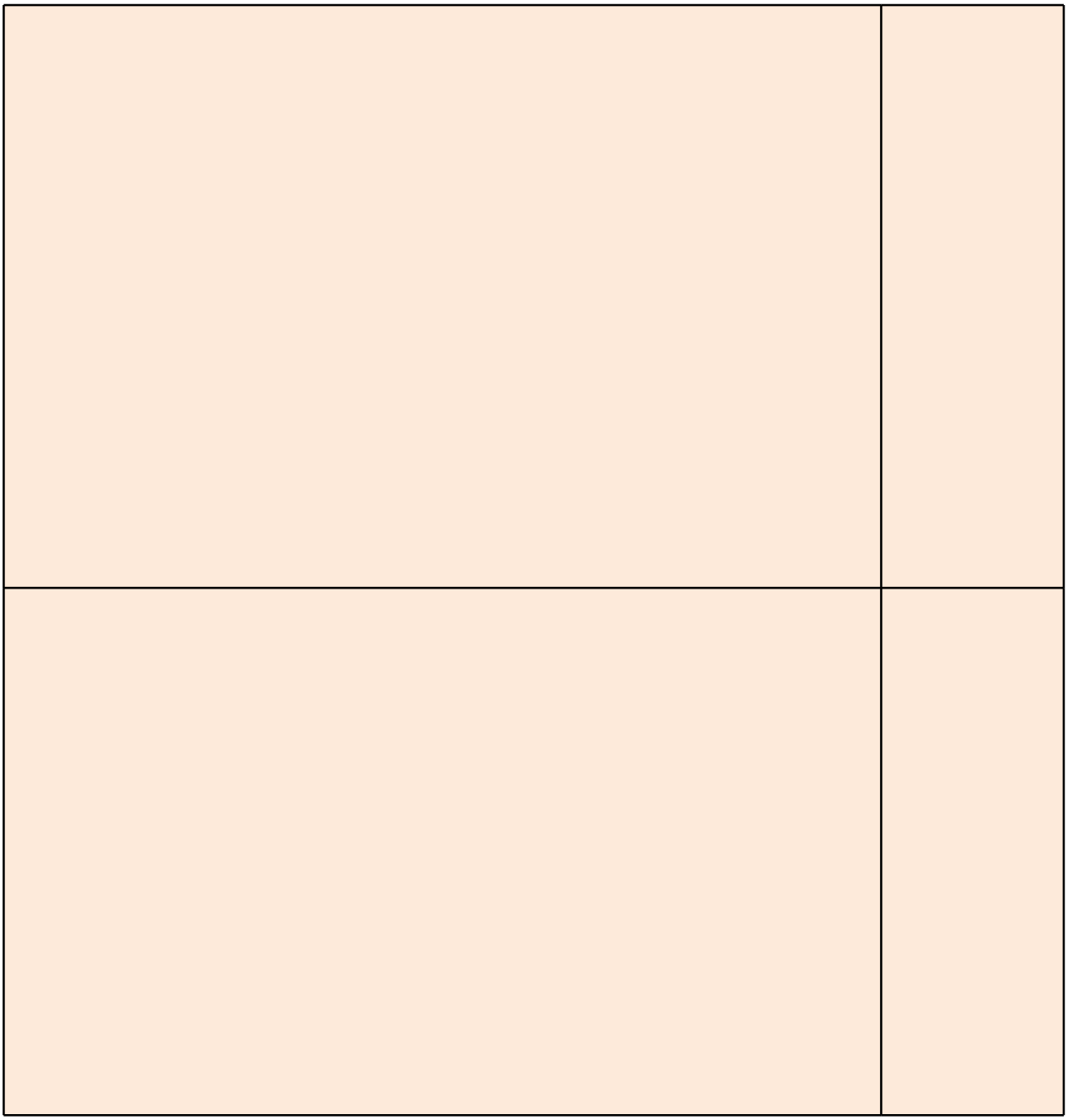


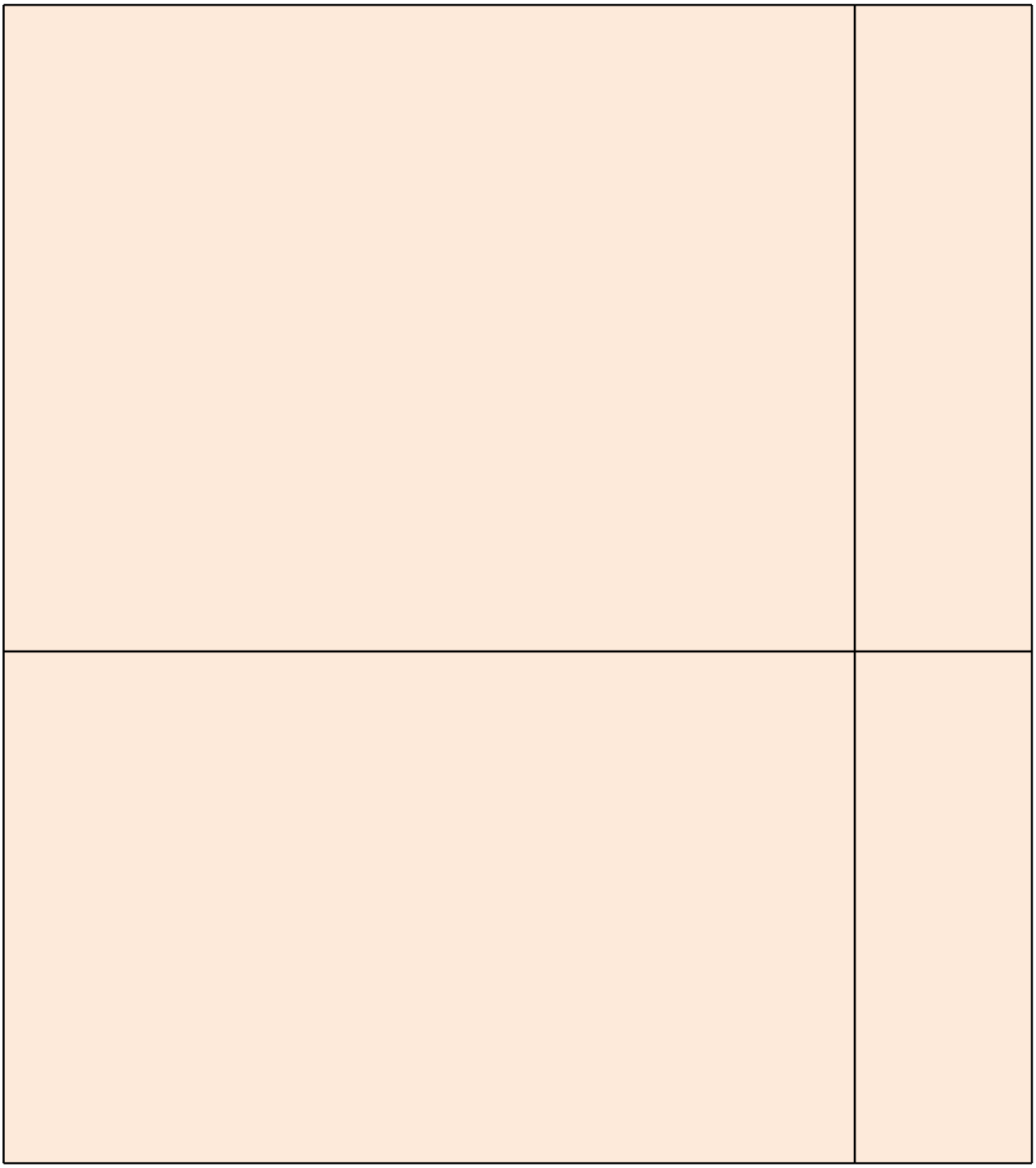


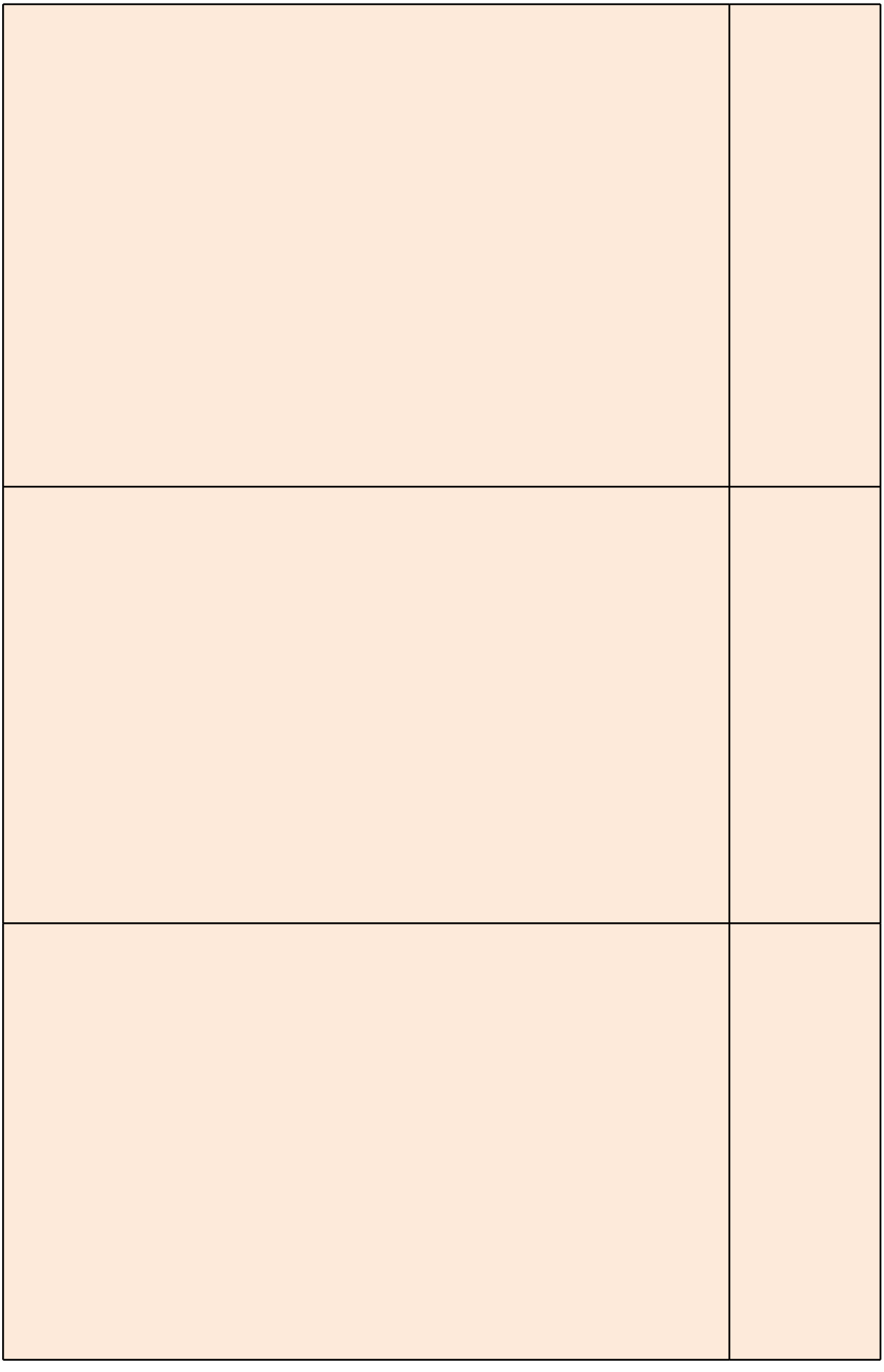


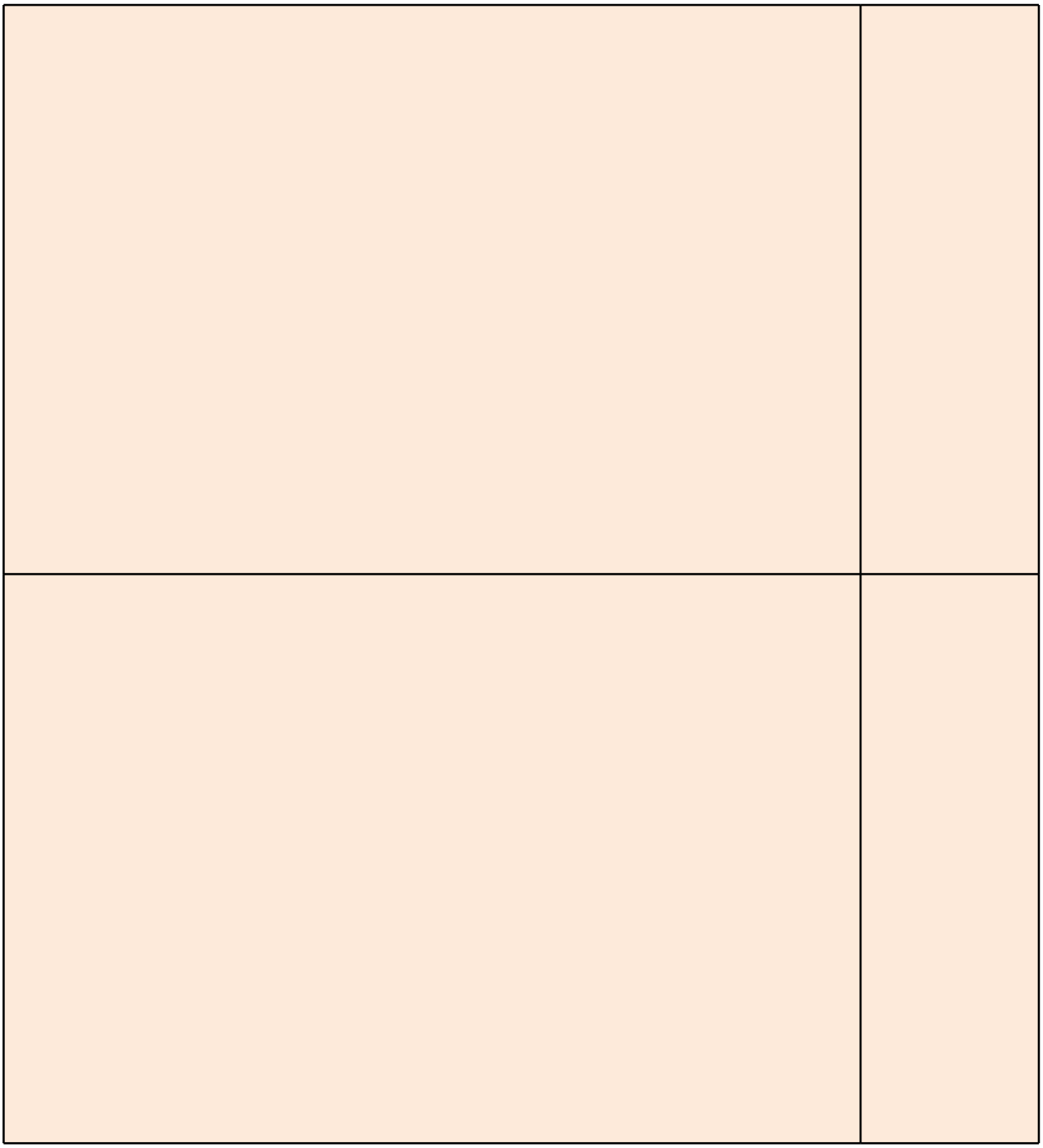


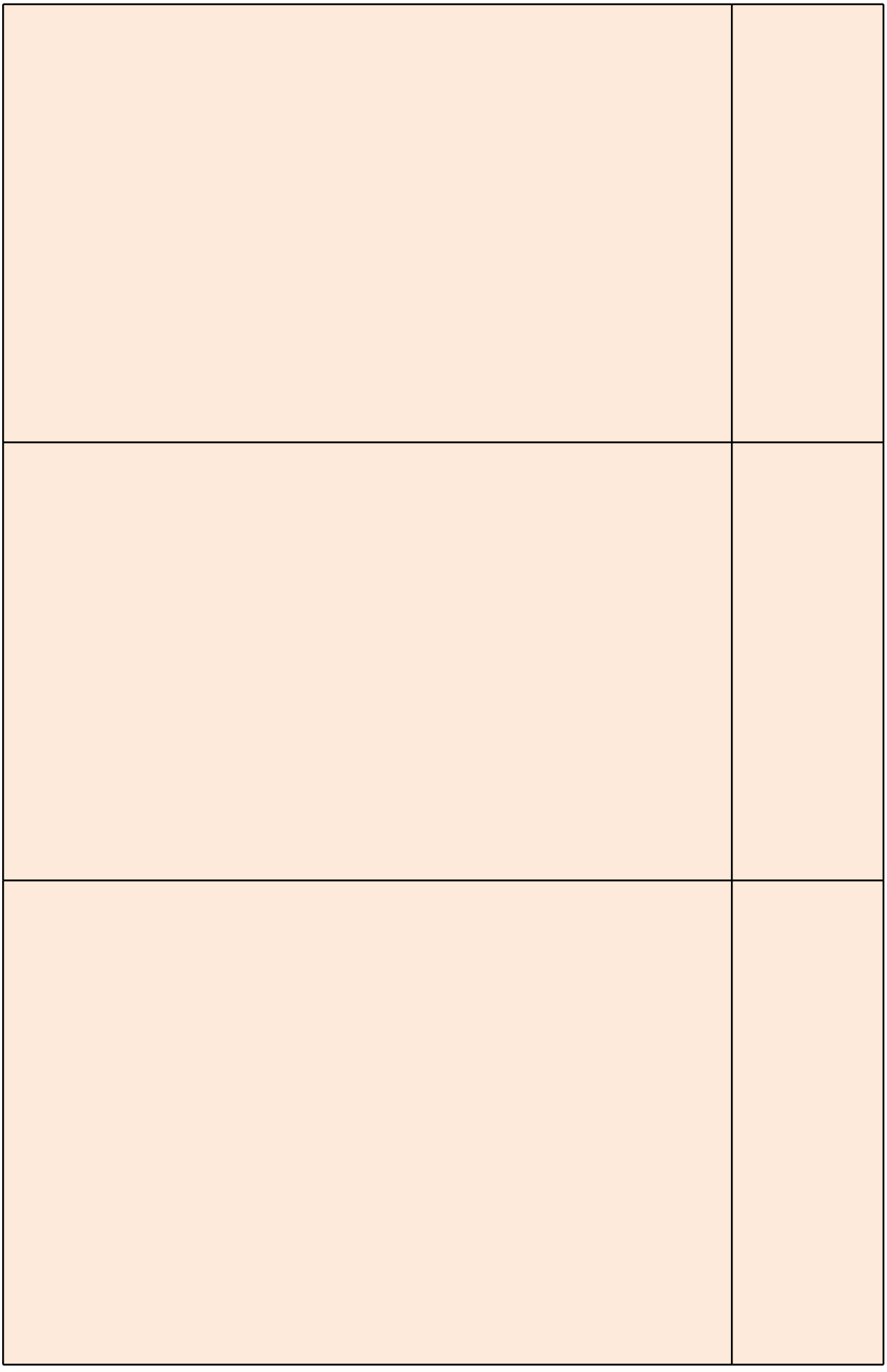


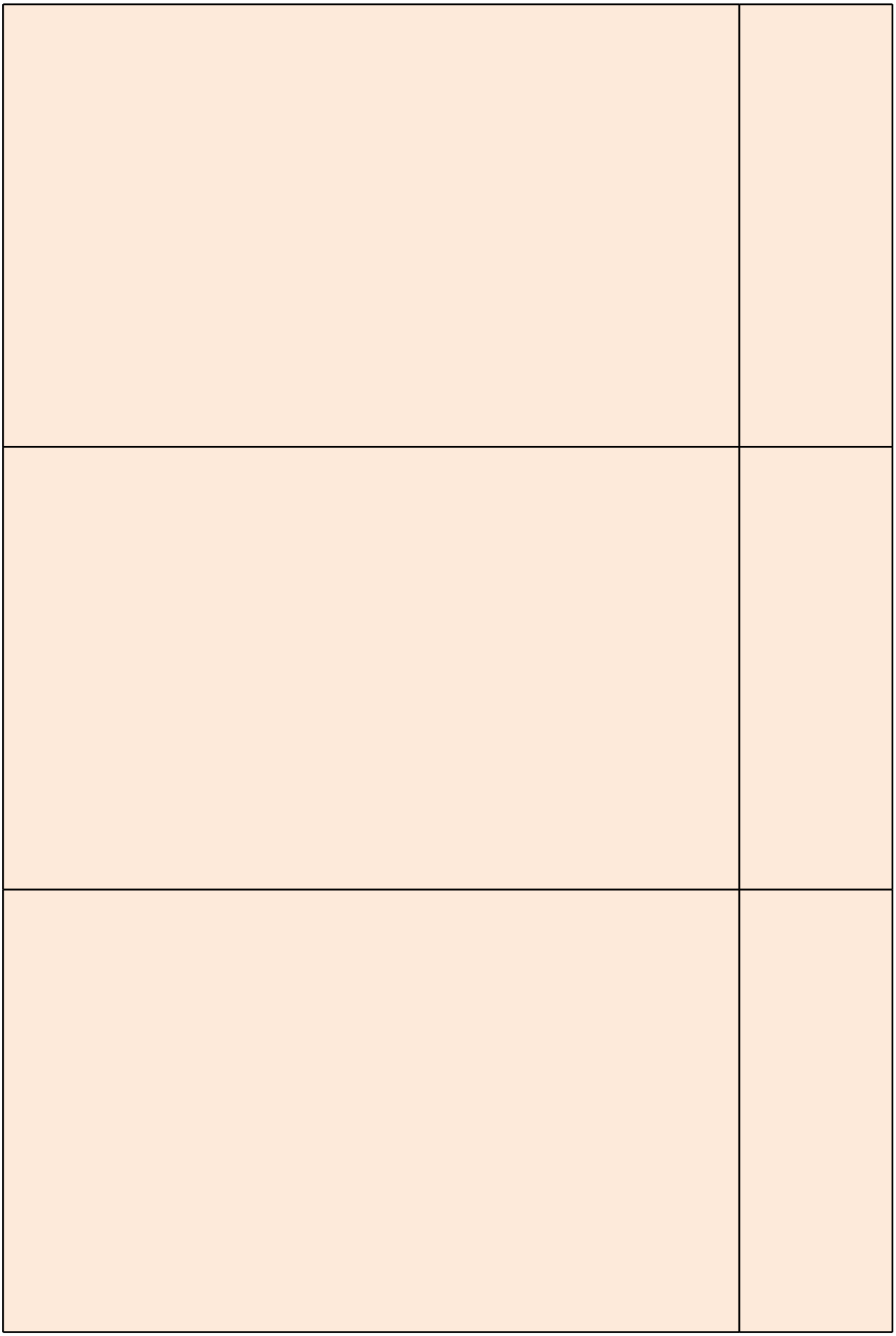


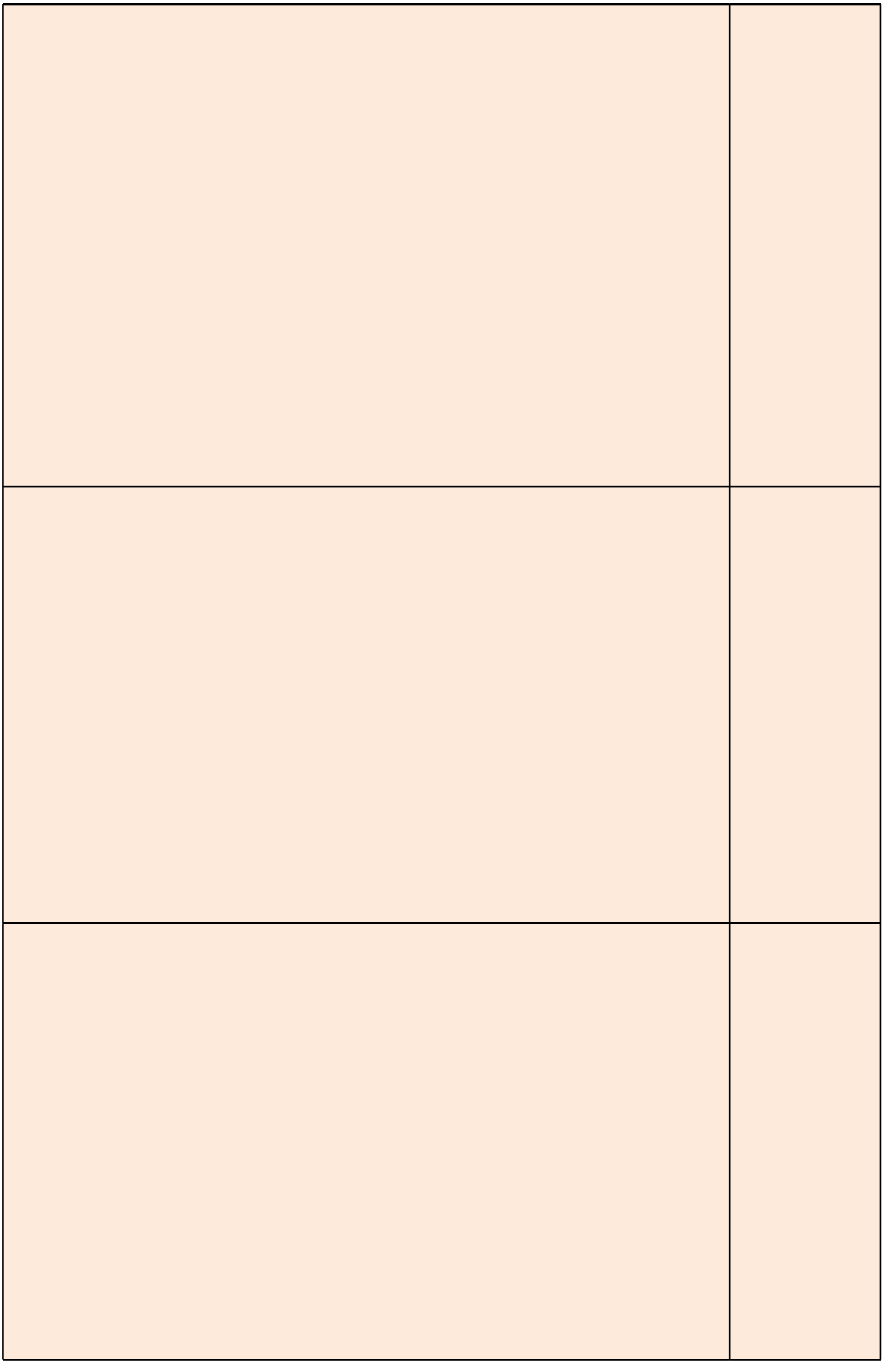


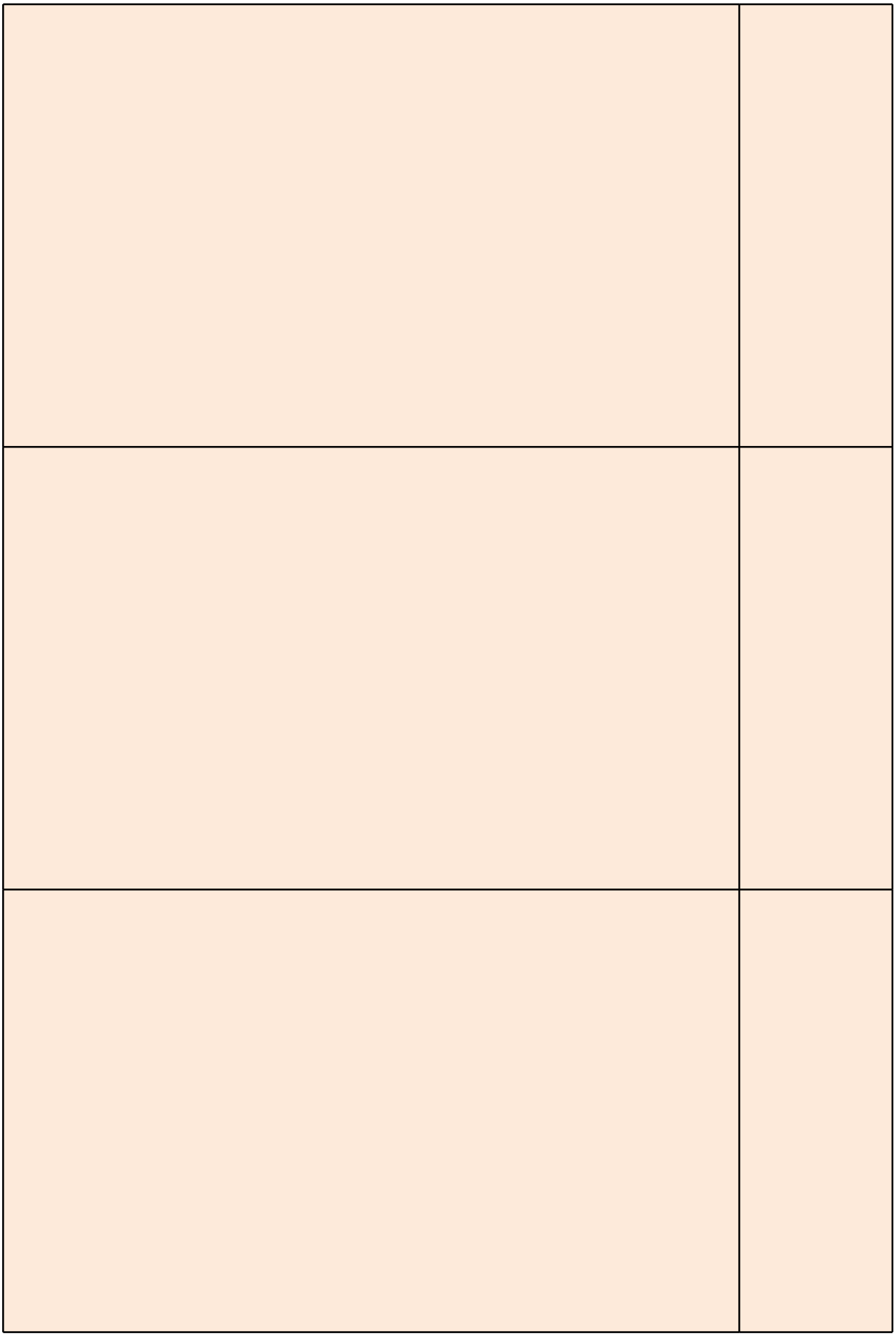


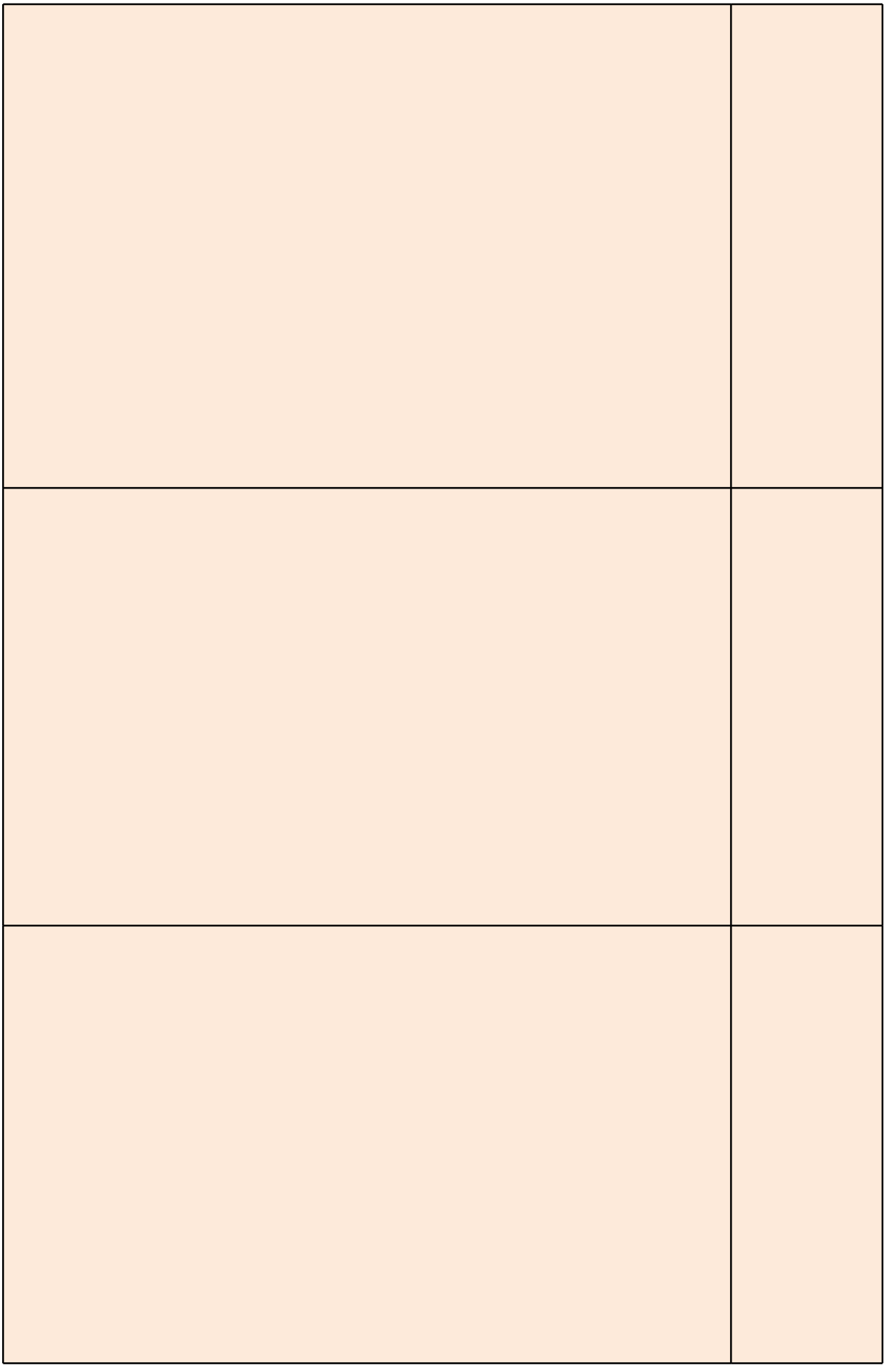


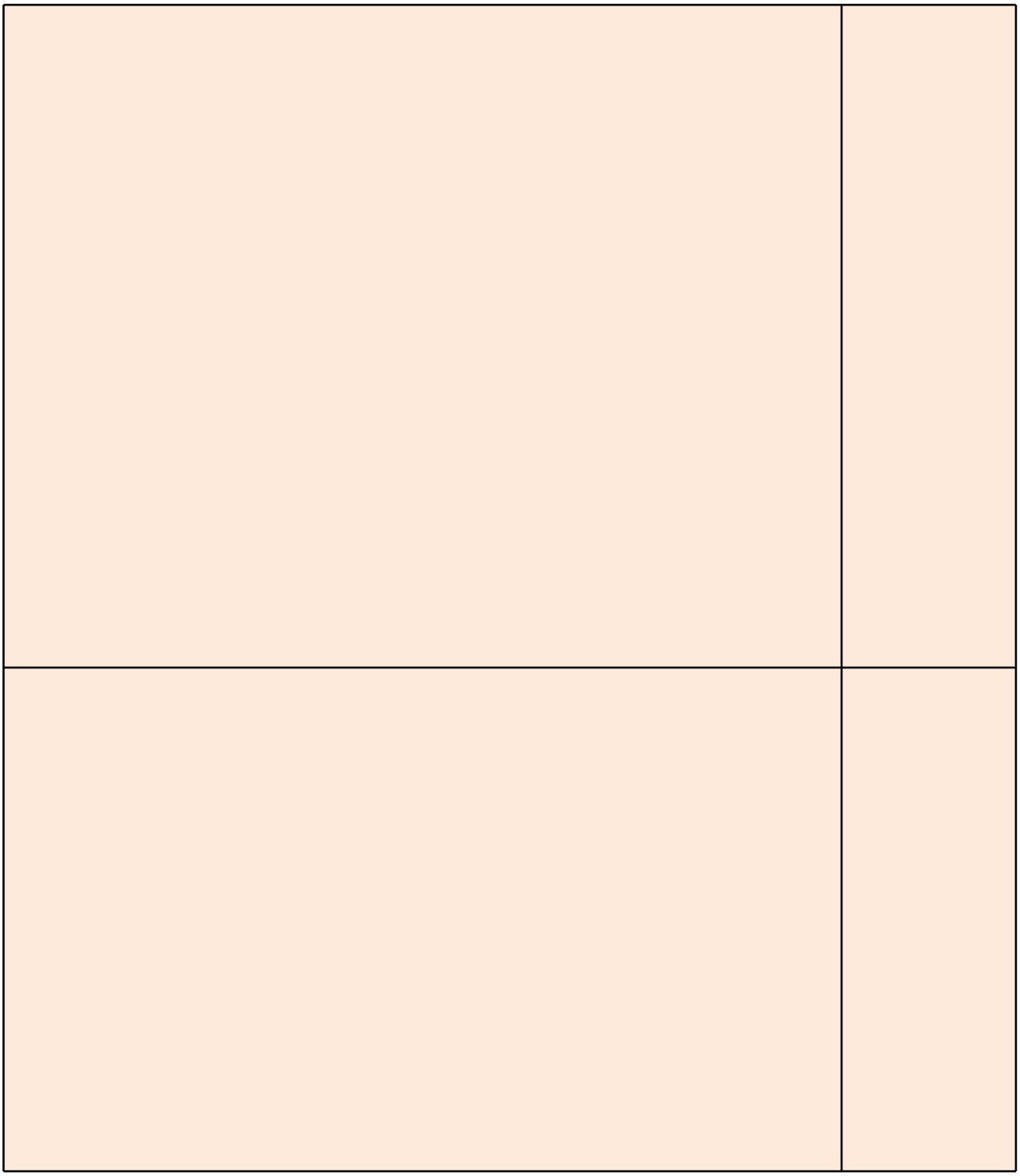


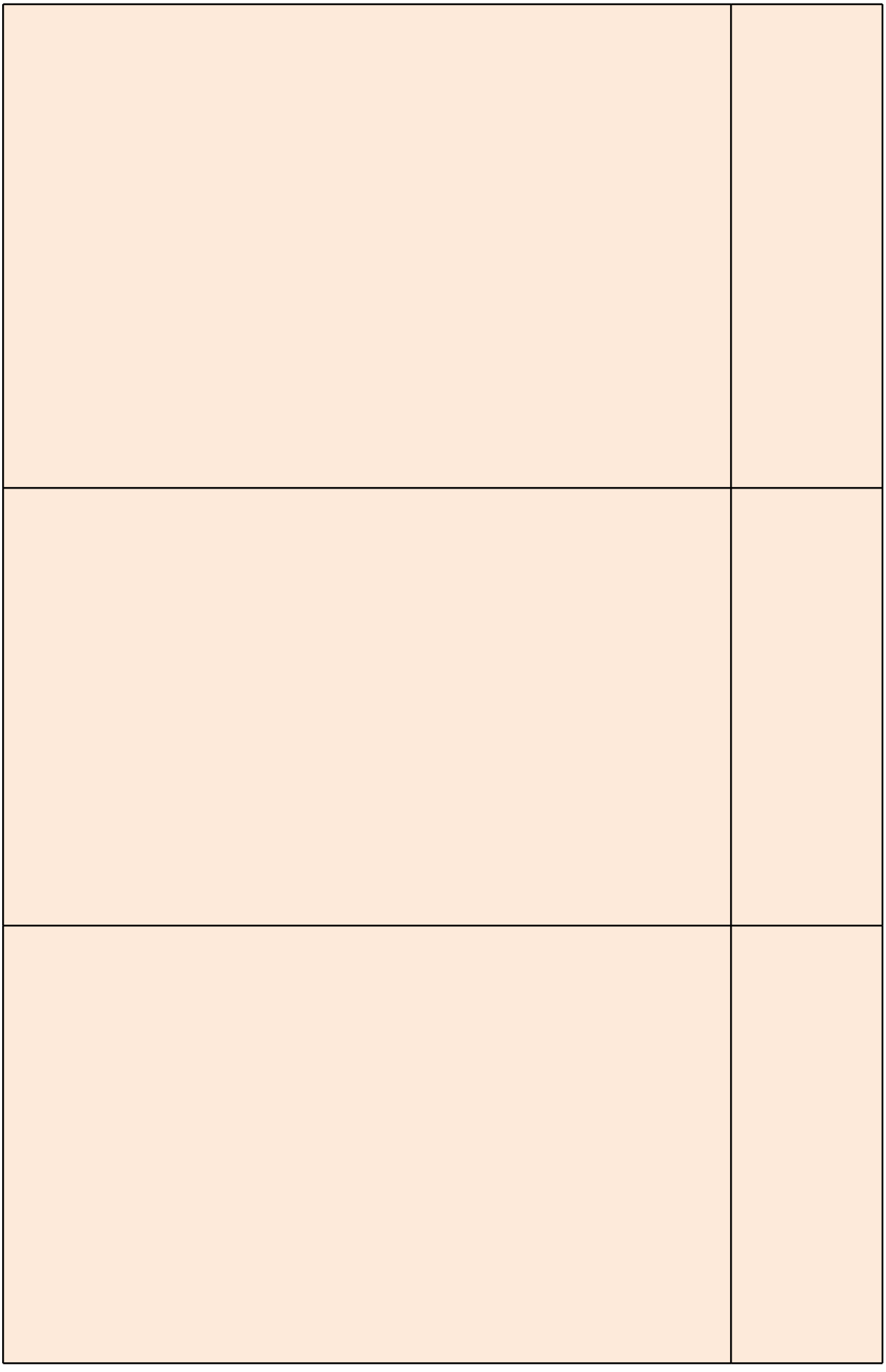


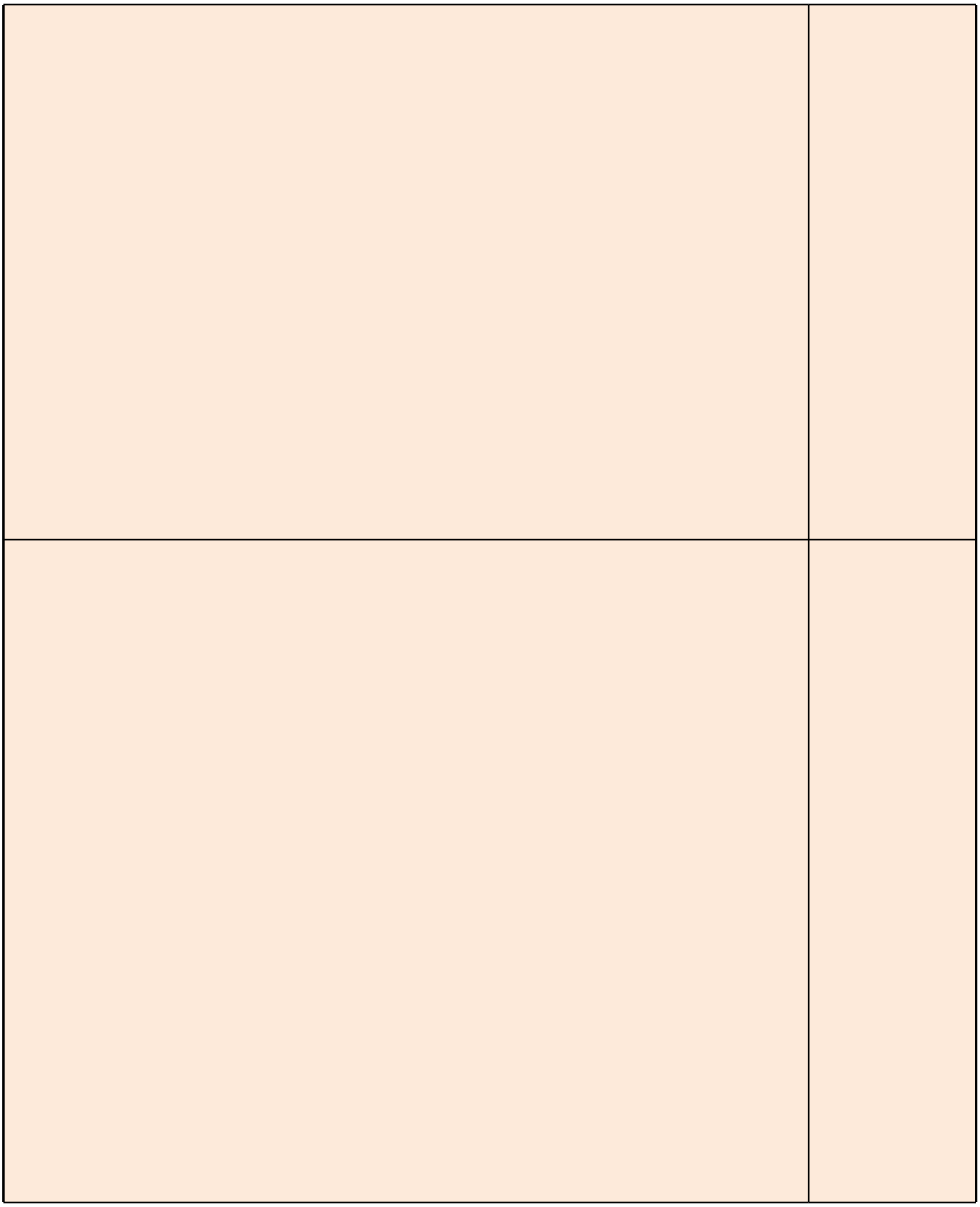


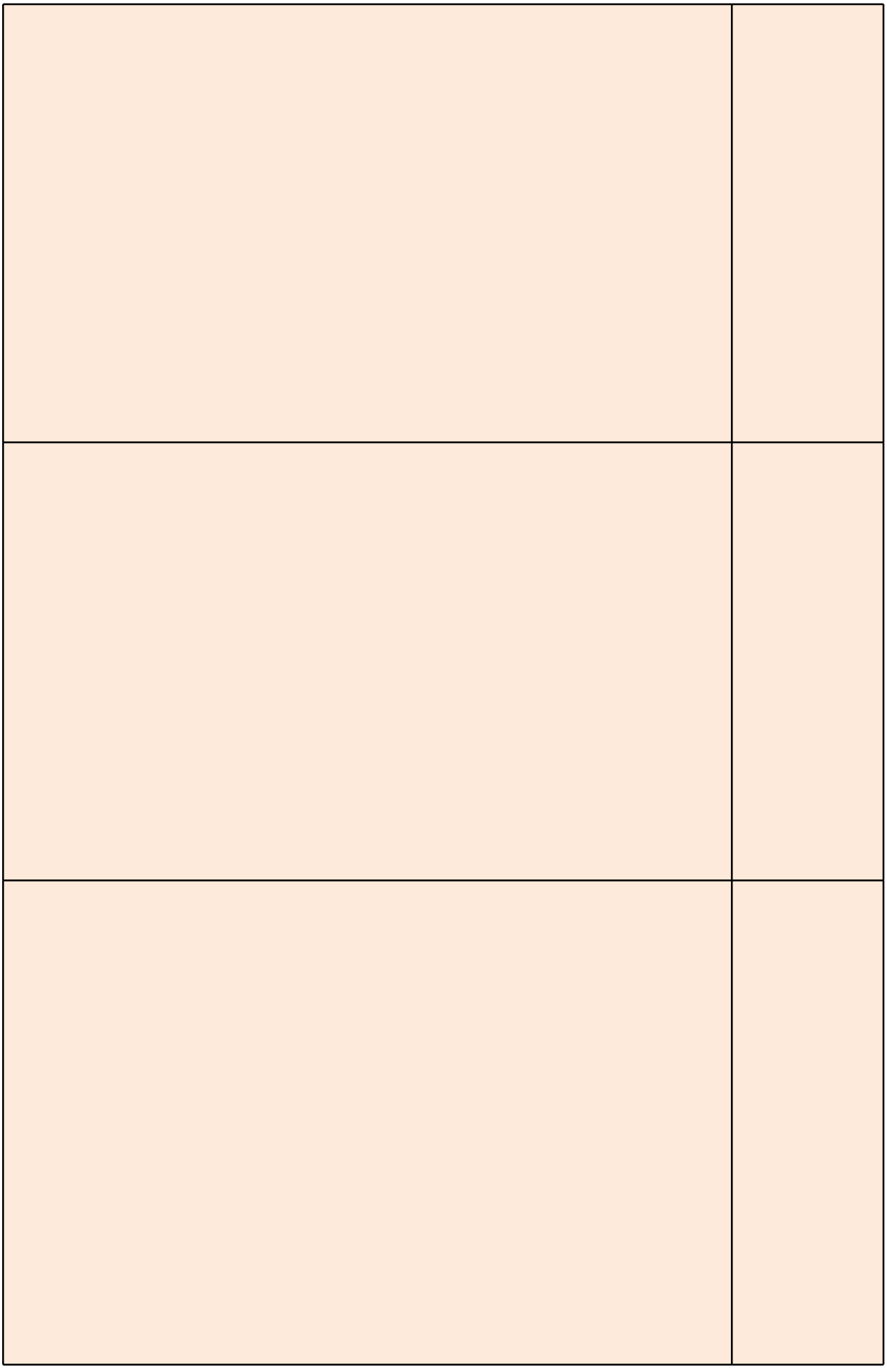


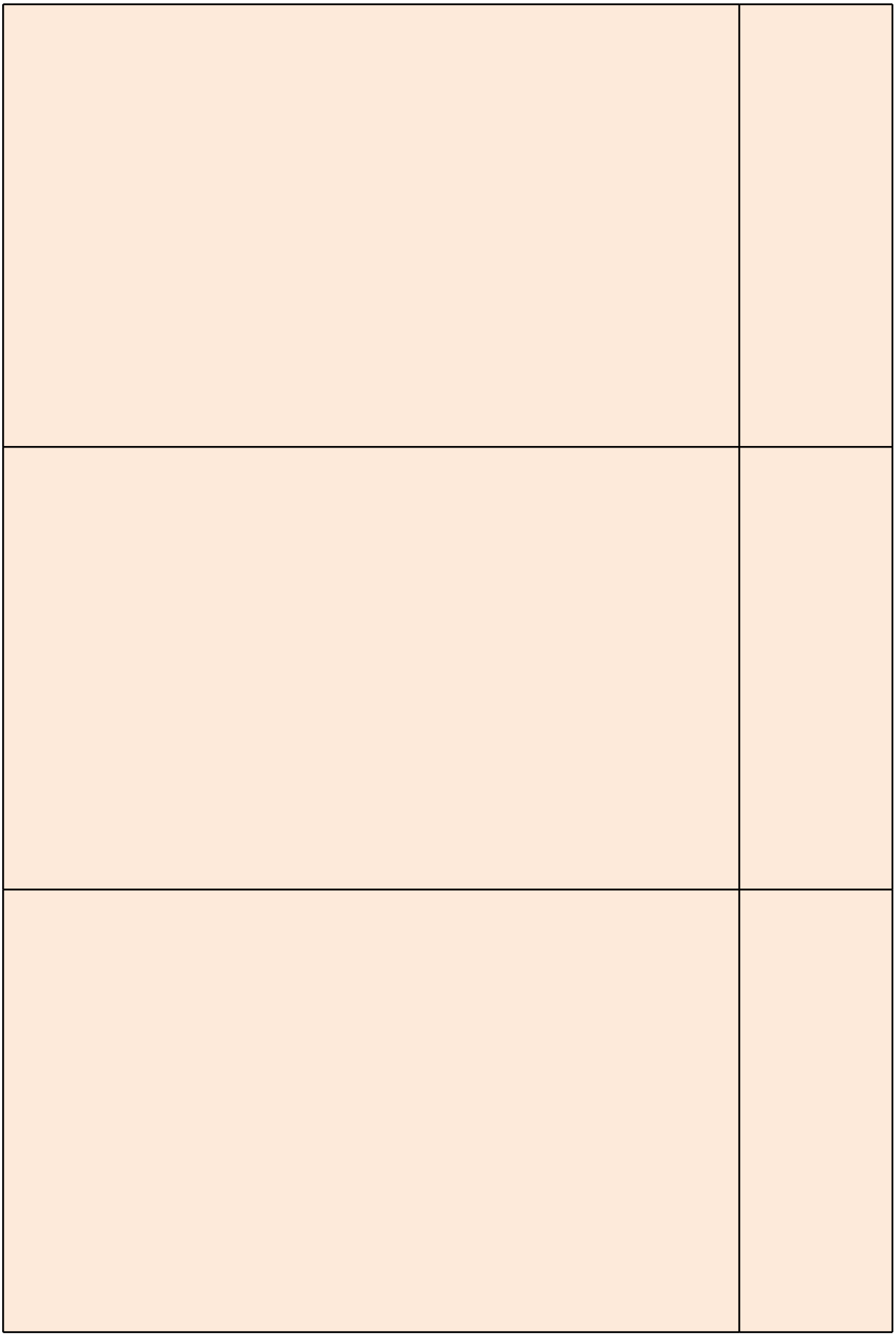


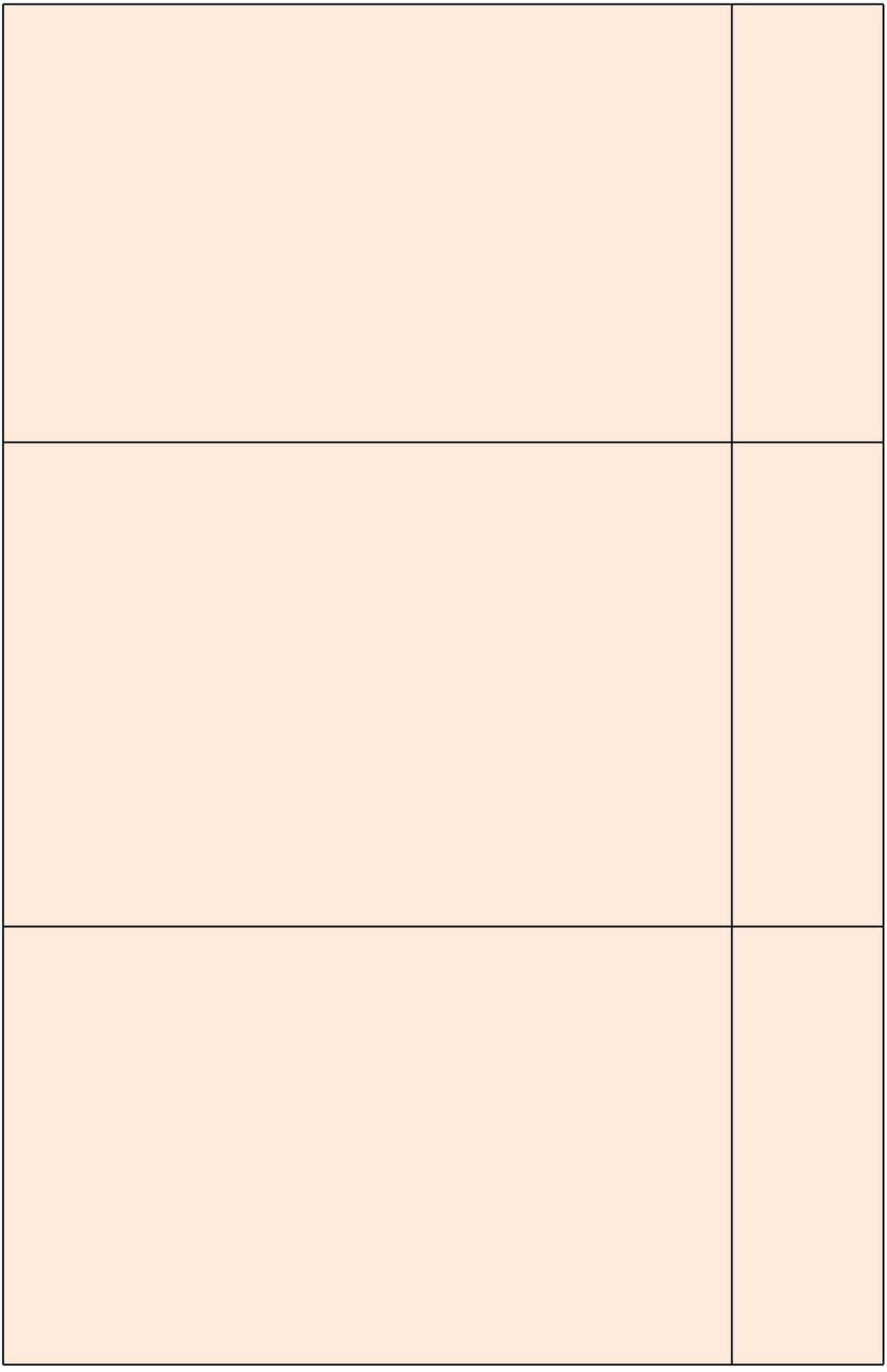


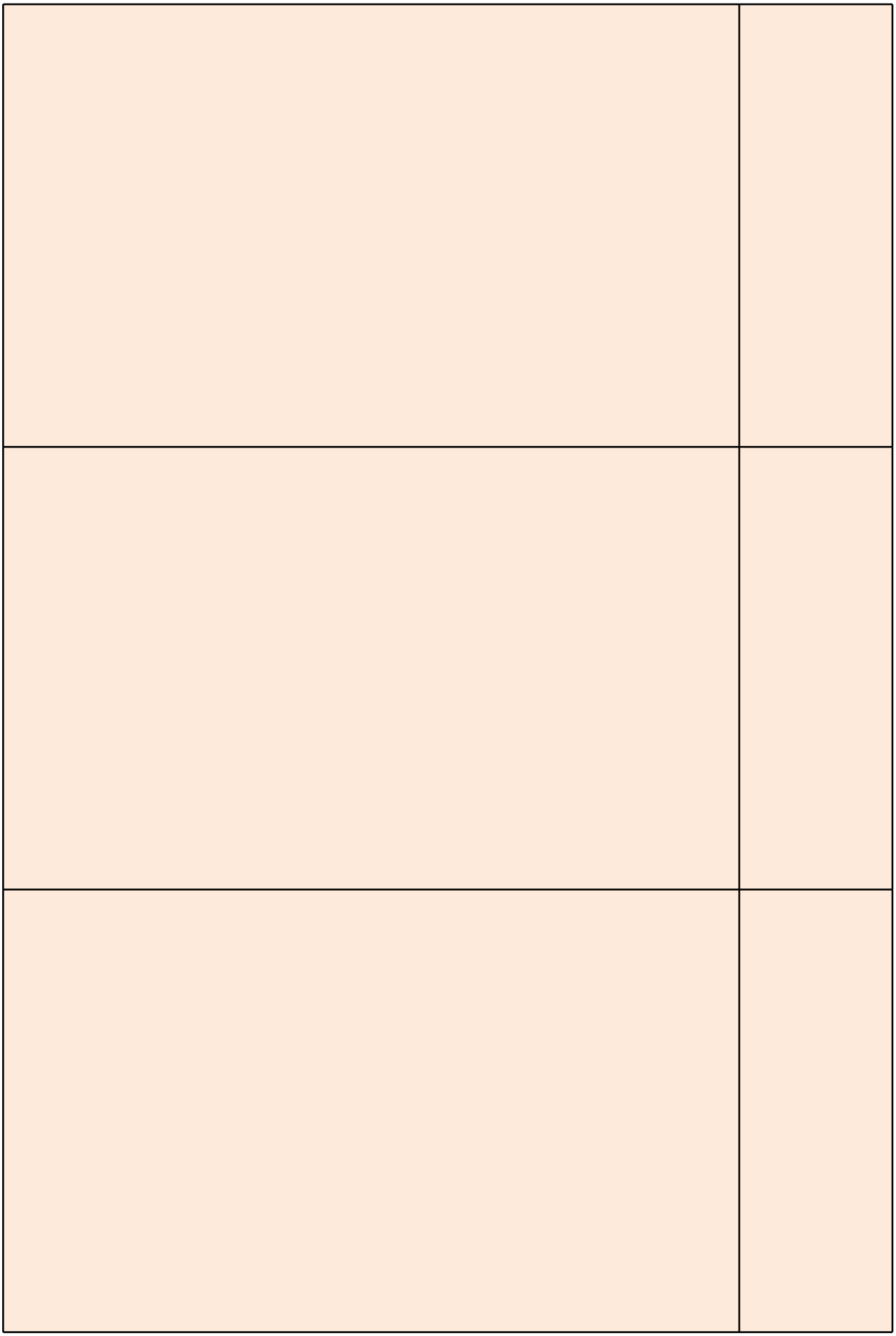


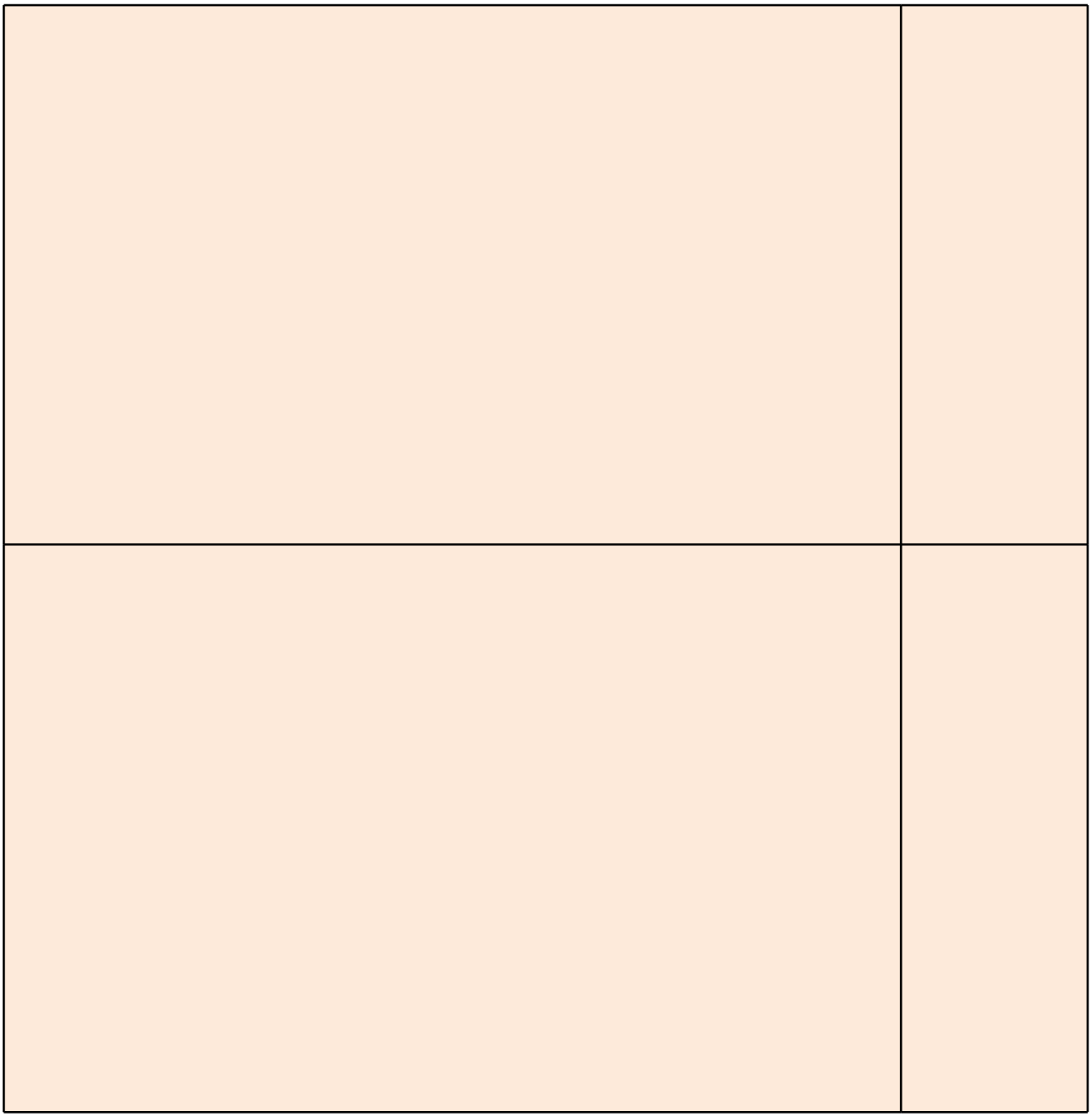


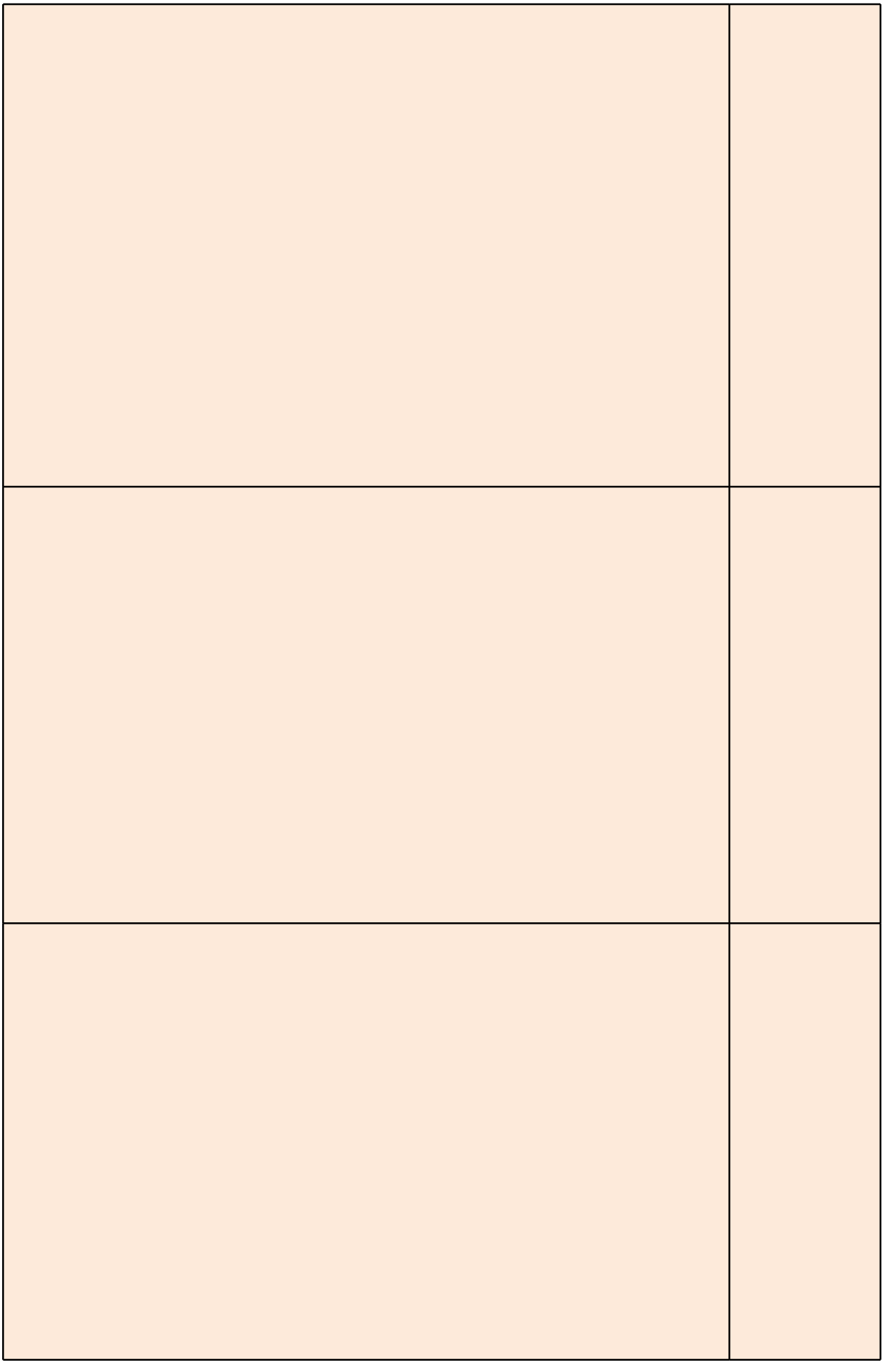


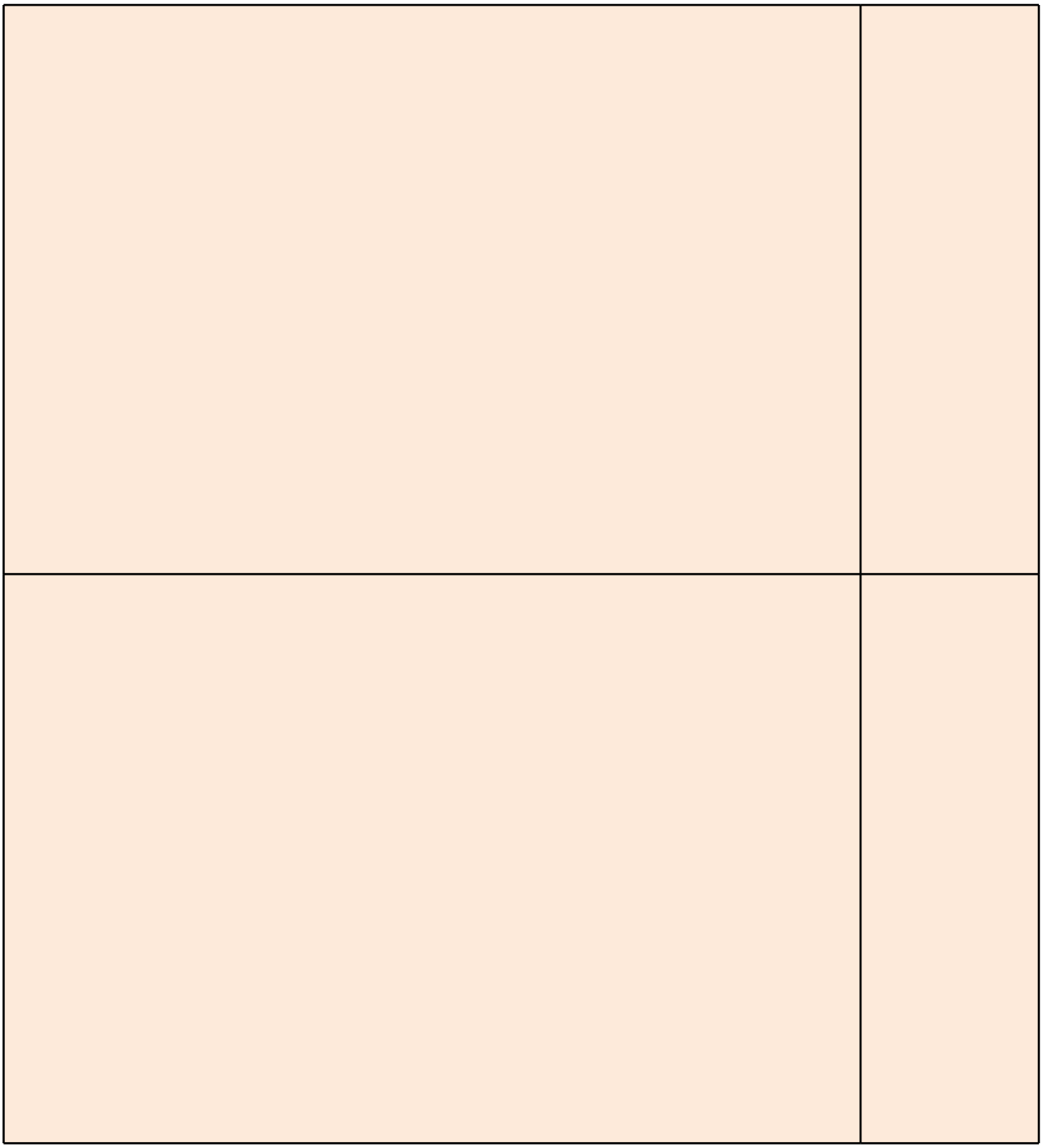


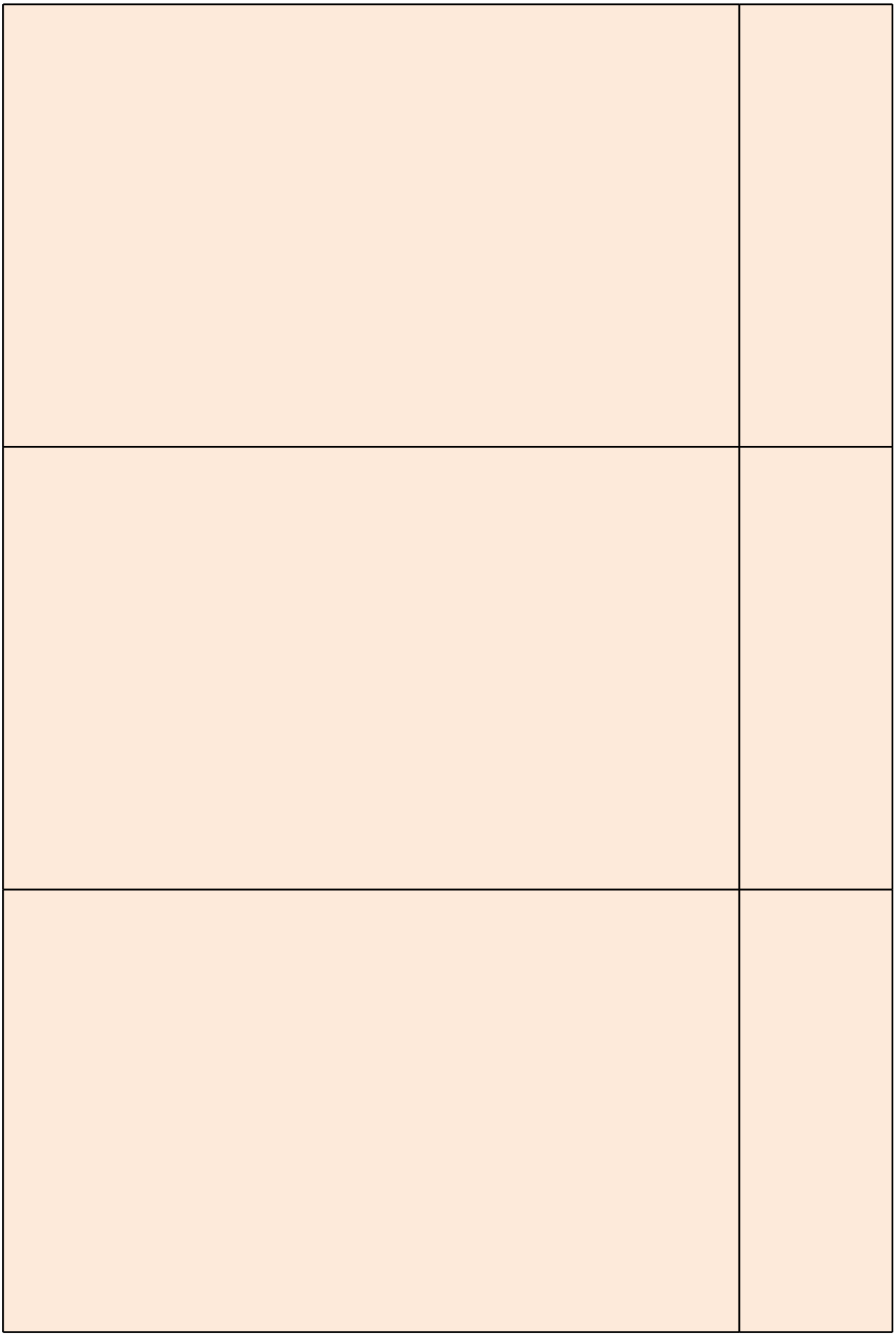


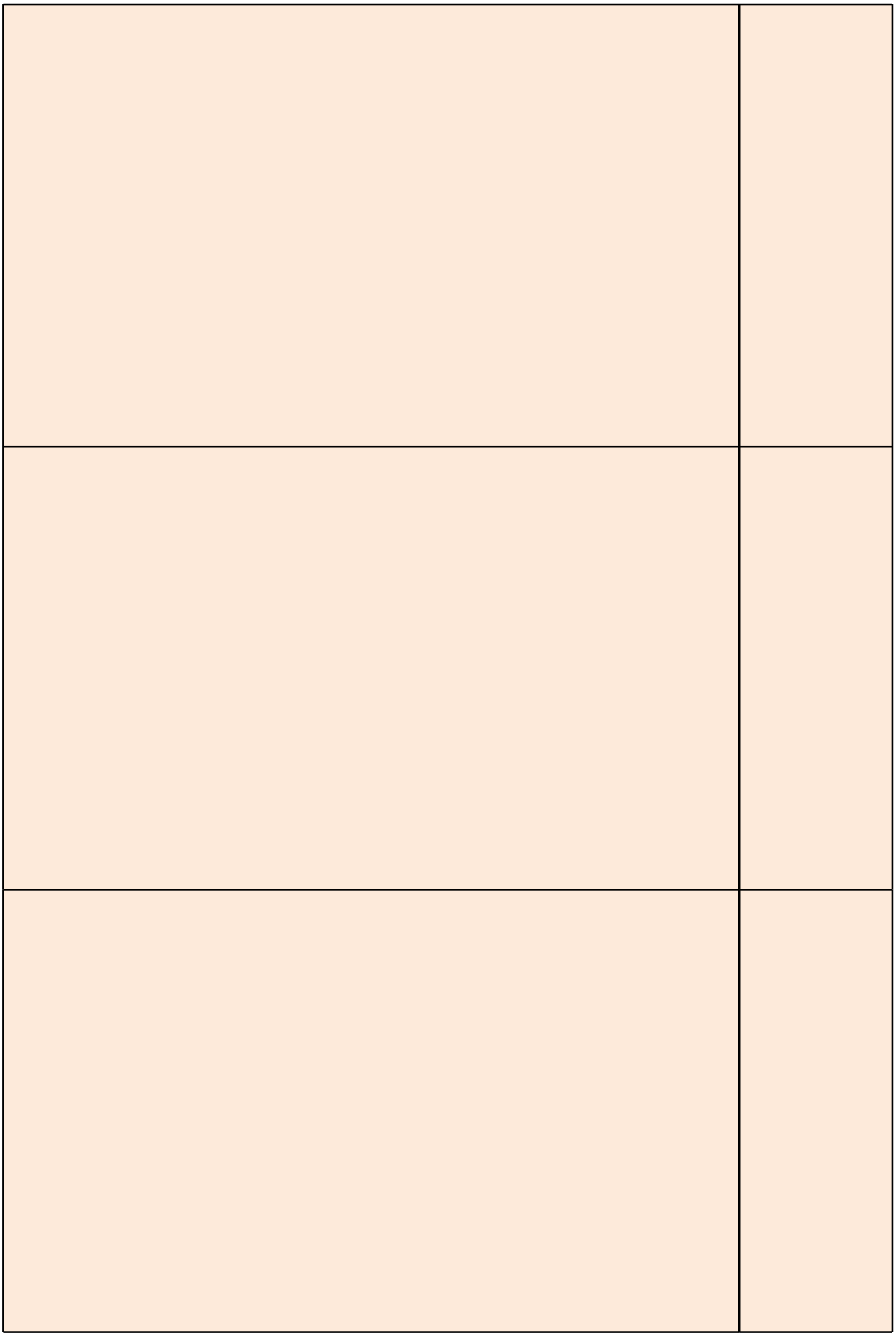


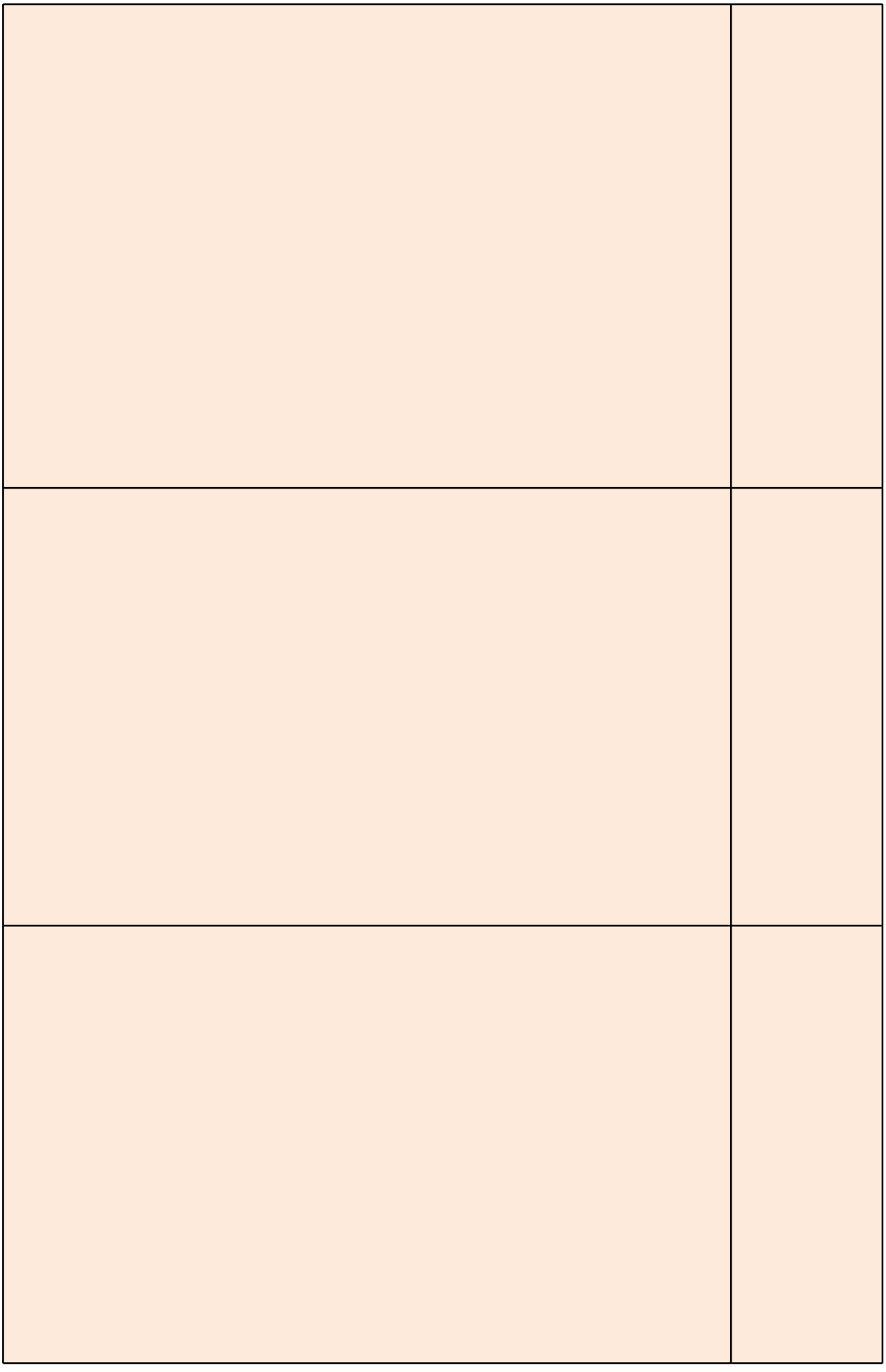


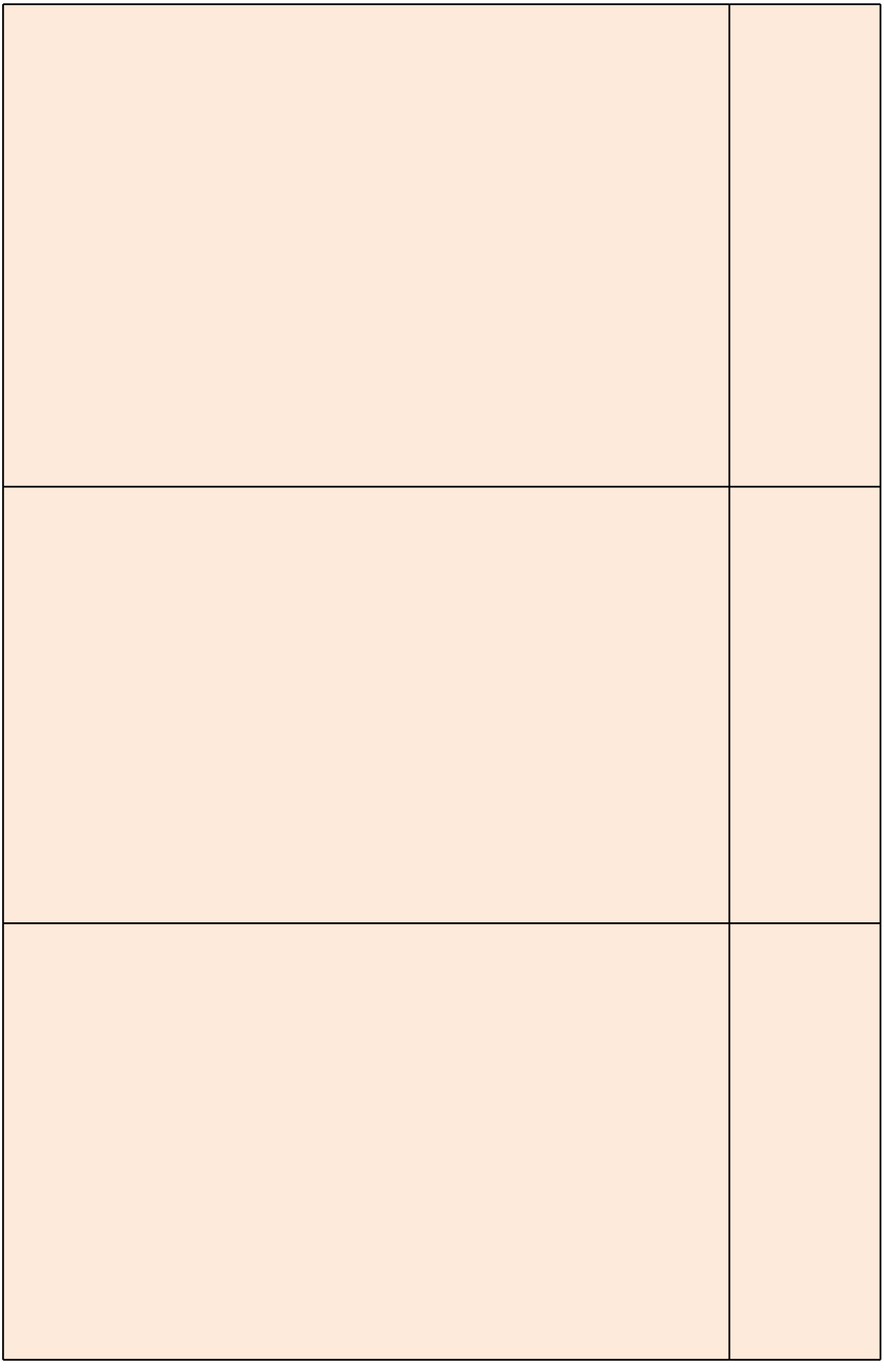


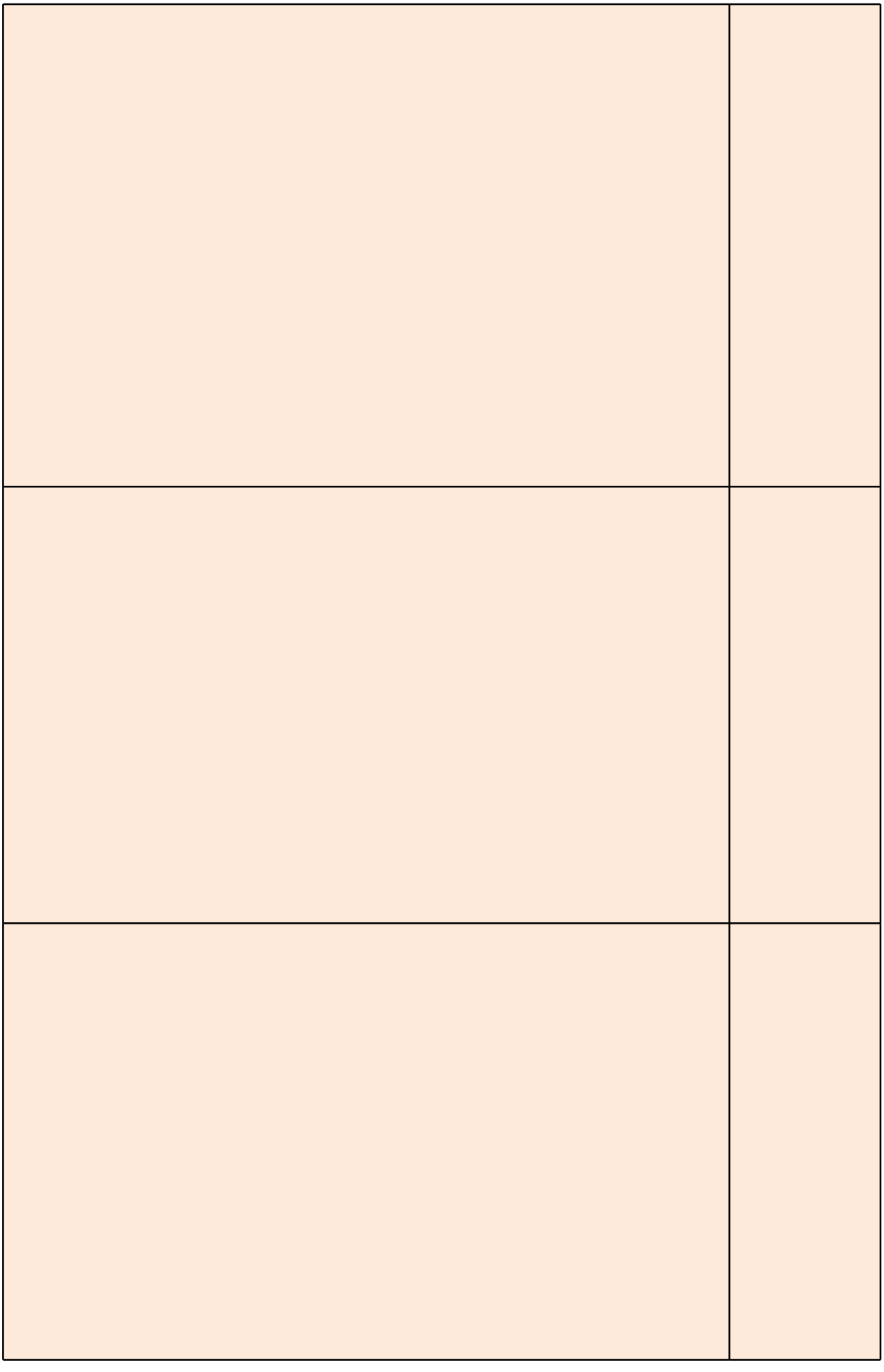


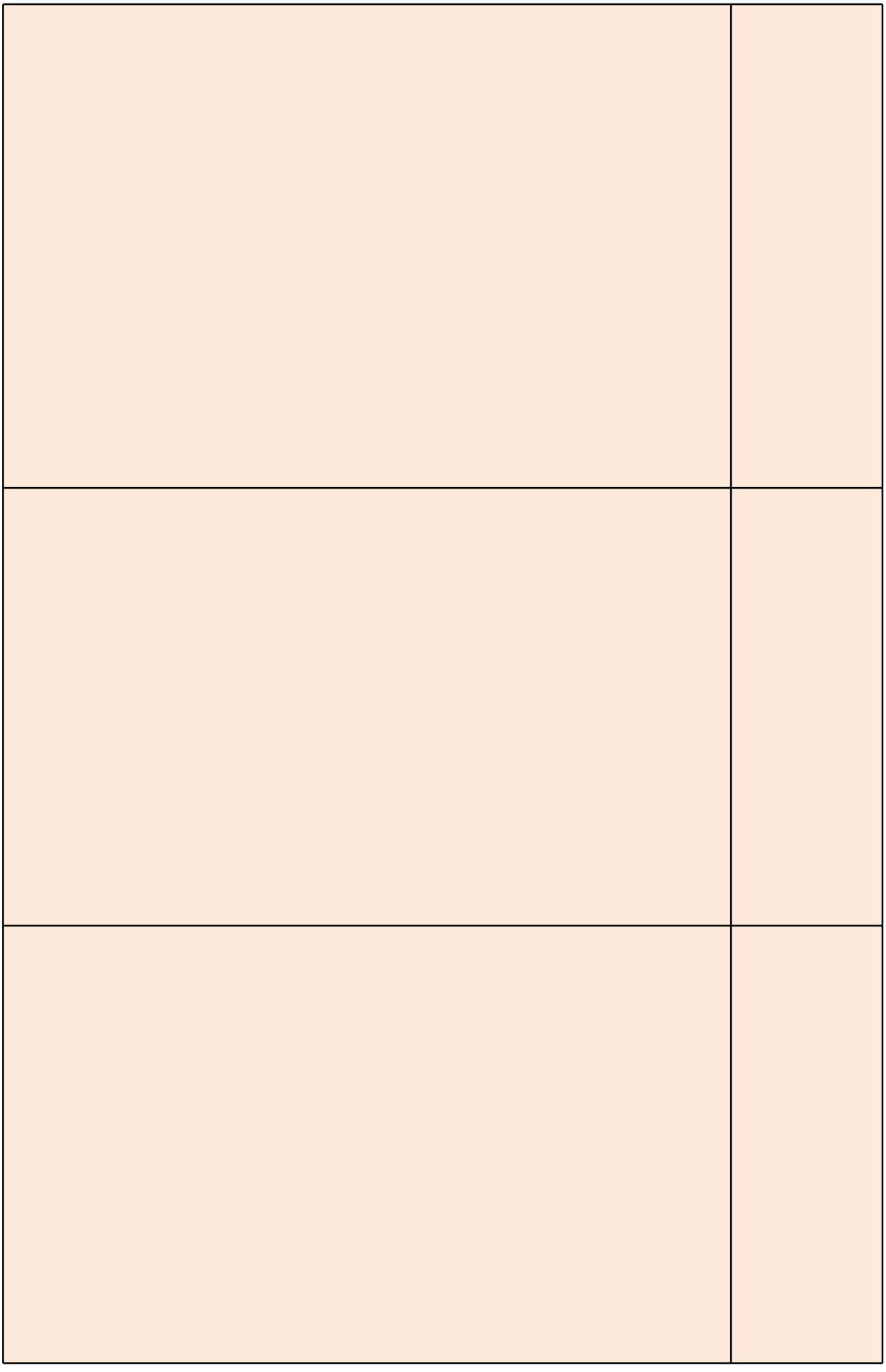


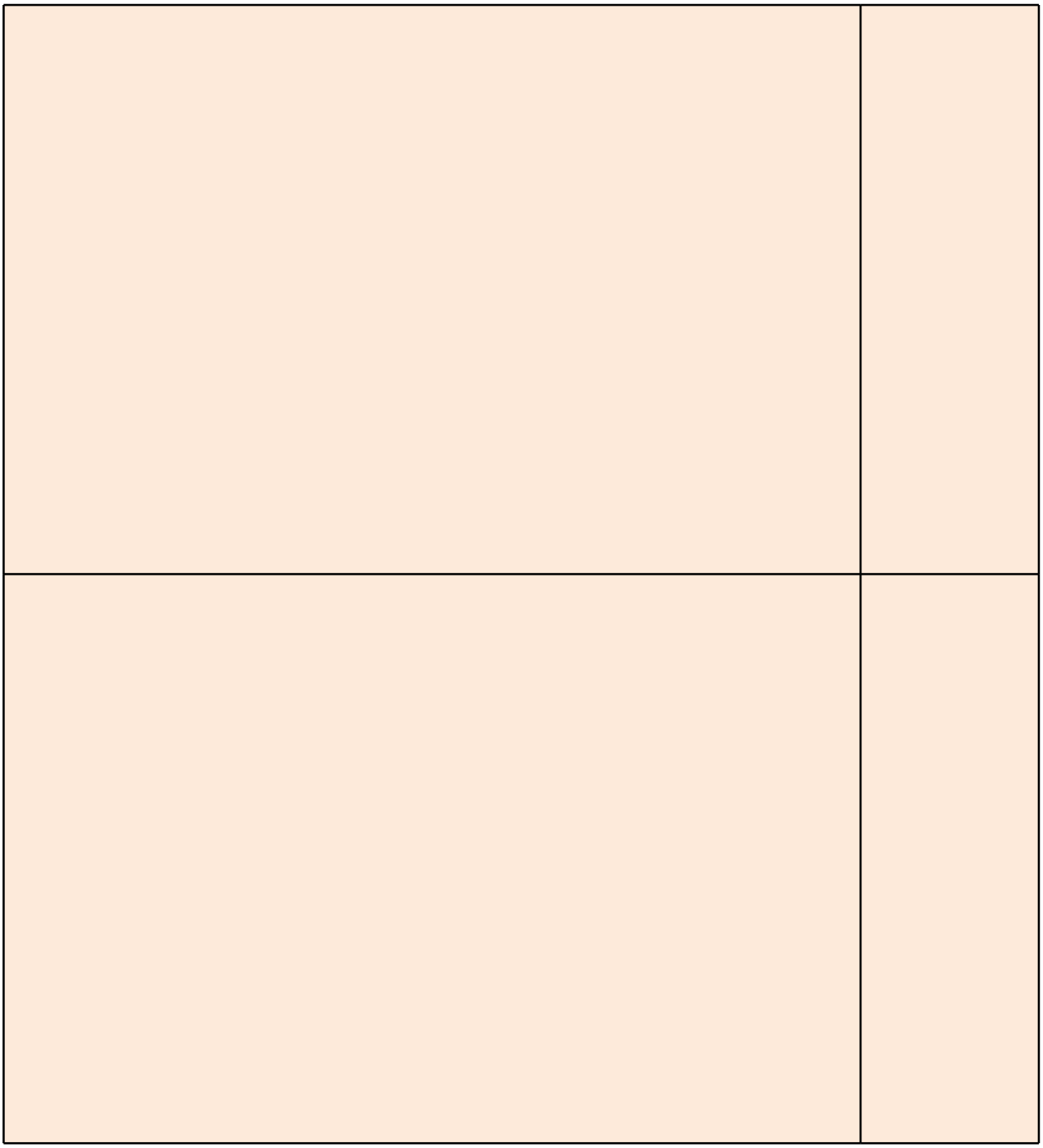


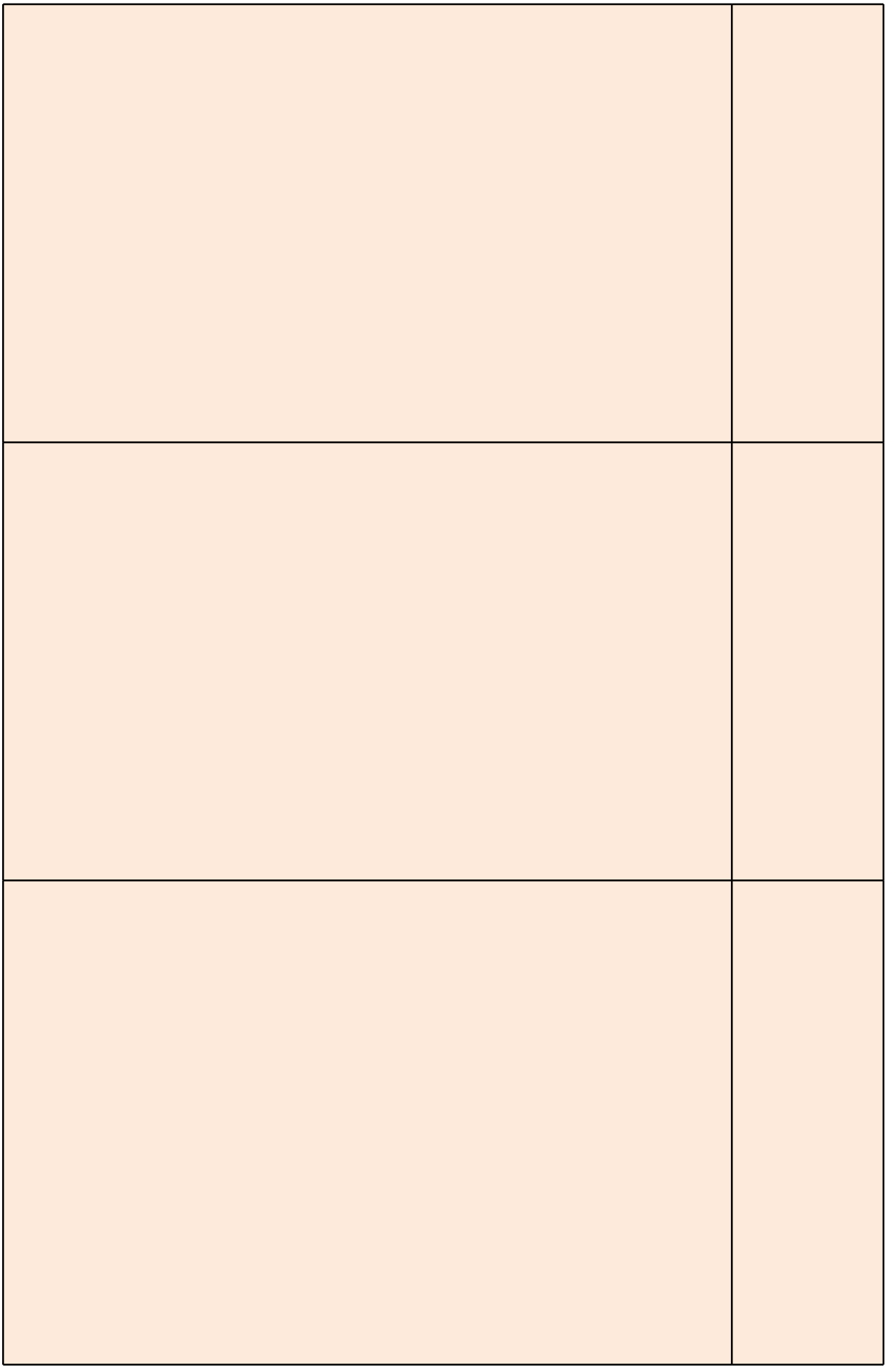


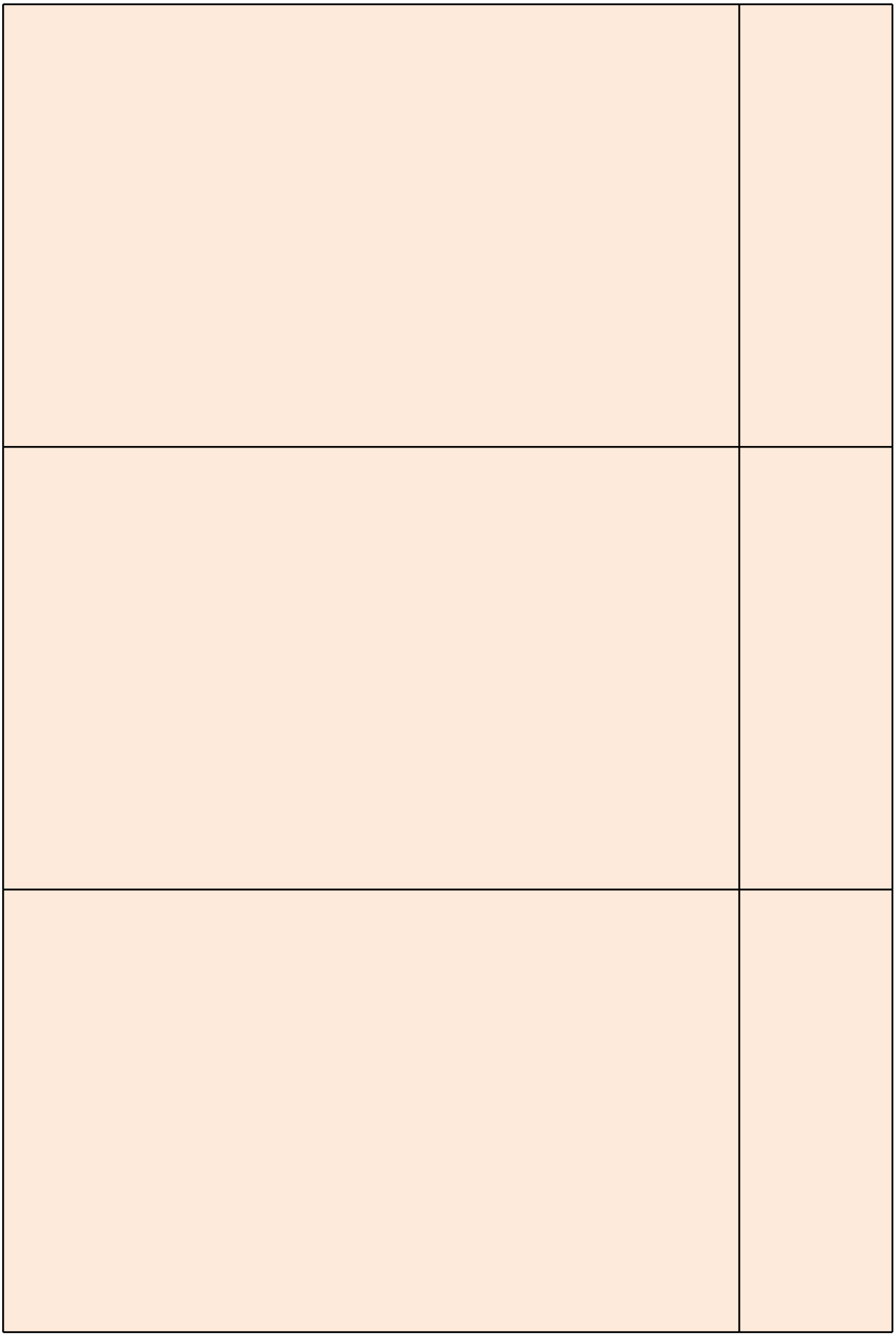


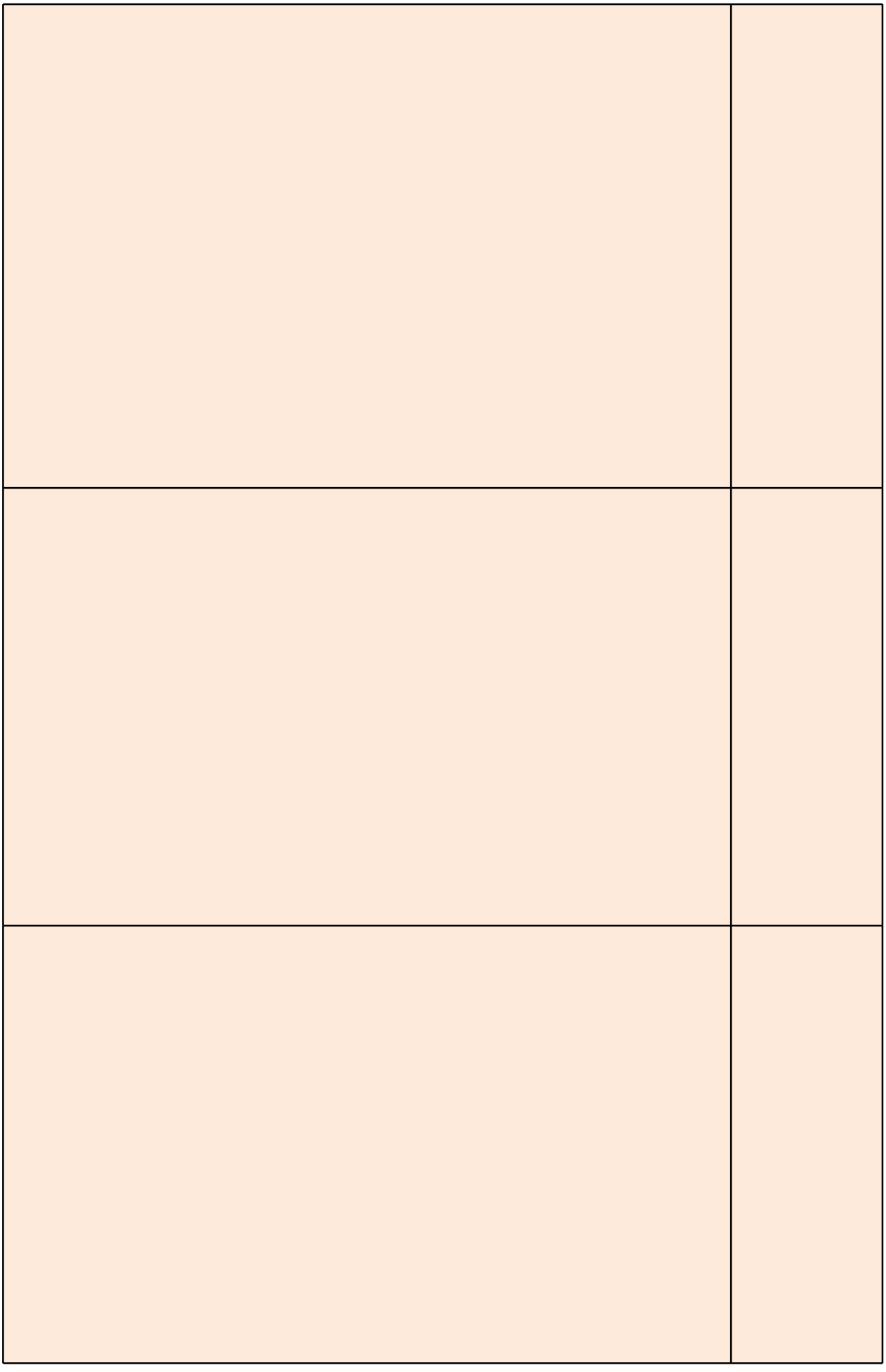


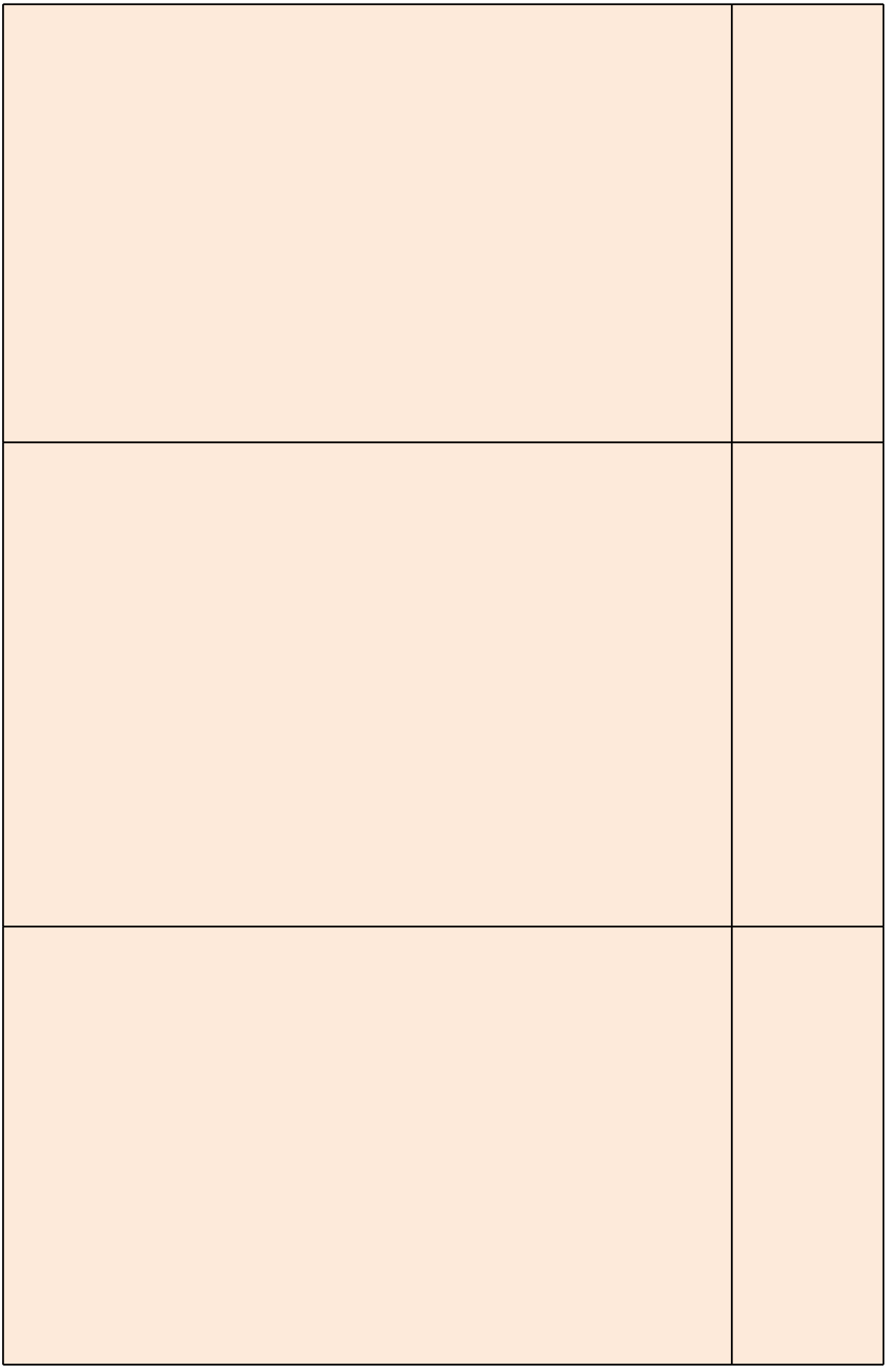


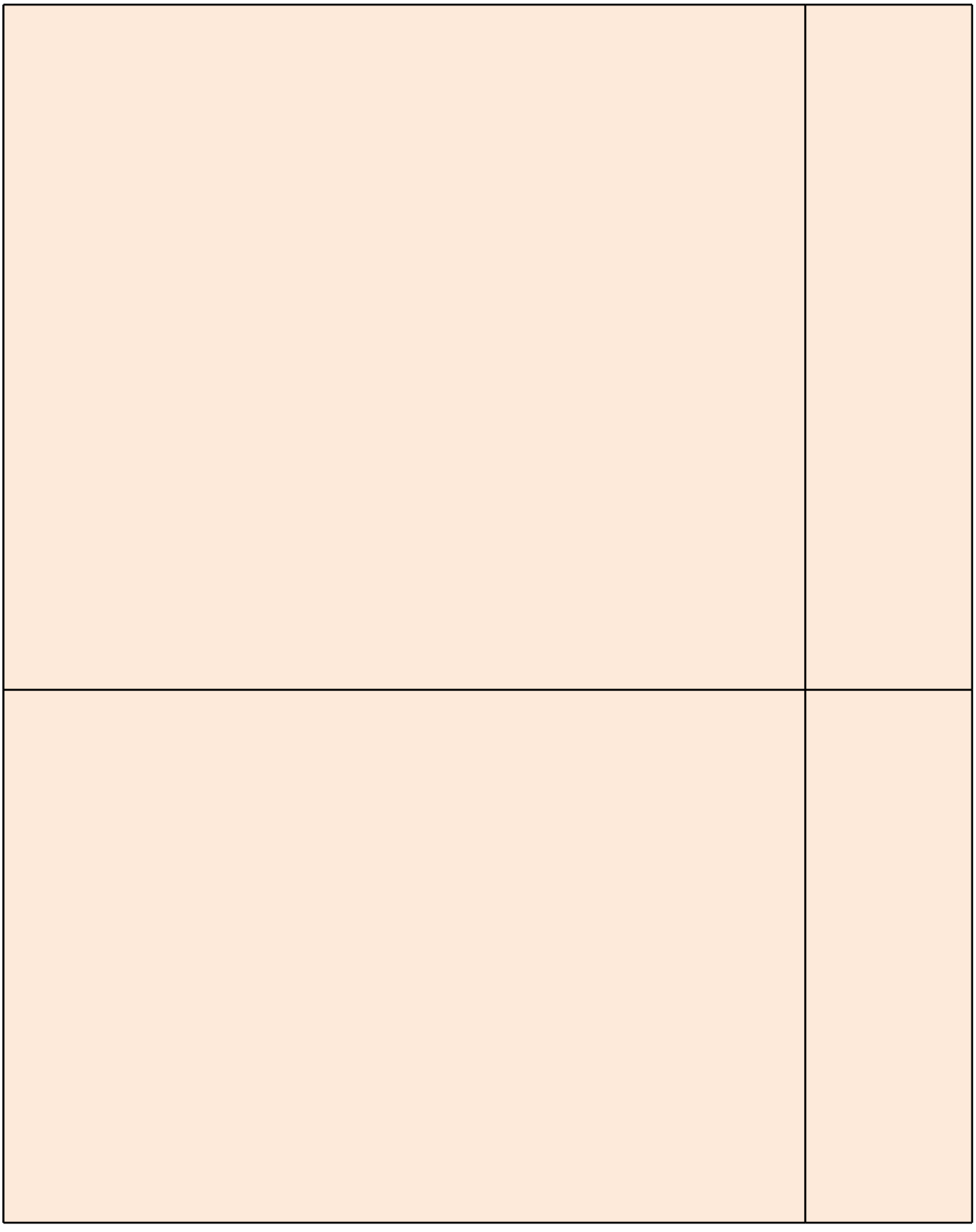


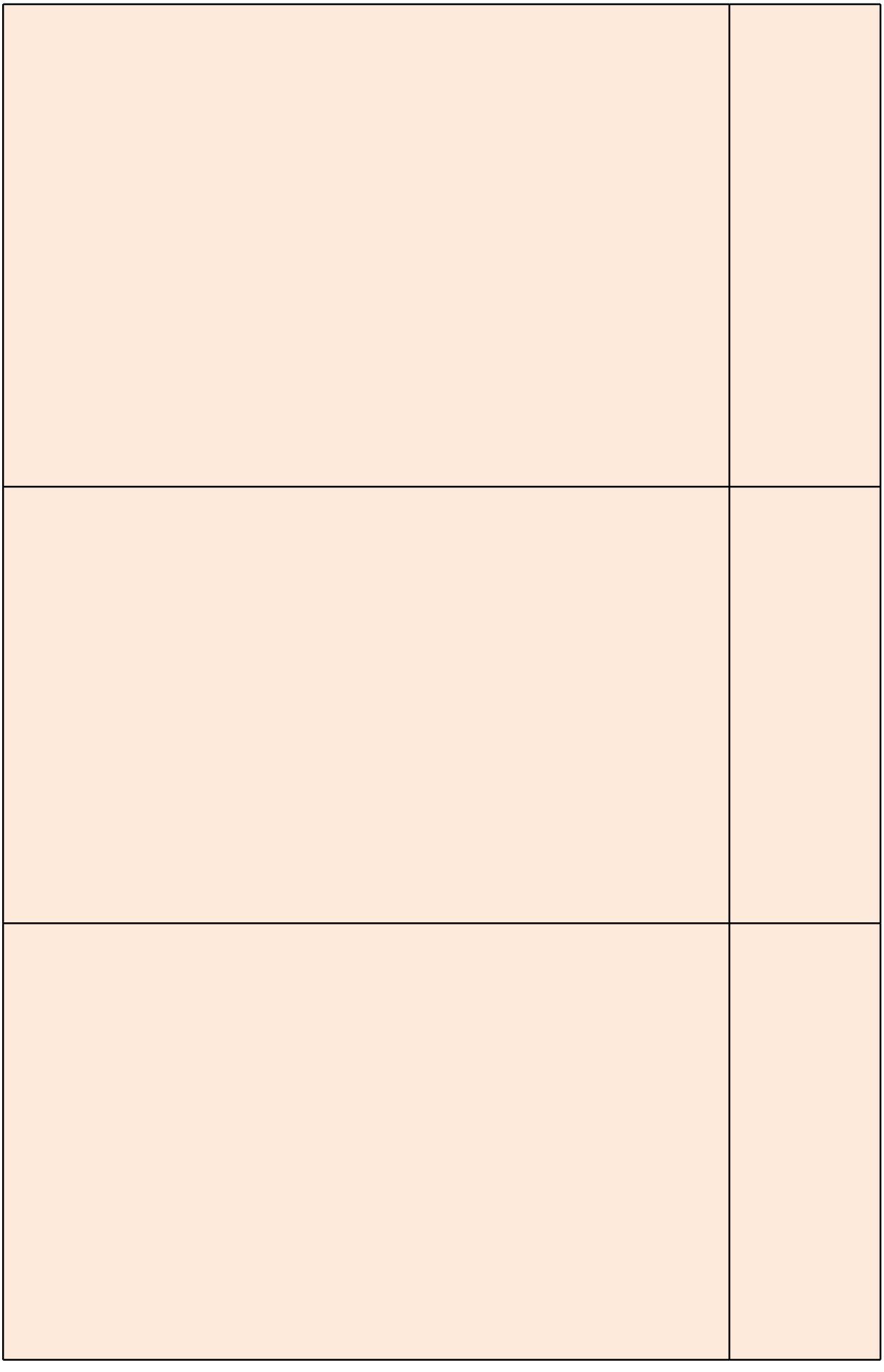


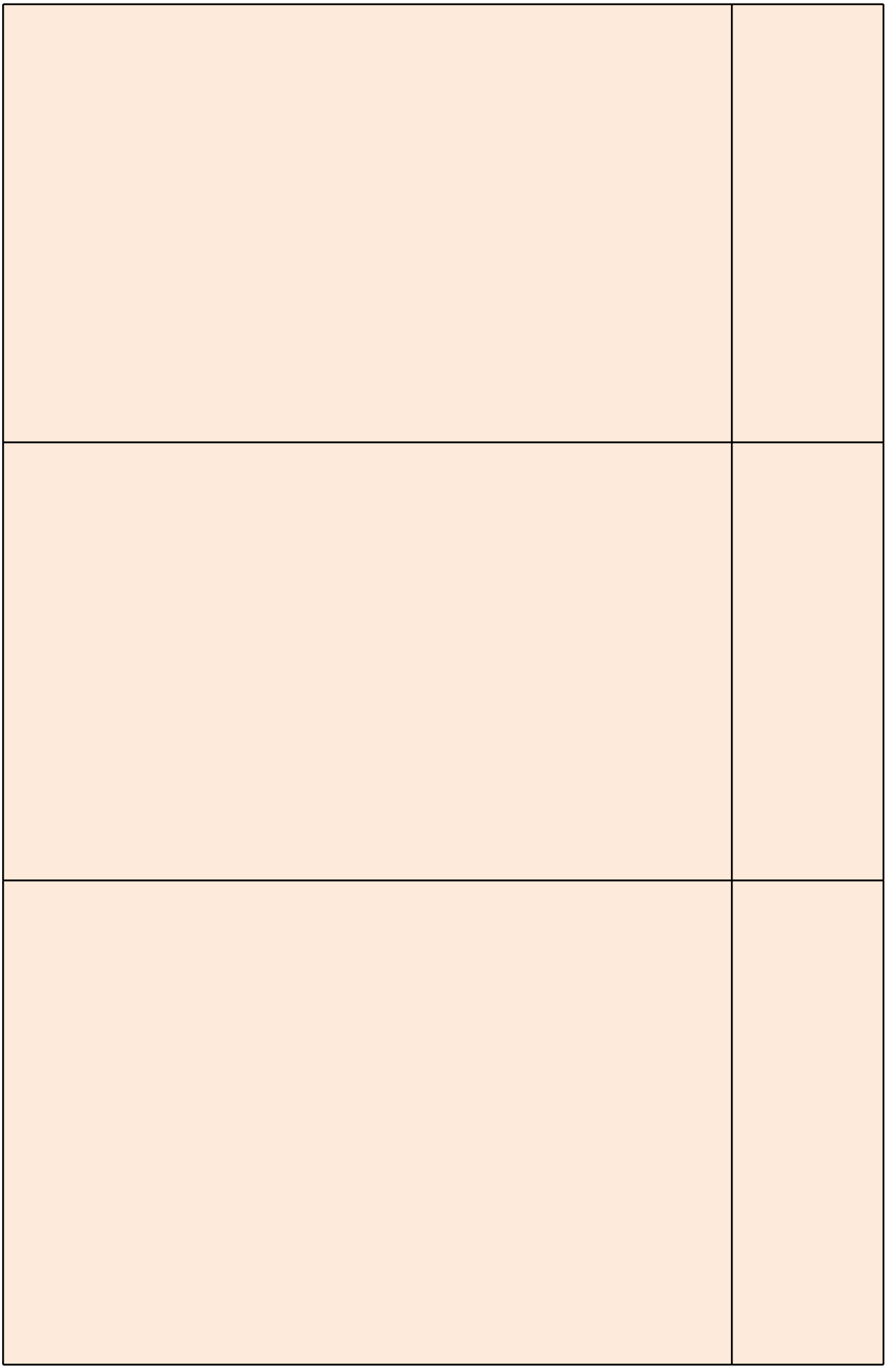


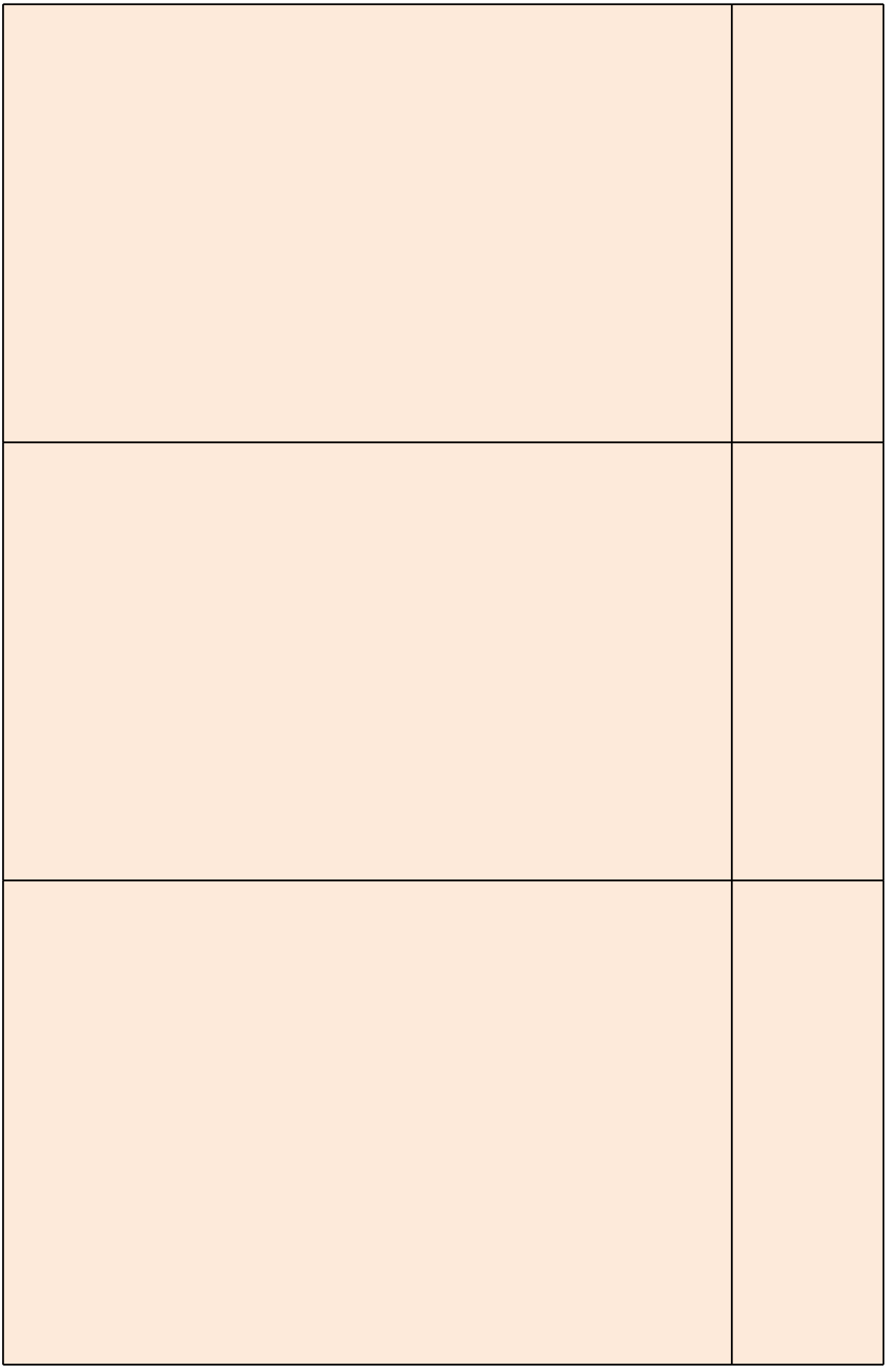


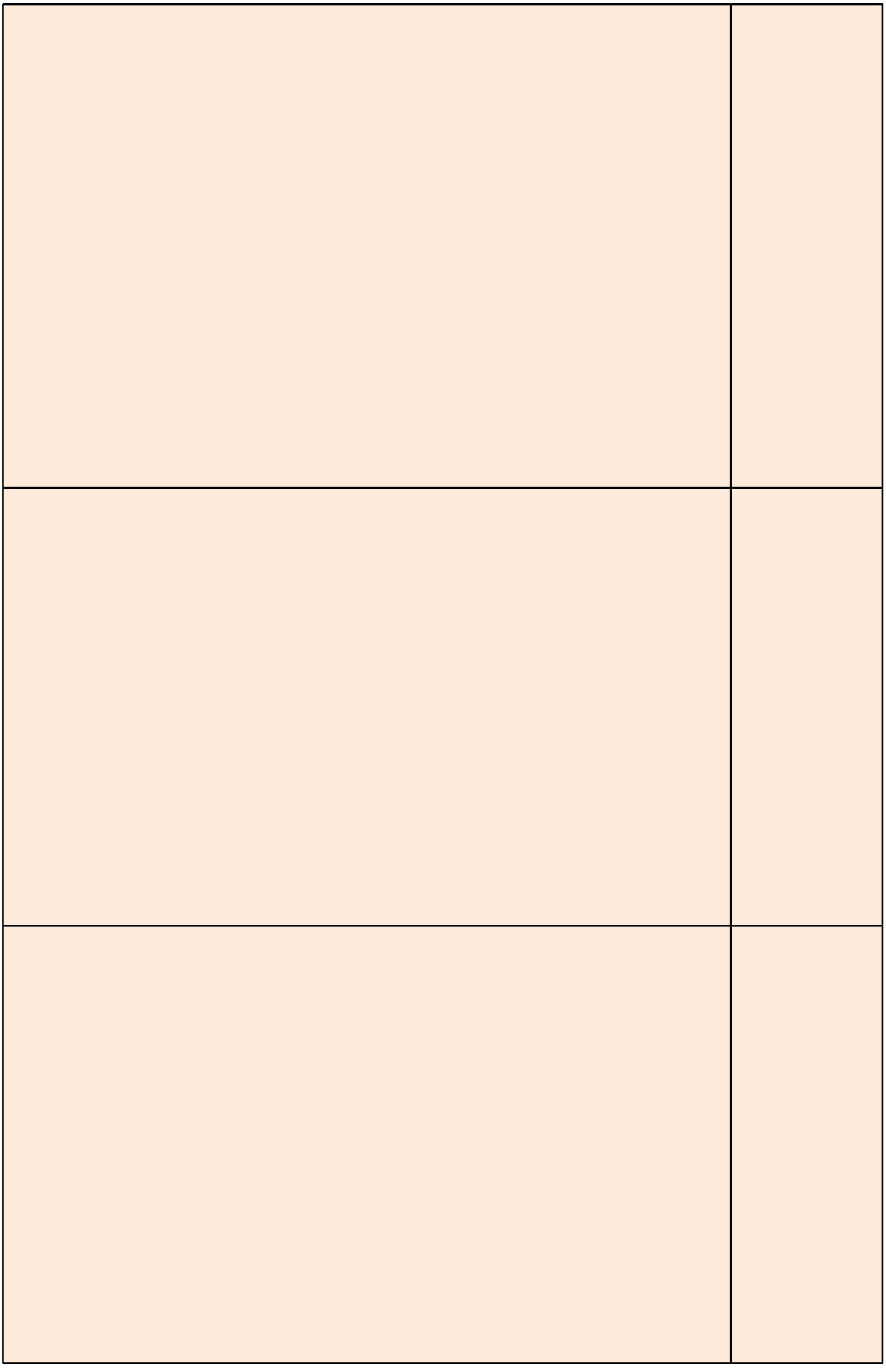


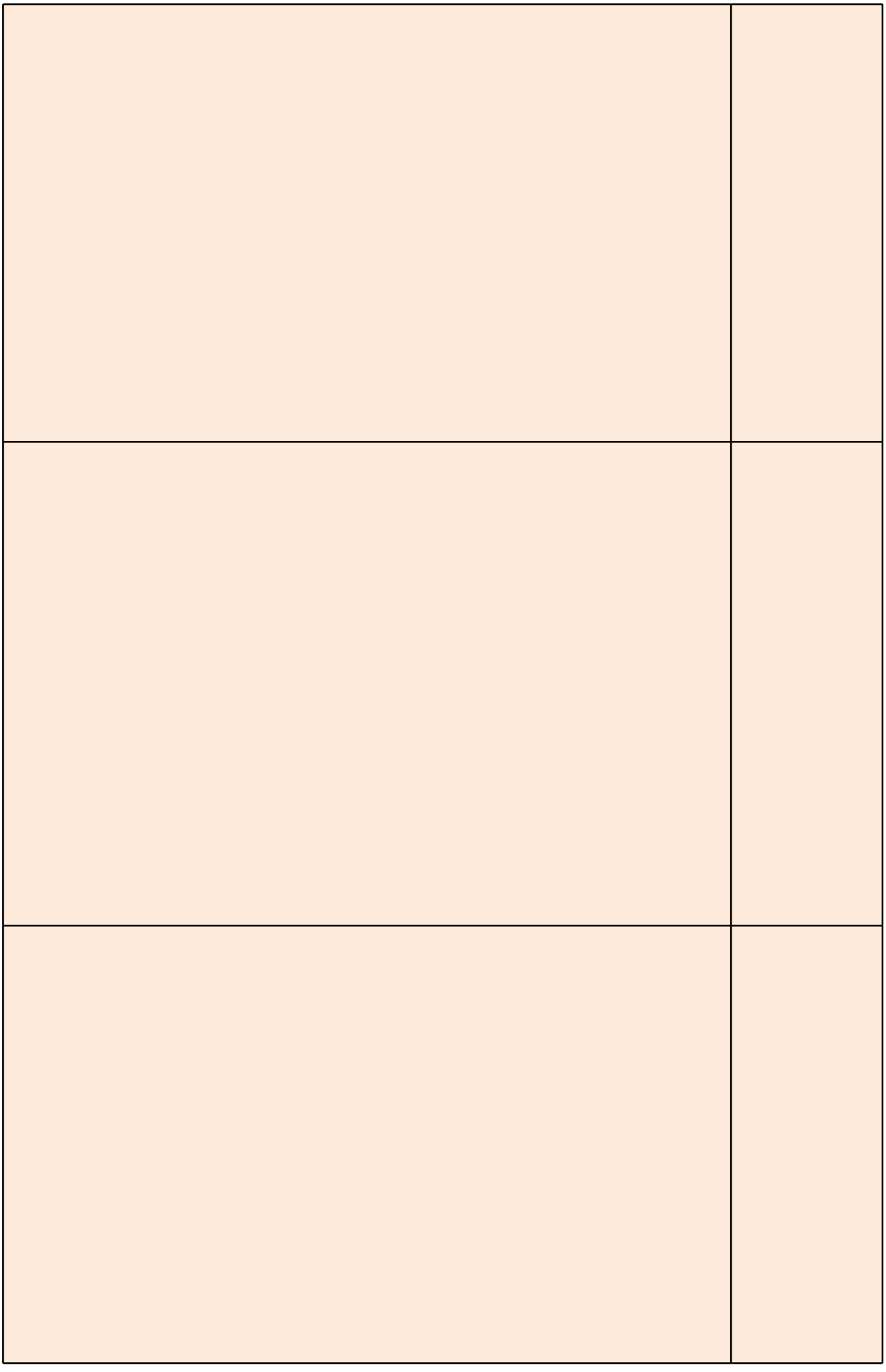


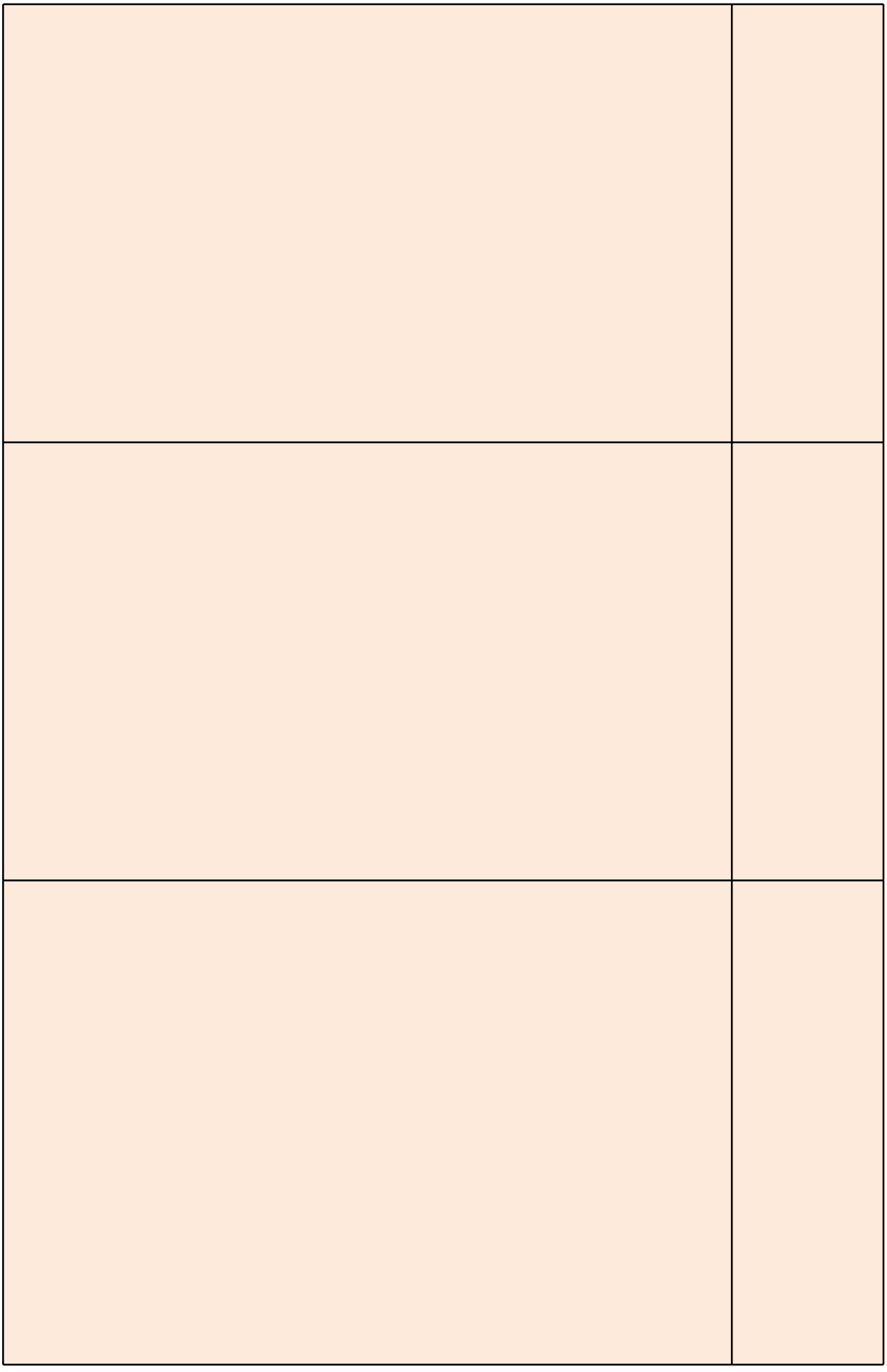


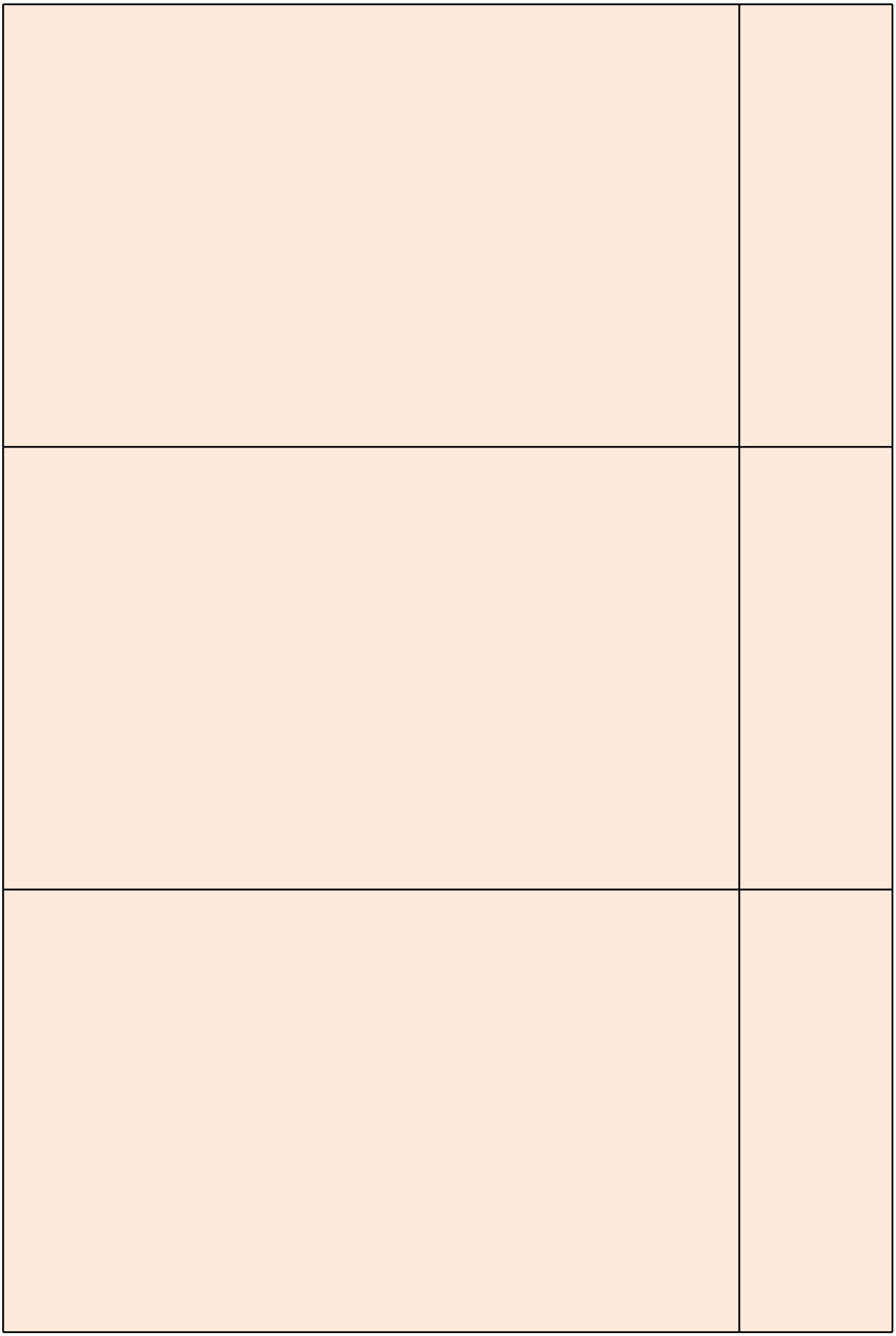


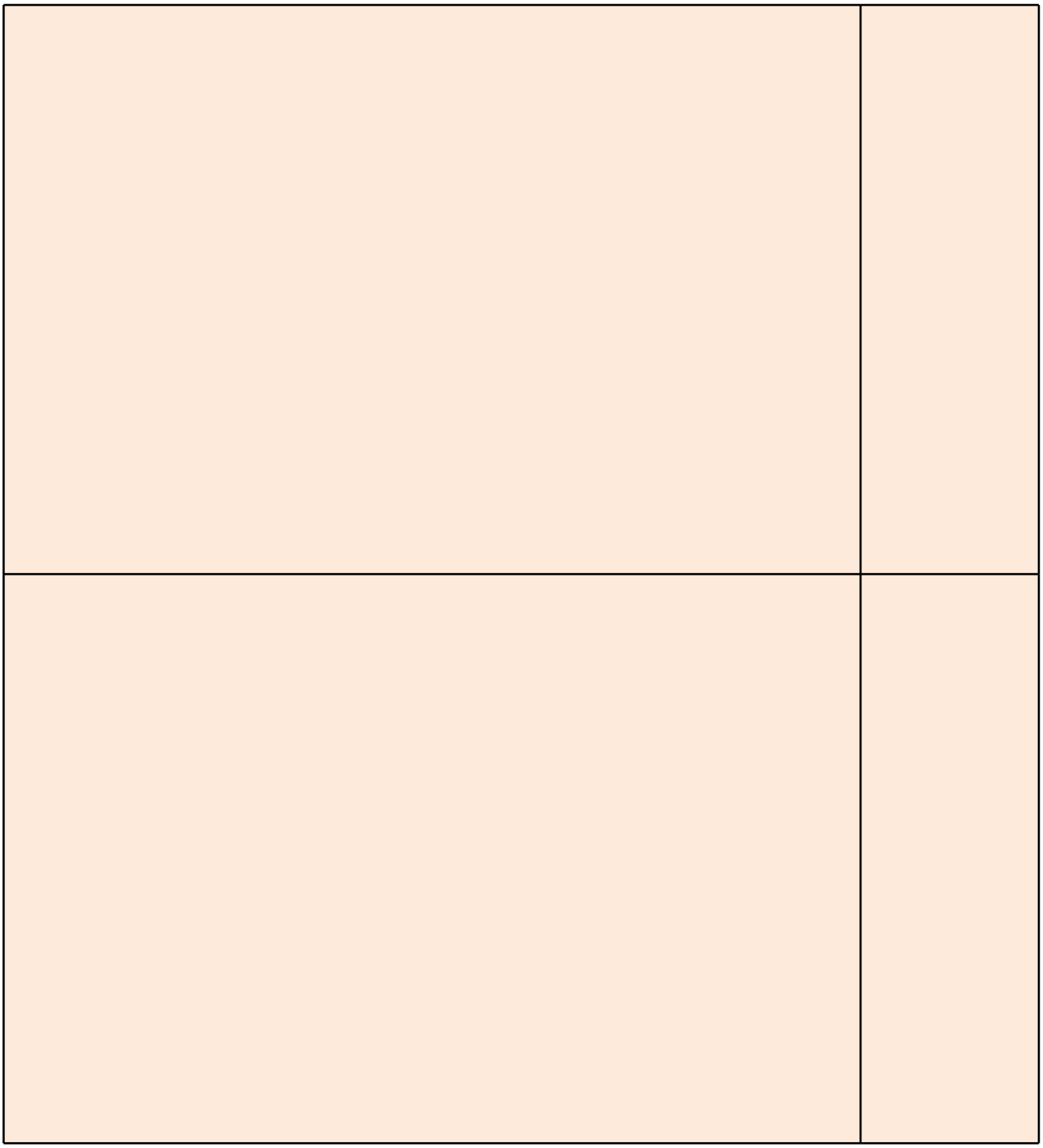


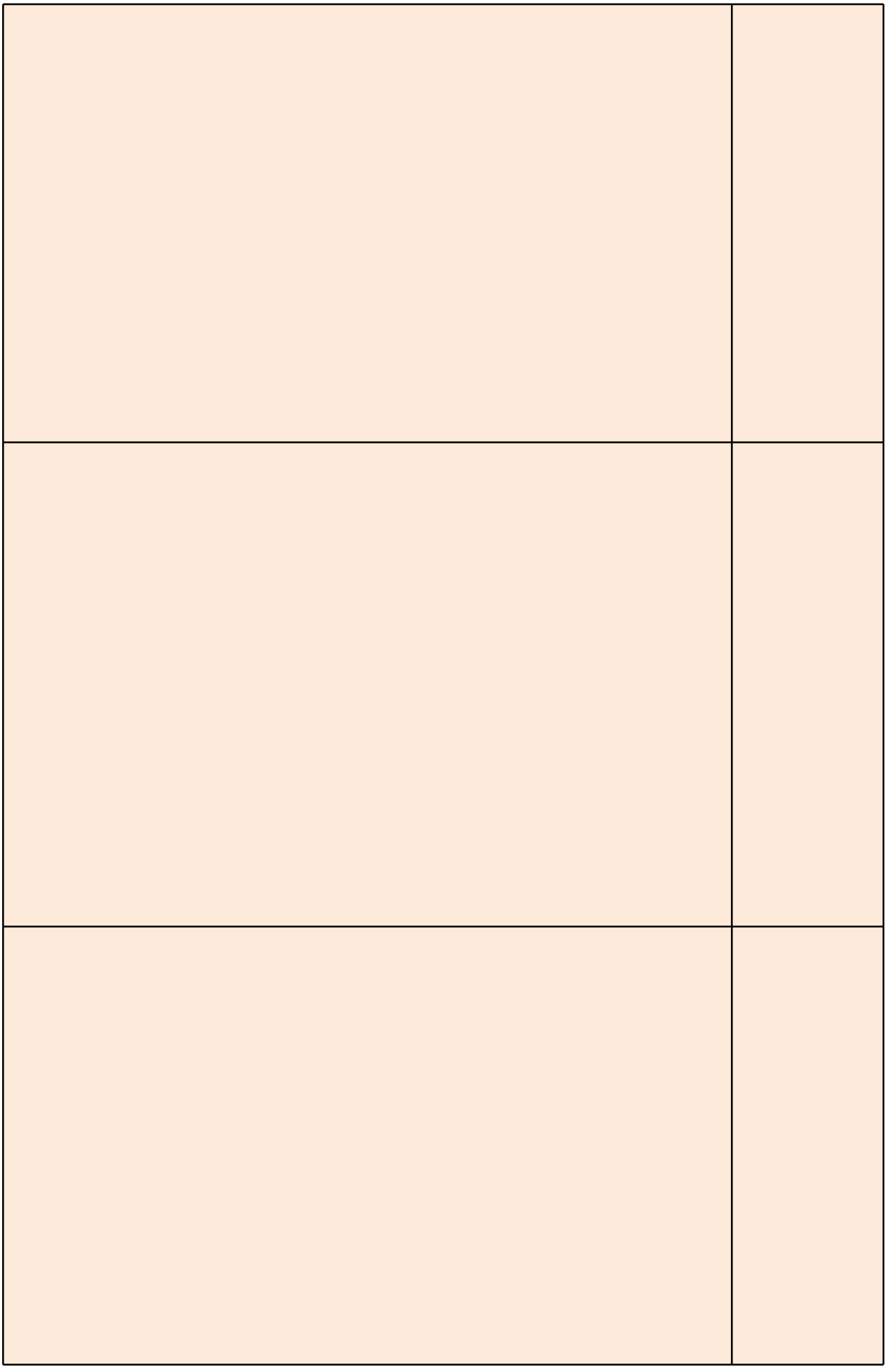


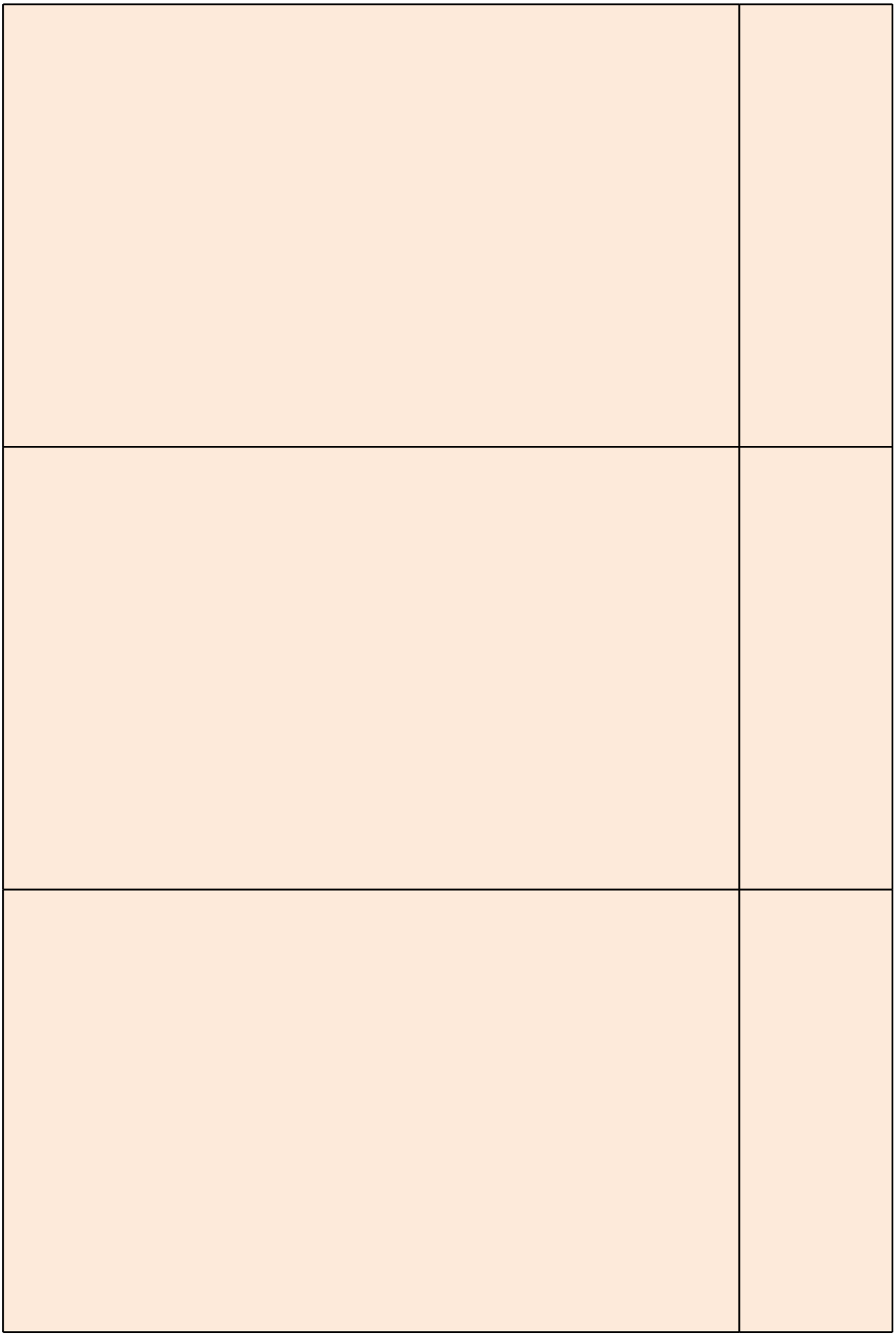


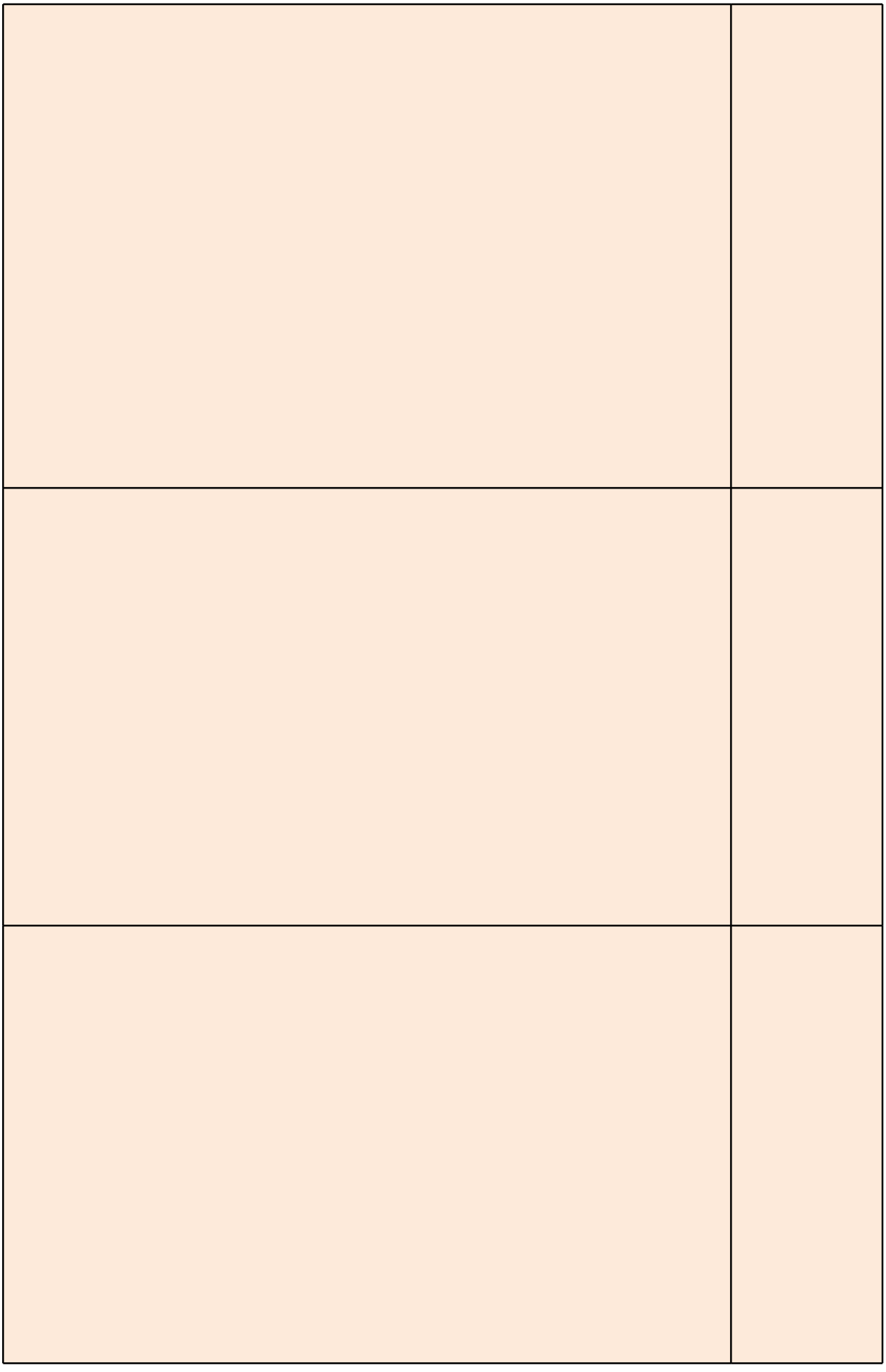


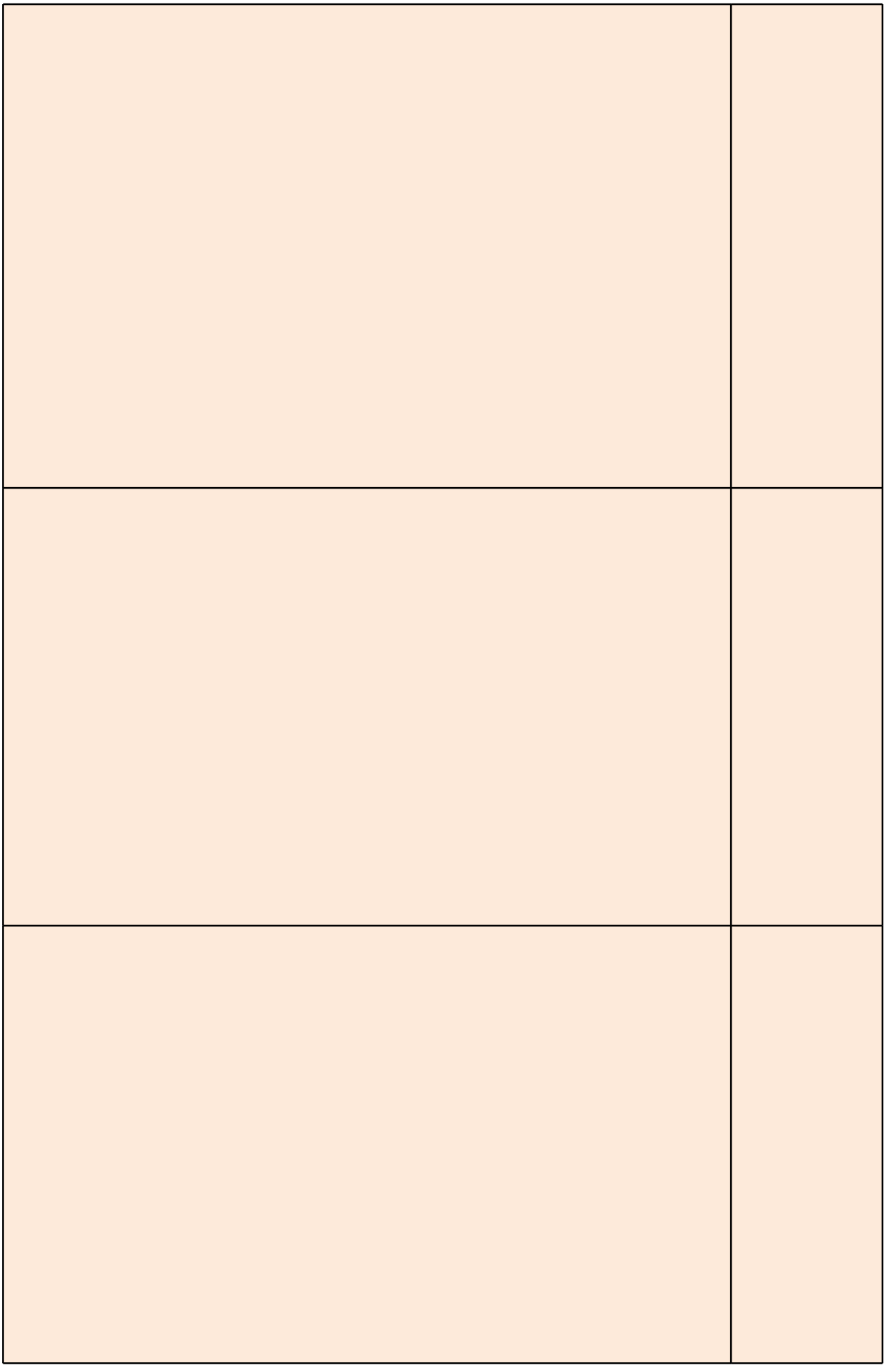


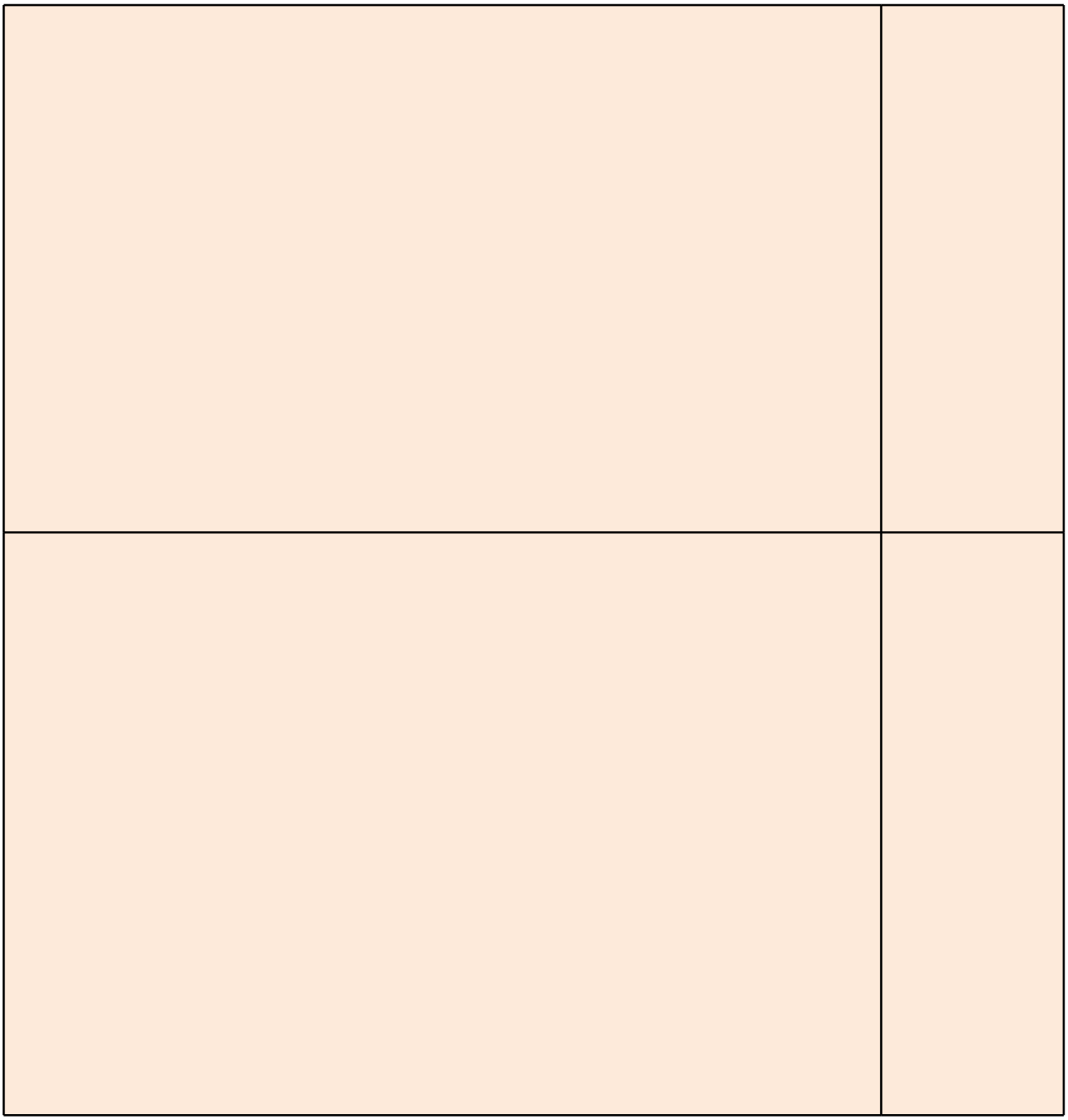


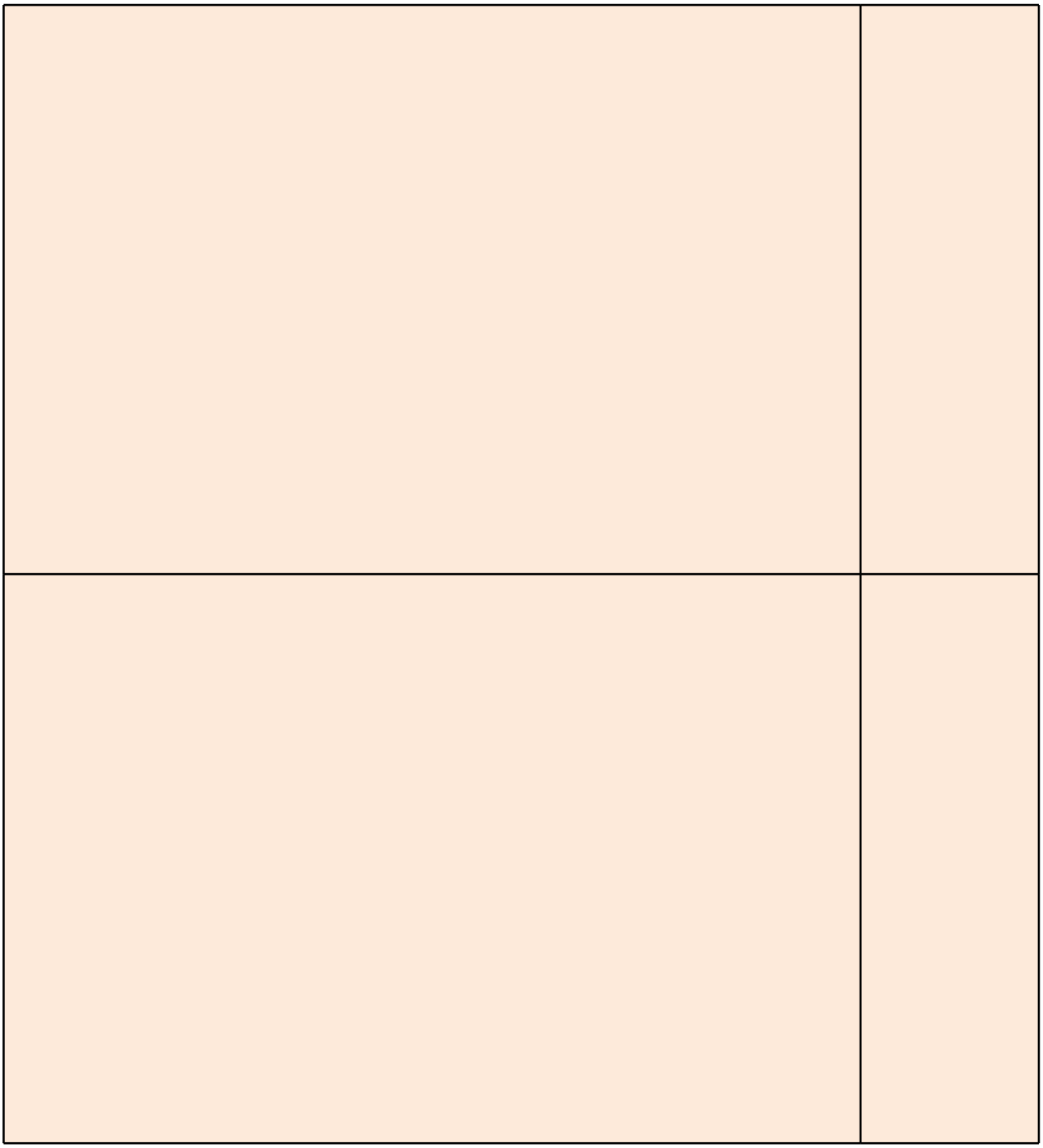












Kenttä
Ehdotus uudeksi tekstiksi
Muu mahdollinen kommentti
Ehdotuksen perustelut
Siirtymäsäännöstarve (ext)
Organisaatio

Ohjeistus
Kirjataan ehdotettu korvaava teksti. Korostukset voi tehdä fontin väreillä, alleviivauksella tai *kursiivilla*. Yliviivausta ei tule käyttää.
Kirjataan nimikkeeseen/vaatimukseen, pykälään, lukuun tai määräykseen kohdistuva kommentti. Korostukset voi tehdä fontin väreillä, alleviivauksella tai *kursiivilla*. Yliviivausta ei tule käyttää.
Kirjataan kommentin ja/tai uuden tekstin perustelut.
Kirjataan tunnistettu tarve mahdolliselle siirtymäsäännökselle. (Vain ulkoiset toimijat.)
Kirjataan kommentoiva organisaatio.
Yleisohje: Kun haluat kommentoida määräystä yleisesti, kirjaa kommenttisi määräyksen nimeä vastaavalle riville taulukossa. Vastaavasti voit kommentoida lukua, pykälää tai vaatimusta kohdistamalla kommentin sitä vastaavalle riville taulukossa.