IKT rekomendācijas aizsargājamo datu izmantošanai pētniecībā

Konsolidēts kopsavilkums par rekomendācijām aizsargājamo datu izmantošanai pētniecībā

2026. gada 15. maijā

The better the question. The better the answer. The better the world works.

Shape the future with confidence

Par sagatavotajām rekomendācijām

Šī prezentācija ir sagatavota Augstākās izglītības un zinātnes informācijas tehnoloģiju koplietošanas pakalpojumu centra īstenotā ANM projekta "Atbalsts atvērtās zinātnes ieviešanai praksē, kā arī izveidoti risinājumi zinātnes datu koplietošanai un dalībai ES atvērtajā zinātnes mākonī" ietvaros.

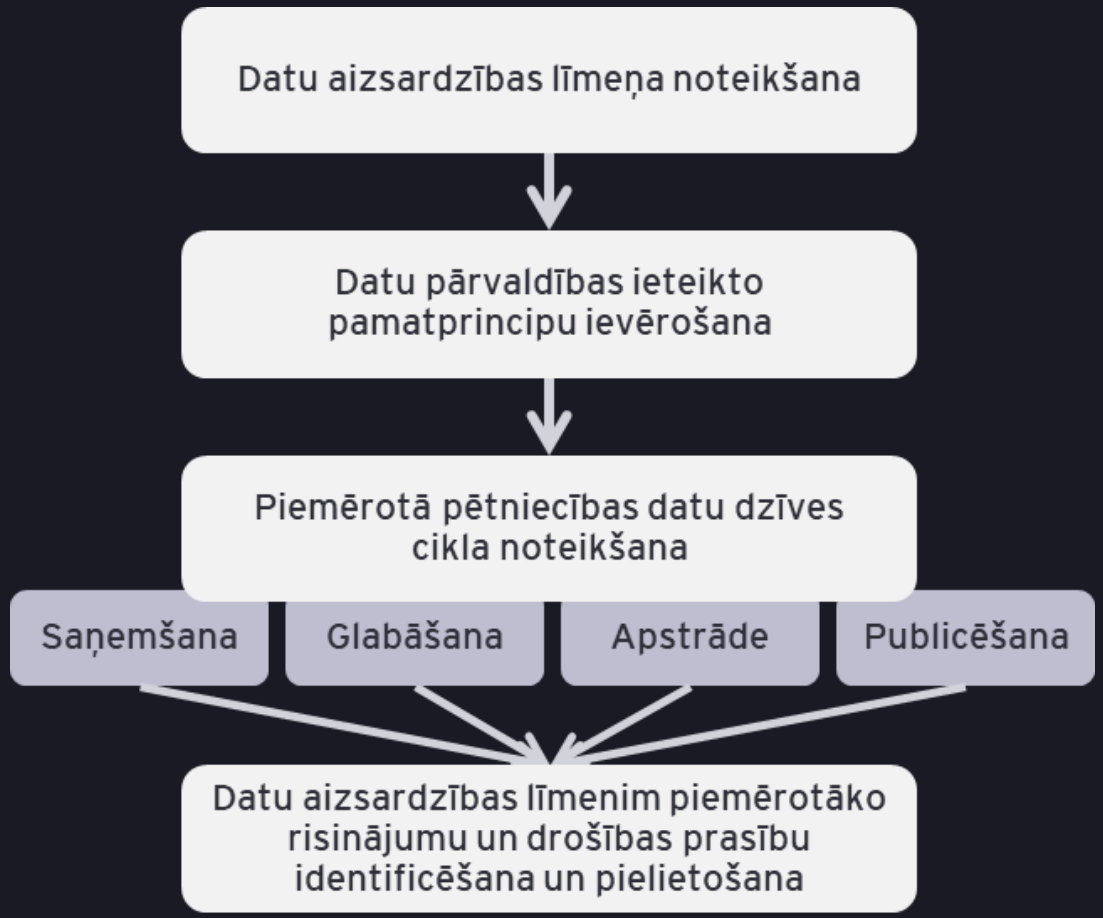
Tā apkopo galveno informāciju par ieteicamo pieeju aizsargājamo datu drošai izmantošanai pētniecībā. Pilns rekomendāciju kopums, detalizēts skaidrojums un piemērošanas loģika ir aprakstīta dokumentā "IKT risinājumi, prasības un procedūras drošai aizsargājamo datu izmantošanai pētniecībā"

Materiāls izstrādāts projekta "Atbalsts atvērtās zinātnes ieviešanai praksē, kā arī izveidoti risinājumi zinātnes datu koplietošanai un dalībai ES atvērtajā zinātnes mākonī" ietvaros (ANM projekta Nr. 2.1.3.1.i) ar Eiropas Savienības Atveseļošanas fonda un Latvijas valsts finansiālo atbalstu.

Praktisks ceļvedis drošai aizsargājamo datu izmantošanai pētniecībā

Pieaugot digitālo datu izmantošanai pētniecībā, pētnieki arvien biežāk strādā ar aizsargājamiem datiem. Tas nozīmē, ka līdztekus pētniecības vajadzībām ir jāspēj nodrošināt arī kontrolēta piekļuve, droša glabāšana, apstrāde un datu neizpaušana neatļautām personām.

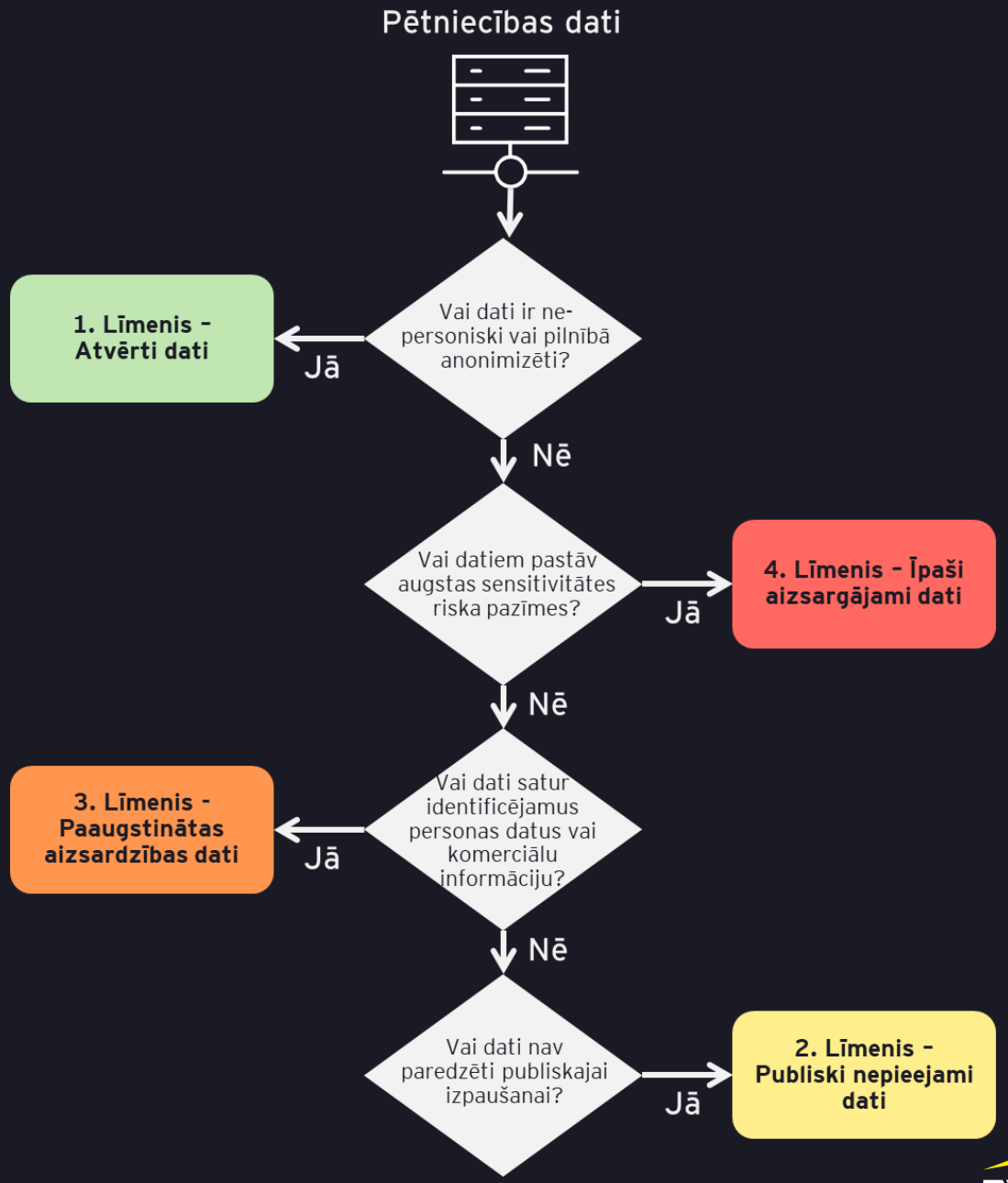
Sagatavotās rekomendācijas palīdz noteikt, kāda IKT pieeja, vide un kontroles ir nepieciešamas konkrētajā situācijā, lai dati tiktu izmantoti droši, bet datu devējiem būtu lielāka pārliecība par to nodošanu pētniecībai.



Datu aizsardzības līmeņa noteikšana

Dati pētniecībā var atšķirties pēc sensitivitātes un iespējamā riska to neatbilstošas izmantošanas vai izpaušanas gadījumā. Datu klasifikācija palīdz noteikt, kāds aizsardzības līmenis, glabāšanas vide un apstrādes nosacījumi katram datu veidam ir nepieciešami.

1. Līmenis – Atvērti dati	2. Līmenis – Publiski nepieejami dati	3. Līmenis - Paaugstinātas aizsardzības dati	4. Līmenis – Īpaši aizsargājami dati
Publiski , anonimizēti vai apkopoti dati, kuru izmantošana nerada būtisku risku.	Iekšēji pētniecības vai projektu dati ar zemu jutību, kuru neatļauta izpaušana radītu ierobežotu kaitējumu.	Identificējami personas dati, pseidonimizēti vai komerciāli jutīgi dati, kuriem nepieciešama kontrolēta piekļuve.	Ļoti sensitīvi dati, tostarp īpašu kategoriju personas dati, kuru izpaušana var radīt nopietnu kaitējumu.



Pamatprincipi datu pārvaldībai

Aizsargājamu datu (2., 3., un 4. līmeņa datu) izmantošanā neatkarīgi no izvēlētā risinājuma ir ieteicams balstīties uz vienotiem pārvaldības un drošības principiem. Tie kalpo kā kopīgs sākuma punkts drošākai un pārskatāmākai datu izmantošanai pētniecībā.

Ja datu aizsardzības līmeņa izvēles brīdī pastāv šaubas par piemērojamo pieeju, tad ieteicams izvēlēties stingrāk kontrolētus risinājums, nevis ērtāko variantu.

Sākotnējā nenoteiktībā ieteicams izvēlēties drošāki ceļu arī, ja tas ir sarežģītāks, jo kļūdaini izvēlēts risinājums ar nepietiekamām drošības kontrolēm paaugstina saistītos datu noplūšanas riskus.

Vispārīgie pamatprincipi aizsargājamo datu izmantošanai

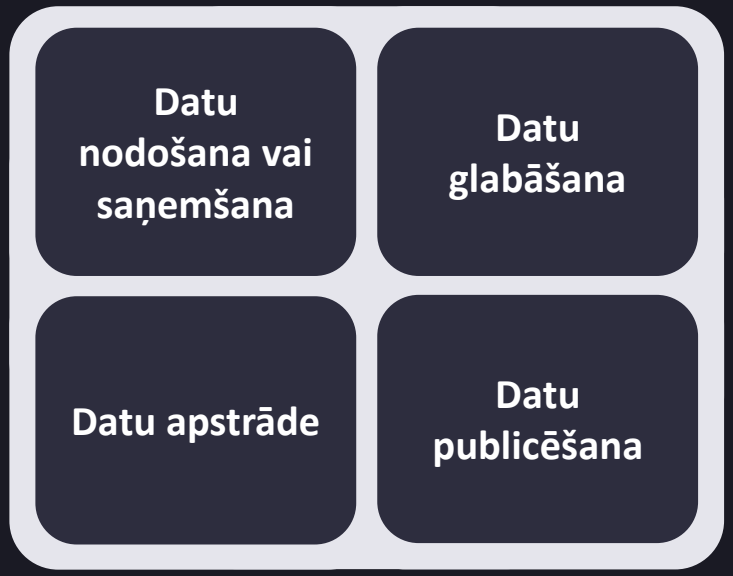
- **Datus drīkst izmantot tikai apstiprinātam un dokumentētam pētniecības mērķim.**
- **Datu pārvaldība jāīsteno atbilstoši FAIR principiem.**
- **Jāpiemēro datu minimizācijas princips.**
- **Piekļuve datiem piešķirama tikai autorizētām personām ar pamatotu nepieciešamību.**
- **Jānodrošina piekļuves un darbību žurnalēšana.**
- **Aizsargājamu datu glabāšanai, apstrādei un kopīgošanai priekšroka jādod institūcijas nodrošinātiem vai saskaņotiem risinājumiem.**
- **Datu glabāšanā un pārsūtīšanā jāizmanto šifrēšana.**
- **Datu pārvaldības procesā jāievēro datu devēja vai normatīvā regulējuma noteiktie papildu ierobežojumi.**
- **Jānosaka datu glabāšanas termiņš, pārskatīšanas kārtība un dzēšanas vai arhivēšanas nosacījumi.**

Pētniecības datu dzīves cikls

Pētniecības datu pārvaldība jāvērtē ne tikai pēc datu veida vai aizsardzības līmeņa, bet arī pēc tā, kurā dzīves cikla posmā dati atrodas un kā tie konkrētajā brīdī tiek izmantoti.

Sagatavotā rekomendāciju struktūra balstās gan uz pētniecības dzīves cikla posmiem, gan uz trim datu pamatstāvokļiem, kas raksturo atšķirīgus riskus un piemērojamos risinājumus.

Pētniecības datu dzīves cikls



Datu pamatstāvoklis

Dati pārsūtīšanā *"data in transit"*	Galvenais uzsvars uz drošiem nodošanas kanāliem un kontroli pār datu pārvietošanu.
Dati glabāšanā *"data at rest"*	Galvenais uzsvars uz piemērotu glabāšanas vidi, piekļuves kontroli, rezerves kopijām un datu saglabāšanas noteikumiem.
Dati apstrādē / izmantošanā *"data in use"*	Galvenais uzsvars uz to, kur un kā dati tiek analizēti, kam ir piekļuve videi un vai iespējams kontrolēt datu iznešanu.

Datu nodošana vai saņemšana

Droša nodošana nozīmē ne tikai drošu tehnisko kanālu, bet arī skaidru vienošanos par to, kādi dati tiek nodoti, kam tie tiek nodoti, kādā formā, uz kādu vidi, uz cik ilgu laiku un ar kādiem ierobežojumiem.

Ieteicamā pieeja

Priekšroka dodama tiešai datu nodošanai uz institucionāli pārvaldītu vai iepriekš saskaņotu vidi, izmantojot drošus datu apmaiņas risinājumus.

No kā izvairīties

Izvairīties no e-pasta, personīgi pārvaldītiem mākoņrisinājumiem un nevajadzīgu lokālu datu kopiju veidošanas ārpus kontrolētas vides.

Galvenie pamatprincipi datu nodošanas vai saņemšanas laikā

- **Datu nodošanai jāizmanto pārvaldīti, autentificēti un auditējami tehnoloģiskie risinājumi.**
- **Ja dati paredzēti glabāšanai vai apstrādei konkrētā apstiprinātā vidē, tie pēc iespējas jānogādā tieši šajā vidē.**
- **Ja tiek izmantotas pagaidu augšupielādes vai starpmehānismi, pēc datu saņemšanas piekļuve tiem jāslēdz vai kopijas jādzēš.**
- **Paaugstināta riska datu nodošanai jāizmanto šifrēta pārsūtīšana un droša atslēgu apmaiņa.**
- **Izvēlētais risinājums jāvērtē pēc tā, vai tas atbilst datu devēja nosacījumiem, institūcijas prasībām un konkrētā datu līmeņa vajadzībām.**

Detalizētāka informācija par piemērotāko praksi atrodama kopējā rekomendāciju dokumentā.

Datu glabāšana un kopīgošana

Datu glabāšanas un kopīgošanas laikā galvenais mērķis ir nodrošināt, ka dati ir pieejami attiecīgajām personām pētniecības vajadzībām, vienlaikus saglabājot kontroli pār piekļuvi, kopiju veidošanos un datu pārvietošanu ārpus pārvaldītas vides.

Ieteicamā pieeja

Priekšroka dodama vienotai, institucionāli pārvaldītai videi, kur dati tiek glabāti un kopīgoti ar kontrolētu piekļuvi tikai iesaistītajām personām.

No kā izvairīties

Izvairīties no situācijām, kad datu glabāšana notiek pētnieka darba stacijā vai personīgi pārvaldītā glabāšanas risinājumā. Izvairīties no datu kopīgošanas, izmantojot publiskas saites vai piešķirot plašākas piekļuves tiesības, nekā tas ir nepieciešams.

Galvenie pamatprincipi datu glabāšanas un kopīgošanas laikā

- **Projektam nepieciešams noteikt vienu galveno glabāšanas vidi un priekšroku dot institucionāli pārvaldītam vai saskaņotam risinājumam ar piekļuves kontroli un projektu nodalīšanu.**
- **Darba kopijas uz gala iekārtām pieļaujamas tikai izņēmuma gadījumos un nedrīkst kļūt par projekta galveno datu glabāšanas risinājumu.**
- **Datus ieteicams kopīgot tajā pašā vidē, kur tie tiek glabāti vai apstrādāti, lai mazinātu papildu kopiju un nekontrolētu datu aprites risku.**
- **Piekļuve kopīgotajiem datiem jāpiešķir tikai konkrētām personām vai skaidri definētām grupām, neizmantojot publiskas saites vai plašākas tiesības, nekā nepieciešams darba uzdevumu veikšanai.**
- **Augstākiem datu aizsardzības līmeņiem jānodrošina iespēja kontrolēt datu lejupielādi, sinhronizāciju, eksportu un citu datu iznešanu no pārvaldītās vides.**

Detalizētāka informācija par piemērotāko praksi atrodama kopējā rekomendāciju dokumentā.

Datu apstrāde

Datu apstrādes posmā svarīgākais aspekts nav tas, kuru rīku izmantot, bet gan vai dati tiek apstrādāti atbilstošā un pietiekami kontrolētā vidē. Jo sensitīvāki ir šie dati, jo svarīgāk ir nodrošināt, ka piekļuve un datu iznešana ārpus rīka ir pārvaldīta un pārskatāma.

Ieteicamā pieeja

Priekšroka dodama institucionāli nodrošinātai, institucionāli apstiprinātai vai citādi kontrolētai apstrādes videi, kas ir piemērota konkrētajam datu aizsardzības līmenim un ļauj pārvaldīt piekļuvi un datu iznešanu no vides.

No kā izvairīties

Izvairīties no aizsargājamu datu apstrādes personīgās, neizvērtētās vai publiskās vidēs, kur nav iespējams kontrolēt piekļuvi, datu apriti un iespējamu datu nodošanu trešajām pusēm.

Galvenie pamatprincipi datu apstrādes laikā

- **Priekšroka dodama institucionāli nodrošinātiem vai institucionāli apstiprinātiem apstrādes risinājumiem.**
- **Aizsargājamu datu apstrādei nevajadzētu izmantot publiskus vai neizvērtētus rīkus, kas var radīt nekontrolētu datu nodošanu vai sekundāru apstrādi.**
- **Datu apstrādes laikā ieteicams pēc iespējas samazināt datu pārvietošanu starp vairākām apstrādes vidēm.**
- **Ja analīzes laikā nepieciešams pievienot papildu programmatūru, tas jādara tikai kontrolētā un iepriekš izvērtētā kārtībā.**
- **Ja apstrādes laikā dati tiek sasaistīti ar citām datu kopām, būtiski pārveidoti vai izmantoti tā, ka var pieaugt identificēšanas, izpaušanas vai citas neatļautas izmantošanas risks, apstrādes pieeja jāizvērtē atkārtoti.**

Detalizētāka informācija par piemērotāko praksi atrodama kopējā rekomendāciju dokumentā.

Datu publicēšana

Datu publicēšanas posmā galvenais jautājums nav tikai, vai dati tiks publicēti, bet arī kādā apjomā, kādā formā un ar kādu piekļuves modeli tas ir pieļaujams.

Publicēšana ne vienmēr nozīmē pilnas datu kopas publisku pieejamību, jo atkarībā no datu satura un ierobežojumiem tā var notikt arī ar ierobežotu vai kontrolētu piekļuvi, tikai metadatu vai tikai rezultātu veidā.

Datu publicēšanas veidi

Atklāta publicēšana	**Publicēšana ar embargo**	**Ierobežotas piekļuves publicēšana**
Kontrolētas piekļuves publicēšana	**Tikai metadatu publicēšana**	**Tikai rezultātu publicēšana**

Ieteicamā pieeja

Pirms datu publicēšanas ieteicams izvērtēt piemērotāko publicēšanas modeli, nodrošināt nepieciešamās atļaujas, sagatavot datus un metadatus drošai publicēšanai un izmantot uzticamu, institucionāli pārvaldītu vai saskaņotu publicēšanas vidi.

No kā izvairīties

Izvairīties no pieņēmuma, ka publicēšana vienmēr nozīmē pilnas datu kopas atklātu publicēšanu, kā arī no publicēšanas pirms ir izvērtēti juridiskie, līgumiskie, konfidencialitātes un personas datu aizsardzības ierobežojumi.

Detalizētāka informācija par piemērotāko praksi atrodama kopējā rekomendāciju dokumentā.

Drošas apstrādes vide izmantošana

Drošas apstrādes vide ir īpaši svarīga gadījumos, kad pētniecībā tiek izmantoti dati, kuru neatļauta izpaušana var radīt risku personām, datu devējiem vai institūcijai. Šāda vide palīdz nodrošināt, ka dati tiek glabāti, apstrādāti un analizēti kontrolēti, nevis brīvi kopēti vai iznesti ārpus apstiprinātās vides.

Droša apstrādes vide ir kontrolēta un nodalīta tehnoloģiskā vide, kurā pētnieki var piekļūt aizsargājamiem datiem, tos glabāt un analizēt, ar ierobežojumiem datus iznest ārpus tās.

Kādos gadījumos droša apstrādes vide ir nepieciešama?

2. Līmeņa datiem

Droša apstrādes vide ir vēlama, bet ne vienmēr obligāta. Iespējama arī cita ar pārvaldīta vide, kas nodrošina iepriekšējās sadaļās definētās drošības prasības.

3. Līmeņa datiem

Droša apstrādes vide ir ieteicamā noklusējuma pieeja. Iespējams izmantot līdzvērtīgi stingri kontrolētu vidi, ja veikta tās drošības kritēriju izvērtēšana un atbilstoša konfigurēšana.

4. Līmeņa datiem

Droša apstrādes vide ir uzskatāma par noklusējuma prasību.

Detalizētāka informācija par piemērotāko praksi atrodama kopējā rekomendāciju dokumentā.

Minimālās tehnoloģiskās kontroles

Aizsargājamu datu drošība nav atkarīga tikai no izvēlētā produkta vai platformas, bet no tā, vai konkrētais risinājums spēj nodrošināt attiecīgajam datu aizsardzības līmenim nepieciešamās kontroles. Tāpēc tehnoloģiskais risinājums jāvērtē pēc tā drošības un pārvaldības spējām, nevis tikai pēc lietošanas ērtuma vai ierastās prakses.

Nepieciešams izvairīties no pieejas, kur risinājuma piemērotība tiek pieņemta pēc produkta nosaukuma vai ierastās prakses, neizvērtējot, kā risinājums nodrošina piekļuves kontroli, datu aizsardzību un datu iznešanas ierobežošanu.

Produktu līmeņa drošības konfigurācijas izvērtējumam ieteicams balstīties uz ražotāja dokumentāciju un, kur pieejams, uz *CIS Benchmarks* vai citiem līdzvērtīgiem nozares atzītiem drošas konfigurācijas resursiem.

Galvenie tehniskās kontroles virzieni

Piekļuves kontrole un identitāte

Individuāli lietotāju konti, lomu balstīta piekļuve, daudzfaktoru autentifikācija un piekļuves ierobežošana tikai autorizētiem lietotājiem.

Datu aizsardzība un nodalīšana

Šifrēšana pārsūtīšanā un glabāšanā, datu rezidences ievērošana un loģiska datu nodalīšana starp projektiem.

Pārvaldīta vide

Institucionāli pārvaldīta konfigurācija, apstiprināta programmatūra, drošības atjauninājumi un rezerves kopēšana.

Auditējamība un uzraudzība

Piekļuves un darbību žurnalēšana, pārskatāma uzskaite un iespēja izsekot darbam ar datiem.

Datu iznešanas kontrole

Lejupielādes, kopēšanas, sinhronizācijas un eksporta ierobežošana, īpaši 3. un 4. līmeņa datiem.

Detalizētāka informācija par piemērotāko praksi atrodama kopējā rekomendāciju dokumentā.

Materiāls izstrādāts projekta «Atbalsts atvērtās zinātnes ieviešanai praksē, kā arī izveidoti risinājumi zinātnes datu koplietošanai un dalībai ES atvērtajā zinātnes mākonī» ietvaros (ANM projekta Nr. 2.1.3.1.i) ar Eiropas Savienības Atveseļošanas fonda un Latvijas valsts finansiālo atbalstu