AIZSARDZĪBAS MINISTRIJA

Nacionālais kiberdrošības centrs

VADLĪNIJAS 2. PIELIKUMA AIZPILDĪŠANAI

(MK noteikumi Nr. 368)

SATURS

Nacionālais kiberdrošības centrs (NKDC) ir nacionālā kompetentā institūcija, kas darbojas Aizsardzības ministrijā (AM) kā vienotais kontaktpunkts kiberdrošības jautājumos. NKDC īsteno nacionālo kiberdrošības pārraudzību, izstrādā un koordinē nacionālās kiberdrošības politikas iniciatīvas, kā arī nodrošina starptautisko sadarbību savas kompetences ietvaros.

Saskaņā ar **MK noteikumu Nr. 368** 5. punktu:

- 5.1. – VARAM vērtē atbilstību normatīvajiem aktiem informācijas un komunikācijas tehnoloģiju (turpmāk IKT) attīstības jomā;
- **5.2.** – nozares ministrija vērtē atbilstību politikas prioritātēm;
- **5.3.** – **Aizsardzības ministrija** vērtē **plānotos informācijas sistēmas drošības pasākumus**.

Aizpildot anketu, iestādēm jāņem vērā, ka NKDC vērtē iesniegto informāciju no kiberdrošības viedokļa.

Vadlīniju mērķis ir sniegt atbalstu iestādēm, aizpildot **Ministru kabineta noteikumu Nr. 368 (04.07.2023.)** *"Informācijas sistēmu un to darbībai nepieciešamo informācijas un komunikācijas tehnoloģiju resursu un pakalpojumu attīstības aktivitāšu un likvidēšanas uzraudzības kārtība"* 2. pielikuma anketu.

Vadlīnijas apkopo:

- tipiskās kļūdas, kas konstatētas izvērtēšanas gaitā;
- anketas aizpildīšanas labo praksi ar praktiskiem piemēriem.

VISPĀRĪGIE PRINCIPI, AIZPILDOT ANKETU

1. **Terminoloģijas viennozīmība – jāizvairās jaukt jēdzienus "informācijas sistēma" un "programmatūra".**
   - Jālieto normatīvajos aktos noteiktie termini ("informācijas sistēma", "IKT resurss", "pakalpojums").
   - Jāizvairās no neformāliem jēdzieniem un sinonīmiem vai saīsinātiem apzīmējumus (piem. "programmatūra" kā sinonīms informācijas sistēmai).

2. **Saīsinājumi – pirmo reizi tekstā jāatšifrē, turpmāk jālieto nemainīgi.**
   - Saīsinājumus norāda anketas sākumā vai vietā, kur tie pirmo reizi izmantoti.
   - Viena sistēma visā tekstā jāapzīmē ar vienotu nosaukumu vai saīsinājumu.

3. **Pamatoti apgalvojumi**
   - Jebkurš postulāts (piem., "risinājums būs augstas pieejamības") jāpamato ar konkrētiem parametriem (piem., pieejamība 99.982%, atjaunošanas laiks (RTO): ≤ 60 minūtes, reakcijas laiks incidenta gadījumā ≤ 15 min).
   - Jāizvairās no vispārīgām frāzēm; aprakstos jānorāda fakti un tehniskie parametri. Ja iespējams, jāpievieno norāde uz informācijas avotu.

4. **Pilnīga atbilde, arī ja dati vēl nav pieejami**
   - Ja informācija vēl nav zināma, jānorāda, kad tā būs pieejama (piem., "tiks noteikta projektēšanas fāzē 2026. gada I ceturksnī").
   - Ja VIRSIS identifikators nav piešķirts, jānorāda "nav piešķirts" vai "tiks piešķirts pēc sistēmas nodošanas lietošanā".

5. **Budžets un pamatojums – finansējuma apjoms jāsaskaņo ar 3.2. punktā norādīto indikatīvo finansējumu, sniedzot skaidrojumu par starpībām un to iemesliem.**
   - Ja starpība starp sadaļām (piem., 3.2. un 8. punkts) pastāv, jānorāda, kādām darbībām vai mērķiem tā paredzēta.

6. **Tehnisko alternatīvu izvērtējums – vēlams norādīt, vai ir analizēti citi risinājumi un kāpēc izvēlēts konkrētais.**
   - Jāsniedz īss apraksts par vērtētajām alternatīvām un atteikuma pamatojumu.

7. **Atsauces – informāciju nevajadzētu sniegt tikai kā ārējas saites, jo to saturs var mainīties.**
   - Saites drīkst pievienot, bet aprakstam jābūt pašpietiekamam, lai to varētu izvērtēt arī bez ārēja resursa.

8. **Kiberdrošība**
   - Informācija par drošības pārvaldību, testiem un kontrolēm jānorāda konkrēti, nevis vispārīgi.
   - Aprakstam jābūt pietiekami detalizētam, lai izvērtētājs varētu objektīvi spriest par atbilstību normatīvajām prasībām.

9. **Lieku atkārtojumu un liekvārdības novēršana**
   - Nav nepieciešams atkārtot prasību tekstu no anketas – jāsniedz tieši prasītā informācija.
   - Ja kāda informācija šobrīd nav zināma, jānorāda, ka tā tiks precizēta konkrētā attīstības posmā.

3.1. RISINĀMĀ PROBLĒMA

Kas jānorāda

Īss un konkrēts apraksts par situāciju un problēmu, kuru nepieciešams atrisināt, **nevis** jau paredzēto risinājumu.

Tipiskās kļūdas

- Problēma tiek aizstāta ar gatavā risinājuma aprakstu.
- Nav skaidrots, kāpēc aktivitāte ir nepieciešama.
- Pārlieku vispārīgi formulējumi ("Nepieciešams modernizēt sistēmu").

Labā prakse

- Aprakstīt biznesa vajadzību, normatīvo aktu prasību vai procesa trūkumu.
- Piemērs: "Esošajā sistēmā nav iespējas elektroniski iesniegt dokumentus, kā to paredz MK noteikumi Nr. XYZ, radot kavējumus lietotāju apkalpošanā."

3.2. GALVENĀS DARBĪBAS

Kas jānorāda

Visas būtiskās darbības aktivitātes īstenošanai, katrai paredzot indikatīvu finansējumu.

Tipiskās kļūdas

- Nav finansējuma sadalījuma pa darbībām.
- Kiberdrošības, testēšanas un kvalitātes nodrošināšanas darbības nav iekļautas.

Labā prakse

- Norādīt finansējumu arī drošības pārbaudēm un lietotāju apmācībai.
- Piemērs:
  - Funkcionalitātes izstrāde, ieviešana– 50 000 EUR
  - Drošības tests un audits – 8 000 EUR
  - Lietotāju apmācība – 5 000 EUR

3.3. SAGAIDĀMIE REZULTĀTI

Kas jānorāda

Konkrēti, izmērāmi un pārbaudāmi rezultāti, kas sasniedzami aktivitātes noslēgumā.

Tipiskās kļūdas

- Rezultāti ir vispārīgi ("Sistēma būs uzlabota").
- Nav mērīšanas kritēriju.

Labā prakse

- Lietot konkrētus rādītājus:
  - "Samazināts dokumentu iesniegšanas laiks no 5 uz 2 dienām"
  - "Samazināts manuālo datu ievades apjoms par 80 %".
  - "Nodrošināta atbilstība MK noteikumiem Nr. XYZ attiecībā uz e-rēķinu apstrādi."

4. IETEKME UZ CITĀM INFORMĀCIJAS SISTĒMĀM

Šī sadaļa ir būtiska, lai izvērtētu projekta radītās pārmaiņas esošajā IKT vidē, identificētu ietekmētās sistēmas, datu apmaiņu un koplietošanas komponentes. Aizpildot, jānodrošina saskaņotība ar 3. punktā sniegto informāciju.

4.1. Aizvietojamās un ietekmētās informācijas sistēmas

Kas jānorāda

- Katra ietekmētā informācijas sistēma (tai skaitā aizvietojamās vai likvidējamās sistēmas), kas tiks skarta projekta īstenošanas rezultātā.
- Ietekmes apraksts katrai sistēmai (ieteicams izmantot klasifikāciju):
  - **Augsta ietekme** – funkcionalitātes darbības pārtraukšana vai būtiska izmaiņa.
  - **Vidēja ietekme** – izmaiņas integrācijās, API, datu struktūrā.
  - **Minimāla ietekme** – neliela konfigurācijas vai saskarņu pielāgošana.
- Norādīt VIRSIS identifikatoru katrai sistēmai.
- Ja tiek norādīts "Nav ietekmēto sistēmu", jāsniedz pamatojums, kāpēc projekta rezultātā netiks ietekmēta neviena sistēma (ņemot vērā, ka aizvietojamās sistēmas arī ir uzskatāmas par ietekmētām).

Tipiskās kļūdas

- Norādīts "Nav ietekmēto sistēmu", lai gan 3. punktā ir minētas saistītās vai aizvietojamās sistēmas.
- Ietekme aprakstīta vispārīgi ("būs izmaiņas"), bez norādes uz to apjomu vai būtību.
- Nav sasaistes ar VIRSIS identifikatoriem.
- Vienā rindā uzskaitītas vairākas sistēmas.

Piemērs

- "IS 'Personas reģistrs' (VIRSIS ID 1234) – augsta ietekme: sistēma tiks aizvietota ar jaunu risinājumu. Migrācija plānota līdz 2025. gada beigām."
- "IS 'Datu analītikas platforma' (VIRSIS ID 5678) – vidēja ietekme: izmaiņas API datu struktūrā, paredzot jaunu lauku pievienošanu."

4.2. Dati, kas tiks saņemti vai nodoti citām informācijas sistēmām

Kas jānorāda

- Detalizēts datu apmaiņas apraksts pa sistēmām (viena rinda – viena sistēma).
- Norādīt, vai dati tiks **saņemti** vai **nodoti**, kā arī datu veidu (piem., personas dati, finanšu dati, reģistra ieraksti).
- Norādīt attiecīgās sistēmas VIRSIS identifikatoru.
- Ja datu apmaiņa mainās (piem., datu formāts, biežums, pārraides kanāls), tas jāapraksta.

Tipiskās kļūdas

- Apraksts ir vispārīgs ("notiks datu apmaiņa"), nenorādot sistēmas vai datu saturu.
- Trūkst VIRSIS identifikatoru.
- Netiek norādītas izmaiņas esošajā datu apmaiņā.

Piemērs

- "IS 'Valsts nodevu reģistrs' (VIRSIS ID 4321) – tiks nodoti maksājumu dati XML formātā reizi dienā, izmantojot drošu API kanālu (TLS 1.3)."
- "IS 'Pilsonības un migrācijas lietu reģistrs' (VIRSIS ID 8765) – tiks saņemti personas identifikācijas dati reāllaikā, izmantojot X-Road starpniecību."

4.3. Informācija par attīstāmām koplietošanas komponentēm un pakalpojumiem

Kas jānorāda

- Apraksts par plānotajām koplietošanas komponentēm (piem., datu centri, reģistri, autentifikācijas vai maksājumu moduļi), kuras varētu izmantot citas iestādes.
- Norādīt VIRSIS identifikatoru, ja tas ir piešķirts.
- Aprakstam jābūt līdz 500 rakstzīmēm katrai komponentei, nodalot tās atsevišķās rindās.
- Jāuzsver, kā šīs komponentes veicinās IKT resursu koplietošanu un efektīvu izmantošanu.

Tipiskās kļūdas

- Netiek norādītas koplietošanas komponentes, lai gan projektā tiek izstrādāti risinājumi ar potenciālu lietojumu ārpus konkrētās iestādes.
- Apraksts nav sasaistīts ar VIRSIS.
- Apraksts pārsniedz 500 rakstzīmes vai satur lieku tehnisko detaļu.

Piemērs

- "Vienotais autentifikācijas modulis (VIRSIS ID 9988) – paredzēts valsts un pašvaldību IS lietotāju autentifikācijai, nodrošinot OAuth2 un eID autentifikācijas atbalstu."
- "Datu koplietošanas API komponente – nodrošina standartizētu piekļuvi atvērtajiem datiem CSV un JSON formātos."

5.1. DROŠĪBAS PĀRVALDĪBA

Šis punkts apraksta izstrādājamās vai attīstāmās informācijas sistēmas tehnoloģiskos aspektus, īpašu uzmanību pievēršot kiberdrošībai, piekļūstamībai, datu pārvaldībai un datu aprites risinājumiem.

Aizpildot, jāievēro, ka aprakstam jābūt pietiekami detalizētam, lai to varētu izvērtēt gan tehniski, gan atbilstības ziņā normatīvajiem aktiem (MK noteikumi, likumi).

5.1.1. Atbildīgā persona

Kas jānorāda fiziska persona ar vārdu, uzvārdu, amatu un kontaktinformāciju, kas atbild par drošību projekta laikā un pēc ieviešanas.

Tipiskās kļūdas

- Norādīta tikai organizācija vai struktūrvienība.
- Nav kontaktinformācijas.

Piemērs

- "Atbildīgā persona: Jānis Bērziņš, Informācijas drošības vadītājs, Iestādes nosaukums. Drošības pārvaldības organizēšanā iesaistīts ārpakalpojumu sniedzējs: SIA "Drošais Tīkls" – SOC pakalpojumi un incidentu pārvaldība.""

5.1.2. Drošības kategorija un pamatojums

Kas jānorāda Pieejamības, integritātes un konfidencialitātes līmenis atbilstoši MK noteikumiem.

- Pamatojums katram līmenim, balstoties uz datu kritiskumu un pakalpojuma nozīmi.

Tipiskās kļūdas

- Norāda tikai līmeni (“Augsta”) bez pamatojuma.
- Pamatojums ir deklaratīvs (“jo dati ir svarīgi”);
- Nav sasaistes ar MK noteikumu metodiku.

Piemērs

- Saskaņā ar MK noteikumiem Minimālās kiberdrošības prasības un to 5. pielikuma metodiku informācijas sistēma uzskatāma par B klases (pamata drošības) informācijas sistēmu.
  - “Pieejamība – C klase” (sistēma nodrošina iekšējo datu apstrādi, kuras pārtraukums līdz 24 h nerada kritiskus zaudējumus)
  - “Integritāte – B klase” (jebkuras datu izmaiņas var radīt juridiskas sekas).
  - “Konfidencialitāte – C klase (neapstrādā personas datus vai komercnoslēpumu).”

5.1.3. Drošības pārvaldības organizēšanas kārtība un tehniskie drošības pasākumi

Kas jānorāda

- Konkrēta informācija par drošības pārvaldības organizēšanu šai attīstības aktivitātei. Piem:
  - Sistēmas īpašnieks / atbildīgā amatpersona.
  - Drošības vadītājs vai koordinētājs.
  - Administratori un lietotāju grupas.
  - Ārpakalpojuma sniedzēji, ja piemērojams
  - Galvenie organizatoriskie pasākumi (politikas, procedūras, atbildības sadale).
- Tehniskie drošības pasākumi, kas tiks ieviesti šai aktivitāte. Piem:
  - Tīkla aizsardzība (piem., ugunsmūri, tīkla segmentēšana, IDS/IPS).
  - Piekļuves autentifikācijas un autorizācijas mehānismi (piem., MFA, PAM).
  - Datu aizsardzība (piem., šifrēšana AES-256, TLS 1.3).
  - WAF publiskajiem servisiem.
  - Rezerves kopiju izveide un glabāšanas risinājumi.
- Ja atsaucas uz iekšējiem normatīvajiem aktiem, jānorāda to apstiprināšanas un pēdējās aktualizācijas datums.
- Ja risinājums izvietots trešās puses infrastruktūrā (piem., LVRTC), jānorāda, kā tehniskie pasākumi tiek integrēti ar tās drošības prasībām.

Tipiskās kļūdas

- Vispārīgs apraksts bez saistības ar konkrēto sistēmu vai projektu.
- Minēti tikai organizatoriskie aspekti, nav konkrētu tehnisko drošības pasākumu un risinājumu vai otrādi.
- Ir atsauce uz iekšējiem normatīvajiem aktiem, kas praksē ir novecojuši un nav aktualizēti vai pieminēta “ISO 27001 sertifikācija” bez konkrētas drošības pārvaldības apraksta.
- Drošības kontroles sajauktas ar tehniskajiem pasākumiem.

Labā prakse

- Apraksts konkrētās sistēmas drošības pārvaldības organizēšanas kārtībai un tehniskajiem risinājumiem.
- Trešās puses infrastruktūras drošības elementi ir saskaņoti ar projekta risinājumiem.
- Tehniskie pasākumi sasaistīti ar noteiktām riska grupām vai draudu scenārijiem.

Piemērs

IS drošības pārvaldību nodrošina satura, lietojuma un infrastruktūras aizbildņi, kuru atbildības sadalījums noteikts iekšējos noteikumos (aktualizēti 15.05.2024).

- Satura aizbildnis – par datiem un metadatiem
- Lietojuma aizbildnis – par lietotāju pārvaldību, rezerves kopijām.
- Infrastruktūras aizbildnis – par tehnisko vidi un drošību.

Tehniskie pasākumi:

- MFA administratīvajiem kontiem
- Ugunsmūru deny-all politika
- IDS Suricata
- AES-256 un TLS 1.3 šifrēšana
- WAF publiskajiem API,
- SIEM monitorings

5.1.4. Plānotās drošības pārbaudes un citas īstenojamās drošības kontroles

Kas jānorāda

- Pārbaudes:
  - Veids (piem., ielaušanās testi, konfigurācijas pārbaudes, ievainojamību skenēšana, koda pārbaudes, neatkarīgi auditi).
  - Metodoloģija/standarts (piem., OWASP, NIST SP 800-115, ISO/IEC 27001, CIS Controls).
  - Biežums (pirms ieviešanas, pēc lielām izmaiņām, reizi gadā utt.).
  - Veicējs (iekšējais resurss, ārpakalpojuma sniedzējs, sertificēts auditors).
- Drošības kontroles (uzraudzības un atbilstības mehānismi, nevis tehniskie elementi):
  - Pieejas tiesību regulāra pārskatīšana.
  - Drošības notikumu žurnālu analīze.
  - Incidentu pārvaldības gatavības pārbaudes.
  - DNP un atjaunošanas plānu testēšana.
  - Konfigurācijas izmaiņu pārvaldības audits.
  - Rezerves kopiju atjaunošanas pārbaude.

Tipiskās kļūdas

- Vispārīgs formulējums (“tiks veiktas pārbaudes”) bez deatalizācijas.
- Metodoloģija un biežums nav norādīti.
- Pārbaudes sajauktas ar tehniskajiem pasākumiem.
- Nav skaidrs, kas pārbaudes veiks.
- Nav iekļautas drošības kontroles kā uzraudzības mehānismi.

Labā prakse

- Skaidri nodalīt pārbaudes no tehniskajiem pasākumiem.
- Norādīt precīzu veidu, metodoloģiju, biežumu un atbildīgo pusi.
- Iekļaut gan ieviešanas, gan ekspluatācijas laikā veicamās pārbaudes.
- Drošības kontroles formulēt kā pastāvīgus uzraudzības procesus.

Piemērs

Pārbaudes pirms ieviešanas:

- Ielaušanās testi pēc OWASP metodoloģijas (veic sertificēts ārpakalpojuma sniedzējs).
- Konfigurācijas pārbaudes (iekšējie drošības speciālisti).
- Koda pārbaudes (iekšējais code review process katram laidienam).

Ekspluatācijas laikā:

- Ievainojamību skenēšana pirms katra lielā laidiena un ne retāk kā reizi gadā.
- Neatkarīgs drošības audits reizi 2 gados.
- DNP un atjaunošanas testi reizi gadā vai pēc būtiskām izmaiņām.

Drošības kontroles:

- Pieejas tiesību pārskatīšana reizi 6 mēnešos.
- Drošības notikumu žurnālu pārskatīšana reizi nedēļā.
- Incidentu pārvaldības galda mācības reizi gadā.
- Rezerves kopiju atjaunošanas pārbaude reizi ceturksnī.
- Konfigurācijas izmaiņu audits vismaz reizi ceturksnī.

5.1.A UN 5.1.P

Kas jānorāda

- **5.1.a** – apliecinājums par atbilstību MK noteikumiem Nr. 442. (pašreiz ir pieņemti MK noteikumi Minimālās kiberdrošības prasības, kas aizstāj MK 442, attiecīgi šis apliecinājums attiecināms uz MK noteikumiem Minimālās kiberdrošības prasības)
- **5.1.p** – noviržu saraksts, pamatojums un novēršanas plāns.

Tipiskās kļūdas

- Novirzes netiek pamatotas.
- Nav norādīts termiņš novēršanai.
- Ja noviržu nav, netiek norādīts "Noviržu nav"

Labā prakse

"Novirze: MFA netiek ieviesta visiem administratoriem. Pamatojums: mantotā sistēma bez MFA atbalsta. Novēršanas plāns: MFA ieviešana līdz 2026. gada 30. jūnijam."

5.2. PIEKĻŪSTAMĪBAS NODROŠINĀŠANA

Kas jānorāda

- **Konkrēti piekļūstamības risinājumi**, kas tiks īstenoti projekta ietvaros, nevis tikai atsauce uz normatīvajiem aktiem vai standartiem.
- **Piekļūstamības prasību avots**:
  - MK 2020. gada 14. jūlija noteikumi Nr. 445 *"Kārtība, kādā iestādes ievieto informāciju internetā"*.
  - LVS EN 301 549:2021 *"IKT produktu un pakalpojumu pieejamības prasības"*.
  - WCAG 2.1 AA līmeņa vadlīnijas.
- **Kā tiks pārbaudīta atbilstība** (piem., manuālā testēšana, automātiskie rīki, lietotāju testēšana ar palīgtehnoloģijām).
- **Kad notiks piekļūstamības testēšana** (piem., akcepttestēšanas posmā, pēc būtiskām izmaiņām).
- **Ja sistēma nav publiski pieejama internetā**, tomēr jāizvērtē piekļūstamības aspekti iekšējai lietotāju grupai (piem., cilvēki ar funkcionāliem traucējumiem organizācijā).
- **Tehniskajā specifikācijā** jāparedz piekļūstamības prasības jau pirms izstrādes uzsākšanas.

Tipiskās kļūdas

- Piekļūstamība tiek jaukta ar **pieejamību** (uptime, darbspējas rādītāji).
- Tiek sniegts vispārīgs apgalvojums "tiks nodrošināta piekļūstamība" bez risinājuma apraksta.
- Teksts dublē apliecinājumu, kas jau sniegts **5.2.a.** apakšpunktā.
- Norādīta tikai atsauce uz standartu, bet nav paskaidrots, kā tas tiks praktiski īstenots.
- Nav aprakstītas piekļūstamības testēšanas metodes un posmi.
- Nav ņemti vērā iekšējās lietotāju grupas piekļūstamības aspekti, ja sistēma nav publiska.

Labā prakse

- Piekļūstamības prasības ir iekļautas tehniskajā specifikācijā un izstrādātājam ir skaidri izpildes kritēriji.
- Aprakstīti konkrēti testēšanas veidi un to regularitāte.
- Ievēroti Latvijas un starptautiskie piekļūstamības standarti (LVS EN 301 549:2021, WCAG 2.1 AA, LVS EN ISO 9241-210).
- Testēšanā izmantoti gan automātiskie validatori, gan manuālā pārbaude, gan lietotāju testēšana ar palīgtehnoloģijām.
- Ir paredzēta piekļūstamības atkārtota pārbaude pēc būtiskām sistēmas izmaiņām.

Piemērs

Tehniskajā specifikācijā iekļautas prasības, lai sistēma atbilstu WCAG 2.1 AA un LVS EN 301 549:2021.

Akcepttestēšanas laikā tiks veikta piekļūstamības izvērtēšana, izmantojot VARAM vadlīnijas un automātiskos validācijas rīkus (axe DevTools, WAVE).

Manuālajā pārbaudē piedalīsies lietotāji ar ekrānlasītājiem (NVDA, JAWS).

Pēc katrām būtiskām izmaiņām tiks veikta atkārtota pārbaude.

Ja sistēma nav publiski pieejama internetā, tiek nodrošināta iekšējā piekļūstamība darbiniekiem ar funkcionāliem traucējumiem (piem., atbilstoši pielāgoti interfeisa kontrasti un klaviatūras navigācija).

5.3.D1. FIZISKO PERSONU DATU APSTRĀDES NOLŪKS

Kas jānorāda

- Skaidrs un konkrēts mērķis, kādam tiek veikta datu apstrāde.
- Nolūkam jāatbilst izvēlētajam tiesiskajam pamatam un sistēmas funkcionalitātei.
- Jānorāda **"kāpēc"** un **"kam"** dati tiks izmantoti, nevis tikai vispārīgs apraksts.

Tipiskās kļūdas

- Norādīts tikai tiesiskais pamats, bet nav formulēts nolūks.
- Nolūks ir pārāk vispārīgs ("lai nodrošinātu sistēmas darbību").
- Nolūks nesaskan ar tiesisko pamatu vai reālo apstrādi.

Piemērs

Nolūks: Fizisko personu datu apstrāde nepieciešama, lai nodrošinātu licencēšanas procesa veikšanu, tai skaitā pieteikumu pieņemšanu, izskatīšanu un lēmumu pieņemšanu, atbilstoši likuma "Par licencēšanu" prasībām.

5.3.D2. FIZISKO PERSONU DATU SUBJEKTU KATEGORIJAS

Kas jānorāda

- To personu grupas, kuru dati tiks apstrādāti (piem., "licenču pieteicēji", "pakalpojumu sniedzēji", "iestādes darbinieki").
- Ja ir vairākas kategorijas – norādīt katru atsevišķi.

Tipiskās kļūdas

- Aprakstīti tikai dati, bet nav norādītas personu grupas.
- Lietoti neskaidri formulējumi ("personas", "lietotāji").

Piemērs

Datu subjekti:

- Fiziskas personas – licenču pieteicēji.
- Juridisko personu pārstāvji – pilnvarotās kontaktpersonas.
- Iestādes darbinieki, kas nodrošina licencēšanas procesu.

5.3.D3. FIZISKO PERSONU DATU IEGUVES AVOTS

Kas jānorāda

- Konkrētie avoti, no kuriem dati tiek iegūti (valsts reģistri, datubāzes, citas sistēmas).
- Datu iegūšanas mehānisms (API integrācija, datu apmaiņas formāts, manuāla ievade).
- Datu aktualizācijas biežums.

Tipiskās kļūdas

- Norādīts tikai "valsts reģistri" bez konkretizācijas.
- Nav aprakstīts, kā dati tiek iegūti un atjaunoti.

Piemērs

Dati tiek iegūti no Iedzīvotāju reģistra (API integrācija, ikdienas sinhronizācija) un Uzņēmumu reģistra (XML datu plūsma, iknedēļas atjaunošana).

5.3.D4. DATU SAŅĒMĒJI – PERSONAS (TO GRUPAS), KAS VAR PIEKĻŪT DATIEM

Kas jānorāda

- Datu saņēmēju kategorijas (iestādes darbinieki, sadarbības partneri, uzturētāji, izstrādātāji).
- Piekļuves ierobežojumus un drošības mehānismus (piem., piekļuve tikai noteiktām lomām, testa vide bez reāliem datiem).
- Pamatojumu, ja izstrādātājiem/uzturētājiem nepieciešama piekļuve.

Tipiskās kļūdas

- Nav norādīti izstrādātāji vai uzturētāji.
- Nav aprakstīti piekļuves ierobežojumi.
- Lietoti pārāk vispārīgi formulējumi ("IT atbalsta personāls").

Piemērs

Datu saņēmēji: iestādes darba vides administrators, portāla administrators, tehnisko resursu turētāji, drošības risinājumu nodrošinātāji, sistēmas uzturētāji (piekļuve tikai dokumentētos gadījumos, pēc atļaujas, bez reāliem datiem testa vidē).

5.3.D5. IETEKMES UZ DATU AIZSARDZĪBU NOVĒRTĒJUMS (DPIA)

Kas jānorāda

- Vai ir veikts sākotnējais riska novērtējums.
- Vai un kad plānots veikt DPIA (pirms apstrādes uzsākšanas vai riska izmaiņu gadījumā).
- Pamatojumu, ja DPIA nav nepieciešams.

Tipiskās kļūdas

- Nav norādīts termiņš vai pamatojums, ja novērtējums nav veikts.
- Nav minēts, kas veiks novērtējumu.

Piemērs

Sākotnējais riska novērtējums veikts 2025. gada februārī. DPIA plānots līdz 2025. gada aprīlim pirms sistēmas ieviešanas ražošanā. Novērtējumu veiks iestādes datu aizsardzības speciālists sadarbībā ar IT drošības vadītāju.

5.3.06. DATU AIZSARDZĪBAS SPECIĀLISTA IESAISTE

Kas jānorāda

- Vai projektā ir iesaistīts datu aizsardzības speciālists.
- Ja ir – norādīt vārdu, uzvārdu un amatu.
- Vai speciālists piesaistīts no iestādes vai ārpakalpojuma.

Tipiskās kļūdas

- Norādīts tikai "datu aizsardzības speciālists iesaistīts" bez papildu informācijas.
- Nav skaidrs, vai speciālists piedalīsies visa projekta gaitā.

Piemērs

Projekta izstrādē iesaistīts datu aizsardzības speciālists – Anna Liepa, sertificēta DVI, Juridiskās nodaļas juriste, piedalās jau no projektēšanas stadijas.

5.4. DATU ATVĒRŠANA UN KONTROLĒTA APRITE

Kas jānorāda

1. **Atveramās/publicējamās datu kopas**
   - Norādīt datu kopas, kas klasificētas kā **vispārpieejama informācija** un publicējamas atbilstoši MK noteikumu Nr. 367 2.2.1. apakšpunktam.
   - Jāiekļauj nosaukums, īss apraksts un publicēšanas vieta/formāts.
2. **Kontrolēti izplatāmās datu kopas**
   - Norādīt datu kopas, kas tiek nodotas citām institūcijām atbilstoši MK noteikumu Nr. 367 2.2.5. un 2.2.6. apakšpunktam (izplatīšanas kontrole, pieejamības nodrošināšana).
   - Tās **nav** publiski pieejamās datu kopas.
   - Jānorāda datu kopas saturs pietiekamā detalizācijā, lai skaidri identificētu tās tvērumu un mērķi.
3. **Ārējās saskarnes un savietotāji**
   - Saskarnes nosaukums un īss funkcijas apraksts.
   - Galvenās datu plūsmas (ievade/izvade).
   - Norādīt, vai tiek izmantoti savietotāji (piem., Valsts informācijas sistēmu savietotājs, nozares risinājumi).
4. **Tehniskie risinājumi kontrolētai apritei**
   - Drošas API, šifrēšanas protokoli (TLS, VPN), piekļuves kontroles mehānismi, auditācijas žurnāli.
   - Datu nodošanas mehānisms (sinhronais, asinhronais, periodiska sinhronizācija u.c.).
5. **Automatizācija un regularitāte**
   - Atbilstoši MK noteikumu Nr. 367 2.2.2. un 2.2.3. apakšpunktiem, norādīt, vai datu atvēršana/izplatīšana notiek automātiski, un kāda ir regularitāte (reāllaikā, reizi dienā, reizi mēnesī u.tml.).
6. **Pamatojums novirzēm (5.4.p)**
   - Ja kādai datu kopai netiek nodrošināta atvēršana vai kontrolēta aprite atbilstoši normatīvajiem punktiem, skaidrot iemeslus (piem., sensitivitāte, konfidencialitāte, tehniski ierobežojumi).

Tipiskās kļūdas

- Sajauc publiskās datu kopas ar kontrolēti izplatāmajām.
- Saskarnes apraksts ir pārāk vispārīgs un nesniedz informāciju par datu saturu vai drošības mehānismiem.
- Nav norādīta datu nodošanas automatizācija vai regularitāte.
- Nav pieminēti izmantotie savietotāji.
- Netiek skaidrots, kāpēc kāda datu kopa netiek atvērta vai izplatīta.

Piemērs

Atveramā datu kopa (5.4.a1): "Licencēto pakalpojumu sniedzēju saraksts" – satur licenču numurus, derīguma termiņus, juridiskās adreses; publicēta atvērto datu portālā kā CSV un JSON.

Kontrolēti izplatāmā datu kopa (5.4.a4): "Operatīvās informācijas plūsma starp uzraudzības iestādēm" – satur konfidenciālu informāciju par uzņēmumu atbilstības pārbaudēm; pieejama tikai noteiktām institūcijām ar API starpniecību.

Ārējā saskarne (5.4.a3): REST API "Licenču pārbaude" – reāllaika datu sniegšana partneriem, izmantojot TLS 1.3 un OAuth 2.0 autentifikāciju; piekļuve tiek reģistrēta auditācijas žurnālā.

Automatizācija (5.4.a2): Publisko datu atjaunošana reizi dienā automātiski no iekšējās datubāzes.

Pamatojums novirzei (5.4.p): Datu kopas "Operatīvās pārbaudes" netiek publicētas, jo satur ierobežotas pieejamības informāciju atbilstoši Informācijas atklātības likumam.

5.5. IDENTIFIKĀCIJA

Mērķis: Nodrošināt, ka aprakstā skaidri un pilnīgi izklāstīts informācijas sistēmas lietotāju identifikācijas un autentifikācijas risinājums, atbilstoši MK noteikumu Nr. 367 2.3.1.–2.3.3. apakšpunktiem un MK noteikumu Nr. 402 prasībām par autentifikācijas līmeņu izvērtējumu.

Kas jānorāda

1. **Autentifikācijas līmeņa izvērtējums**
   - Skaidri norādīt, vai uz identifikācijas risinājumu attiecināms MK noteikumu Nr. 402 līmeņa izvērtējums (zems, vidējs, augsts).
   - Pamatojums līmeņa izvēlei, ņemot vērā piekļūstamās informācijas sensitivitāti.
   - Ja nepieciešams, atsauce uz veiktu autentifikācijas risku novērtējumu.
2. **Tehniskie risinājumi**
   - Norādīt, vai tiek izmantots **divfaktoru autentifikācijas risinājums (2FA)**, un, ja jā, tad kādās situācijās vai lietotāju grupām tas ir obligāts.
   - Aprakstīt lietoto identifikācijas līdzekļu tipus (piem., eID, eParaksts, eParaksts mobile, ID karte, lietotājvārds/parole ar noteiktiem drošības parametriem).
3. **Lietotāju kategorijas un pieeja**
   - Identificēt dažādas lietotāju kategorijas (piem., iestāžu darbinieki, privātpersonas, juridisko personu pārstāvji, pilnvarotās personas).
   - Skaidri norādīt, vai lietotāju identifikācija un autentifikācija atšķiras starp kategorijām.
   - Precizēt, vai un kā ir nodrošināta pilnvaroto personu autentifikācija, ja tās pārstāv citu personu vai uzņēmumu.

4. **Pārrobežu piekļuve**
   - Ja sistēma nodrošina pārrobežu piekļuvi (eIDAS regulējuma ietvaros), jāapraksta, kā tiek nodrošināta identifikācija ārvalstu lietotājiem.

Tipiskās kļūdas

- Nav skaidri norādīts autentifikācijas līmenis vai pamatojums tā izvēlei.
- Apraksts vispārīgi min identifikācijas risinājumu, bet neizšķir dažādu lietotāju grupu piekļuves veidus.
- Nav informācijas par 2FA izmantošanu, pat ja tā ir obligāta noteiktās situācijās.

Piemērs

Sistēmā tiek izmantots **augsts autentifikācijas līmenis** (MK noteikumi Nr. 402), jo piekļuve ir sensitīviem personas datiem.

Privātpersonas autentificējas ar eID, eParaksts mobile vai Smart-ID (augsts līmenis), **iestāžu darbinieki** – ar integrētu LDAP risinājumu un 2FA.

Pilnvarotās personas autentificējas, izmantojot eID vai eParaksts mobile un papildus tiek pārbaudīta pilnvaras derīgums Valsts vienotajā pilnvarojumu reģistrā. Pārrobežu piekļuve tiek nodrošināta ar eIDAS mezgla starpniecību.

5.6. TEHNOLOĢISKĀS ARHITEKTŪRAS APRAKSTS

Mērķis: Nodrošināt, ka informācijas sistēmas tehnoloģiskā arhitektūra atbilst MK noteikumu Nr. 367 prasībām un VARAM publicētajām IKT arhitektūras vadlīnijām, tostarp precīzi norādot izmantotās koplietošanas komponentes un pakalpojumus, atkārtoti izmantojamos risinājumus, atvērtā koda izmantošanu un autortiesību statusu.

Kas jānorāda

- Īss sistēmas tehnoloģiskās arhitektūras apraksts (līdz 2000 rakstu zīmēm).
- Atbilstība MK noteikumu Nr. 367:
  - **2.4.1. un 2.4.6.** – tehnoloģiskās arhitektūras prasības un koplietošanas aspekti.
  - **2.4.2. un 2.4.4.** – koplietošanas un atkārtoti izmantojamu risinājumu izmantošana.
  - **2.4.3.** – neierobežotas mantiskās autortiesības.
  - **2.4.5.** – atvērtais kods un tehnoloģiskās arhitektūras vadlīniju ievērošana.
- Konkrēti **izmantojamie koplietošanas pakalpojumi un komponentes** (piemēram, eParaksts, eAdrese, ePakalpojumu platforma, Vienotā pieteikšanās modulis).
- Atvērto standartu, tehnoloģiju un savietotāju izmantošana (piem., REST API, SOAP, VISS API).
- Pamatojums, ja netiek izmantoti pieejamie koplietošanas risinājumi vai atvērtā koda komponentes.
- Informācija par datu apmaiņas saskarnēm un drošības aspektiem (piem., autentifikācija API lietošanā, auditācijas mehānismi).

Tipiskās kļūdas

- Norādīta tikai vispārīga frāze "sistēma atbilst IKT arhitektūras prasībām" bez konkrētiem risinājumu un komponentu nosaukumiem.
- Nav minēti izmantotie koplietošanas pakalpojumi vai tie minēti vispārīgi ("tiks izmantoti valsts koplietošanas risinājumi") bez detalizācijas.
- Nav aprakstīta autentifikācijas pieeja API vai saskarņu drošības risinājumi.

- Netiek norādīts, vai sistēmai ir neierobežotas mantiskās autortiesības un vai izmantots atvērtais kods.
- Apraksts neatbilst 5.6. apakšpunkta detalizācijas pakāpei (piem., izlaisti konkrēti savietotāji, neprecizēti izmantotie reģistri).
- Saites uz neatbilstošiem vai novecojušiem vadlīniju resursiem.

Piemērs

Vienotā reģistra arhitektūra tiks veidota trīs slāņos:

1. **Prezentācijas slānis –** tīmekļa lietotāja saskarne (HTML, CSS, JavaScript, React) ar pieejamības principu ievērošanu.
2. **Biznesa loģikas slānis –** Java + Spring Boot, nodrošinot datu validāciju, apstrādi un piekļuves kontroli.
3. **Datu piekļuves slānis –** Microsoft SQL Server datubāze ar klasterizācijas atbalstu LVRTC datu centrā.

Tehnoloģijas un savietojamība: RESTful API datu apmaiņai, OAuth 2.0 un OpenID Connect autentifikācijai, savietotāji ar VISS API un API Pārvaldnieku.

Koplietošanas pakalpojumi un komponentes:

- Latvija.lv autentifikācijas pakalpojums (eID, eParaksts Mobile);
- Valsts adreses reģistrs (VAR);
- DAGR datu apmaiņai ar citām valsts IS;
- API Pārvaldnieks saskarņu reģistrācijai un pārvaldībai.

Autortiesības un atvērtā koda izmantošana: Pilnas mantiskās autortiesības tiek nodotas pasūtītājam; atvērtā koda komponentes (PostgreSQL testēšanai, Keycloak pilotprojekta fāzē) tiek izmantotas, ievērojot licenču prasības.

Drošības aspekti: API piekļuve tiek nodrošināta tikai ar drošiem sertifikātiem un autorizāciju; piekļuves un datu apmaiņas darbības tiek auditētas.

6. RISINĀJUMA IEVIEŠANAS PIEEJA UN IKT INFRASTRUKTŪRA

Mērķis: Nodrošināt, ka anketas 6.1. un 6.2. apakšpunktos sniegtā informācija pilnībā atspoguļo plānoto IKT risinājuma ieviešanas pieeju, izmantotās programmatūras, platformu un infrastruktūras pakalpojumus, datu centru izvietojumu, atbalsta mehānismus, kā arī atbilstību MK noteikumu Nr. 367 prasībām. Aprakstam jābūt pietiekami detalizētam, lai vērtētājs varētu pārliecināties par risinājuma drošību, mērogojamību un atbilstību prasībām.

Kas jānorāda

- **Ieviešanas pieeja un metodoloģija** (piem., Agile, Waterfall, iteratīva pieeja), īsi aprakstot ieviešanas posmus.
- **Programmatūras tehnoloģijas** (piem., Java + Spring Boot, .NET, React, HTML/CSS/JS, datubāzes veids – PostgreSQL, MS SQL, Oracle DB utt.), ar piebildi, ja iespējamas tehnoloģiskās alternatīvas atkarībā no sistēmas noslodzes.
- **Platformas** (piem., VMware, OpenStack, Kubernetes, Docker), skaidri atšķirot platformu līmeņus (virtualizācija, konteinerizācija u.tml.).
- **Infrastruktūras pakalpojumi** – serveru tips (fiziski/virtuāli), klasterizācija, tīkla risinājumi (piem., ugunsmūri, komutatori ar LACP), datu glabātuves tips.
- **Atbalsta pakalpojumi** – iekļaut, vai tiks nodrošināti SOC un DDoS aizsardzības pakalpojumi, incidentu reakcijas režīms, SLA.

- **Datu centru izvietojums** – norādīt konkrētus datu centrus un, ja zināms, to VIRSIS reģistrācijas numurus.
- **Ārpakalpojumi** – norādīt, vai tiks izmantoti platformu vai programmatūras kā pakalpojuma risinājumi.
- **Atbilstība MK noteikumu Nr. 367 prasībām**:
  - 2.5.2. – lietotāju galaiekārtu prasības.
  - 2.5.3. – prasības skaitļošanas infrastruktūrai.
  - 2.5.4. – prasības dokumentācijai.
- **Pamatojums** – skaidrot jebkuru prasību nepiemērošanu vai novirzes, norādot, vai tas saskaņots ar pakalpojumu sniedzēju.

Tipiskās kļūdas

- Sniedz tikai ieviešanas posmus, bet neiekļauj tehnoloģiju, platformu un infrastruktūras detalizētu uzskaitījumu.
- Iztrūkst atbalsta pakalpojumu apraksts (SOC, DDoS, incidentu reakcija).
- Nav norādīta infrastruktūras atbilstība sistēmas vajadzībām un drošības prasībām.
- Netiek sniegti apliecinājumi par atbilstību MK Nr. 367 2.5.2., 2.5.3., 2.5.4. apakšpunktiem.
- Nav norādīti VIRSIS reģistrācijas numuri, ja tie jau ir zināmi.
- Noviržu pamatojumi ir vispārīgi vai attiecas uz citiem dokumentiem, bet nav tieši sasaistīti ar 6. apakšpunkta prasībām.

Piemērs

Ieviešana tiks veikta Agile metodoloģijā ar četriem posmiem: plānošana un analīze, izstrāde un testēšana, ieviešana un apmācības, uzturēšana un atbalsts.

- **Programmatūra:** Backend – Java + Spring Boot; Frontend – React, HTML/CSS/JS; DB – Microsoft SQL Server ar iespējamu alternatīvu PostgreSQL, ja tas labāk atbildīs noslodzes analīzei.
- **Platformas:** VMware vSphere virtualizācijas vide; Docker konteinerizācija testēšanai un mikropakalpojumu izvietošanai.
- **Infrastruktūra:** Klasterizēti virtuālie serveri LVRTC datu centrā ar N+1 jaudas rezervi; ugunsmūru klasteris; LACP komutatoru konfigurācija; lokāla datu glabātuve ar RAID-10.
- **Atbalsta pakalpojumi:** LVRTC nodrošina infrastruktūru, SOC un DDoS aizsardzību; incidentu reakcija 24/7 ar kritisku incidentu novēršanu 2h laikā.
- **Datu centri:** Pamatdatu centrs – LVRTC (VIRSIS Nr. 001234); Rezerves DC – Liepājas filiāle (VIRSIS Nr. 005678).
- **Atbilstība prasībām:** Galaiekārtas atbilst MK Nr. 367 2.5.2.; infrastruktūra – 2.5.3.; dokumentācija tiks sagatavota pilnā apjomā atbilstoši 2.5.4.
- **Novirzes:** Nav paredzētas.

7. PAMATOJUMS, PRIEKŠNOSACĪJUMI, RISKI UN PLĀNOTIE TERMIŅI

7.1. Pamatojums un priekšnosacījumi

Mērķis: Nodrošināt, ka pieteikumā ir skaidri un pārbaudāmi norādīti visi būtiskie normatīvie akti, kas pamato aktivitātes īstenošanu, to statuss, kā arī citi priekšnosacījumi, kas nepieciešami projekta uzsākšanai.

Kas jānorāda

- Normatīvie akti, uz kuriem pamatojas aktivitāte, ar pilnu nosaukumu, statusu (piem., "pieņemts", "projekts" u.c.) un tiešu saiti uz **www.likumi.lv** vai citu publisku oficiālo resursu.
- Ja tiek minēti citi normatīvie vai metodiskie dokumenti, jānorāda to publiskā pieejamība (tiešā saite vai norāde "nav publiski pieejams").
- Citi priekšnosacījumi, kas nepieciešami aktivitātes uzsākšanai (piem., atļaujas, saskaņojumi, infrastruktūras pieejamība).

Tipiskās kļūdas

- Nav tiešo saišu uz normatīvajiem aktiem.
- Minēti normatīvie akti bez norādes uz to statusu.
- Minēti dokumenti, bet nav norādīta to pieejamība vai statuss.

Piemērs

Pamatojums balstīts uz MK noteikumiem Nr. 702 "Noteikumi par …" (pieņemti 2023-05-12, saite: https://likumi.lv/…) un NKDL 18. panta prasībām (saite: https://likumi.lv/…).

Projekta uzsākšanai nepieciešama Telpiskās plānošanas valsts inspekcijas atļauja (iesniegta 2024-09-10, sagaidāma atbilde 2024-12).

Citi priekšnosacījumi – datu centra infrastruktūras pieejamība, saskaņota ar LVRTC.

7.2. RISKA APRAKSTS UN PĀRVALDĪBA

Mērķis: Identificēt un izvērtēt riskus, kas var ietekmēt aktivitātes uzsākšanu vai sekmīgu īstenošanu, īpaši IKT un kiberdrošības jomā, un noteikt risku mazināšanas vai pārvaldības pasākumus.

Kas jānorāda

- Vismaz būtiskākie riski (piem., kavēšanās iepirkumā, IKT infrastruktūras nepieejamība, drošības incidenti, cilvēkresursu trūkums).
- Atsevišķi jāizdala **IKT drošības riski** (piem., piekļuves kontroles pārkāpumi, DDoS uzbrukumi, datu noplūde).
- Katram riskam jānorāda:
  - **Novērtējums** (piem., zems/vidējs/augsts vai % ietekmes iespējamība un smagums);
  - **Ietekme** uz projekta īstenošanu;
  - **Pārvaldības/mazināšanas pasākumi** (piem., rezerves risinājumi, drošības kontroles, līgumu punkti ar pakalpojumu sniedzējiem).
- Rekomendē norādīt arī darbības soļus gadījumam, ja IKT infrastruktūra nebūs pieejama plānotajā laikā.

Tipiskās kļūdas

- Risku sadaļā tikai vispārīgi apgalvojumi ("Risku nav" vai "Tiks pārvaldīts"), bez konkrēta novērtējuma.
- Neiekļauj IKT drošības riskus vai neapraksta to ietekmi.
- Nav minēti mazināšanas pasākumi.

Piemērs

Risks: Kritisko sistēmu infrastruktūra nebūs pieejama līdz ieviešanas uzsākšanai. Novērtējums: Vidējs (iespējamība – 40%, ietekme – augsta).

Ietekme: Projekta ieviešanas kavēšanās par ≥3 mēnešiem.

Pasākumi: Alternatīvās izvietošanas līgums ar rezerves datu centru; provizoriski rezervētas resursu jaudas.

Kiberdrošības risks: DDoS uzbrukums ieviešanas laikā (novērtējums – zems, ietekme – augsta). Pasākumi: Pieslēgts AM nodrošinātais DDoS aizsardzības pakalpojums.

7.3. PLĀNOTĀ ATTĪSTĪBAS AKTIVITĀTES UZSĀKŠANA

Mērķis: Precīzi norādīt attīstības aktivitātes uzsākšanas datumu atbilstoši reālajai situācijai.

Kas jānorāda

- Precīzs kalendāra datums (DD.MM.GGGG), nevis gads vai ceturksnis.
- Pārliecināties, ka datums nav pagātnē (izņemot gadījumus, kad projekts jau ir faktiski uzsākts un dokumentēts).
- Datuma izvēle jāsaskaņo ar iepirkuma, līgumu noslēgšanas un priekšnosacījumu izpildes grafiku.

Tipiskās kļūdas

- Norādīts tikai gads vai ceturksnis.
- Datums neatbilst faktiskajam projekta stāvoklim.

Piemērs

Plānotā uzsākšana: 15.04.2025 (pēc iepirkuma līguma parakstīšanas un nepieciešamo saskaņojumu saņemšanas).

7.4. PLĀNOTĀ ATTĪSTĪBAS AKTIVITĀTES PABEIGŠANA – NODOŠANA EKSPLUATĀCIJĀ

Mērķis: Norādīt reālistisku datumu, kad risinājums tiks pilnībā nodots ekspluatācijā, ņemot vērā ieviešanas posmus, testēšanu un pieņemšanas procedūras.

Kas jānorāda

- Precīzs kalendāra datums (DD.MM.GGGG), kad paredzēts pabeigt aktivitāti un nodot sistēmu ekspluatācijā.
- Datums jāsaskaņo ar ieviešanas plānu, risku vadības pasākumiem un līgumu termiņiem.

Tipiskās kļūdas

- Norādīts tikai gads.
- Datums nesakrīt ar projekta grafiku vai tehnisko ieviešanas plānu.

Piemērs

Plānotā pabeigšana: 30.11.2025 (pēc sistēmas testēšanas, lietotāju apmācības un pieņemšanas–nodošanas akta parakstīšanas).

8. FINANSĒJUMA AVOTS UN APJOMS

Kas jānorāda

- Finansējuma avots (piemēram, ES fondu finansējums, valsts budžets, iestādes pašu līdzekļi u. c.).
- Plānotais finansējuma apjoms **noapaļots līdz tūkstošiem euro**, ievērojot konsekvenci ar 3.2. apakšpunktā norādīto **indikatīvo finansējuma apjomu**.
- Gadījumā, ja finansējuma apjoms 8. punktā atšķiras no 3.2. apakšpunktā norādītā, jānorāda pamatots skaidrojums (piem., ja iekļauta papildus darbība, kas nebija iekļauta sākotnējā aprēķinā).
- Finansējuma sadalījums pa darbībām, ja tas ir būtiski, lai izprastu apjoma struktūru.

Tipiskās kļūdas

- Finansējuma apjoms neatbilst 3.2. apakšpunktā norādītajam indikatīvajam apjomam (piem., 3.2. – 2 215 000 EUR, 8. – 2 210 000 EUR).
- Finansējuma starpība nav pamatota un nav skaidrs, kādiem mērķiem tā paredzēta.
- Summas nav noapaļotas līdz tūkstošiem euro.
- Finansējuma avots nav norādīts vai tas ir pārāk vispārīgs.

Labā prakse

- Nodrošināt, ka 8. punktā norādītais finansējuma apjoms **precīzi sakrīt** ar 3.2. apakšpunktā norādīto indikatīvo apjomu vai ir sniegts skaidrs un pamatots atšķirības izskaidrojums.
- Ja plānotas izmaiņas finansējuma sadalījumā starp darbībām vai komponentēm, tās īsi aprakstīt šajā punktā vai pievienot atsauci uz detalizētu tāmi.
- Norādīt finansējuma avotu precīzi (piem., "ERAF 2021.–2027. plānošanas perioda 1.3.1.3. pasākums" nevis tikai "ES fondu finansējums").

Piemērs

Finansējuma avots: ERAF (2021–2027 plānošanas periods, 1.3.1.3. pasākums) – 1 800 000 EUR,

Valsts budžeta līdzfinansējums – 300 000 EUR,

Iestādes pašu līdzekļi – 100 000 EUR.

Kopā: 2 200 000 EUR (atbilst 3.2. apakšpunktā norādītajam apjomam).

Atšķirības no iepriekšējā aprēķina nav, precizēts sadalījums pa finansējuma avotiem.

AIZSARDZĪBAS
MINISTRIJA

Nacionālais
kiberdrošības
centrs