SIA “Koksnes plūsmas datu centra”
IS datu drošības politika

Versijas numurs:1.4.

Versijas datums: 15.01.2024.

Rīga, 2021

Saturs

1. IS drošības politikas mērķi un uzdevumi

1.1. SIA Koksnes plūsmas datu centra (turpmāk tekstā – KpDC) informācijas sistēmas (turpmāk – IS) drošības politikas mērķis ir īstenot uzņēmuma darbības mērķiem atbilstošu, ekonomiski pamatotu un sabalansētu IS aizsardzību, lai KpDC informācijas un tehniskie resursi būtu aizsargāti pret ārējiem un iekšējiem drošības apdraudējumiem.

1.2. IS drošības politika ir saistoša visiem KpDC IS lietotājiem.

1.3. Drošības politikas uzdevumi ir sekojoši

1.3.1. Nodrošināt informācijas pieejamību.

1.3.2. Nodrošināt informācijas integritāti.

1.3.3. Nodrošināt informācijas konfidencialitāti.

1.3.4. Aizsargāt IS informācijas resursus.

1.3.5. Aizsargāt IS tehniskos resursus.

1.3.6. Noteikt iespējamus IS drošības apdraudējumus.

1.3.7. Novērtēt IS drošības riskus.

1.3.8. Noteikt pasākumus iespējamo drošības risku mazināšanai.

1.3.9. Atklāt iespējamus IS drošības incidentus.

1.3.10. Atjaunot IS darbību pēc drošības incidenta.

1.3.11. Definēt nosacījumus IS drošības politikas kontrolei.

2. KpDC IS drošības politikā izmantotie termini un saīsinājumi

Termins/Saīsinājums	Skaidrojums
Ārpakalpojums	Jebkura veida vienošanās starp tirgus dalībnieku un pakalpojuma sniedzēju, saskaņā ar kuru šis pakalpojuma sniedzējs nodrošina procesu, sniedz pakalpojumu vai veic citu darbību, ko citādi darītu pats tirgus dalībnieks.
Auditācijas pieraksti	Analīzei pieejami pieraksti, kuros reģistrēti dati par konkrētiem IT notikumiem (piekļuve, datu ievade, maiņa, dzēšana, izvade u.c.).
AUI	Automatizētās uzmērīšanas sistēma
DEAC	SIA "Digitālās ekonomikas attīstības centrs", uzņēmums, kas KpDC nodrošina datu centra pakalpojumus.
Drošības incidents	Gadījums, kurā IS apdraudējumi ir negatīvi ietekmējuši IS darbību, izmantojot to trūkumus.
Drošības pasākumi	Tehniski vai organizatoriski pasākumi, kas tiek noteikti risku pārvaldības ietvaros un samazina IT risku līdz pieļaujamajam līmenim.
Drošības politika	Informācijas sistēmu drošības politika.
Incidents	Gadījums, kurā KpDC IS apdraudējumi ir negatīvi ietekmējuši IS darbību, izmantojot to trūkumus.
Informācijas integritāte	Pilnīgas un nemainītas informācijas saglabāšana.
Informācijas konfidencialitāte	Informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot.
Informācijas pieejamība	Piekļuve informācijai noteiktā laikposmā pēc informācijas pieprasīšanas.
IS drošības apdraudējums	Ar nodomu (tīši) vai aiz neuzmanības izdarītu darbību vai notikumu, kas var izraisīt sistēmas informācijas vai tehnisko resursu izmaiņas, bojājumu, iznīcināšanu vai nonākšanu tādu personu rīcībā, kuras nav tam pilnvarotas, vai kura dēļ piekļūšana sistēmas informācijas resursiem var būt traucēta vai neiespējama.
IS informācijas resursi	Datnes, arī tās, kuras satur sistēmā glabājamo, apstrādājamo un sistēmas lietotājiem pieejamo informāciju, un sistēmas dokumentāciju.
IS tehniskie resursi	Datori, programmatūra, datu nesēji, datortīkla iekārtas un citas tehniskās iekārtas, kuras nodrošina sistēmas darbību.
IS (Informācijas sistēmas)	Strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek veikta datu ievade, uzglabāšana, apstrāde, izvade un pārraide, kas nodrošina noteiktu funkciju izpildi.
IT	Informācijas tehnoloģijas.
Kontroles	Metodes un pasākumi riska mazināšanai.
KpDC	Koksnes plūsmas datu centrs.
Lietotājs	Persona, kura piešķirto pilnvaru robežās lieto IT sistēmu.
Risks	Varbūtēja nespēja pilnvērtīgi un kvalitatīvi veikt kādu savu saistību vai funkciju izpildi saistībā ar IS funkcionēšanu.

SSL	Angļu val. – ‘Secure Sockets Layer’. Šifrētu datu pārraide tīklā, kas garantē, ka nododamie dati tiks pasargāti ar drošu šifrēšanas algoritmu un nebūs pieejami trešajām personām nesankcionētai apskatei.
VPN	Viruālais privātais tīkls (angļu val. - Virtual private network) ir viena vai vairāku tīklu savienojums kāda tīkla vai vairāku tīklu (piemēram, interneta) ietvaros.

3. Uzņēmuma IS raksturojums un analīze drošības jomā

3.1. IS drošības politika izstrādāta KpDC piederošām sistēmām - IS Apse, IS Ciedrs, IS Linda, IS Dace, kurā ietilpst Atskaišu sistēma datu bāze - Reģistrs.

3.2. IS funkcijas:

3.2.1. IS Ciedrs ir centrālā datu uzskaites sistēma visiem kokmateriālu uzmērīšanas datiem, no kuriem tālāk tiek veidoti aprēķini IS APSE, lai izveidotu Testēšanas pārskatus.

3.2.2. IS Apse ir sistēma, kurā tiek importēta uzmērīšanas datu apstrādes specifikācija (Matrica) un, izmantojot to, automātiski tiek sagatavoti un uz IS Dace nosūtīti testēšanas pārskati.

3.2.3. IS Linda – sistēma, kas nodrošina tiešo datu plūsmu no automatizētām uzmērīšanas iekārtām (AUI) individuālās uzmērīšanas gadījumā.

3.2.4. IS Dace ir komunikācijas platforma, kas nodrošina kokmateriālu plūsmā iesaistīto biznesa dokumentu apmaiņu, izveidi starp sistēmām un lietotājiem. Tai skaitā nodrošinot lietotāju un uzņēmumu lietotāju identitātes pārvaldību un dažādu nozares klasifikatoru uzturēšanu. IS DACE funkcionalitātes:

3.2.4.1. kokmateriālu mērīšanas datu ievade;

3.2.4.2. pilnas kokmateriālu dokumentu ķēdes uzturēšana;

3.2.4.3. atskaišu modulis – atskaišu sagatavošana;

3.2.4.4. datu bāze – Reģistrs ir dokumentos ietilpstošo datu reģistrs;

3.2.4.5. kokmateriālu darījumos izmantotā specifikācija (Matrica);

3.2.4.6. dokumentu reģistrs;

3.2.4.7. klasifikatoru reģistrs.

3.3. IS apstrādā un saglabā datus un informāciju, kas klasificēti kā "ierobežotas pieejamības" informācija.

3.4. IS tiek ievadīti, saglabāti un apstrādāti dati, kuri tiek klasificēti sekojoši:

3.4.1. Kokmateriālu mērījumu dati;

3.4.2. Pilnas dokumentu ķēdes dati;

3.4.3. Pircēju, pārdevēju un uzmērītāju identitātes dati;

3.4.4. Kokmateriālu un brāķu sortimentu klasifikatori;

3.4.5. Specifikācijas (matricas);

3.4.6. Transporta klasifikators;

3.4.7. Testēšanas pārskata dati.

3.5. IS resursi tiek klasificēti sekojoši:

3.5.1. IS informācijas resursi

3.5.2. IS Tehniskie resursi.

3.6. IS lietotāji tiek iedalīti:

3.6.1. KpDC lietotāji – nodrošina administratora, izstrādes un uzturēšanas funkcijas.

3.6.2. Meža nozares pārstāvji, kas nodrošina datu un informācijas ievadi un noslēguši līgumu ar KpDC par pakalpojumu:

3.6.2.1. Kokmateriālu pārdevēji;

3.6.2.2. Kokmateriālu pircēji;

3.6.2.3. Kokmateriālu transportētāji;

3.6.2.4. Kokmateriālu uzmērītāji.

3.7. IS tiek attīstītas iegādājoties standartprogrammatūru, pasūtot programmatūras izstrādi ārējiem izstrādātājiem, izstrādājot jaunu programmatūru ar uzņēmuma resursiem. Katrai izstrādes sistēmai ir izstrādes, testa un produkcijas vide. Atkarībā no sistēmas specifikācijas, var tikt izmantotas vairākas testa vides.

3.8. KpDC sistēmu funkcijas ir radītas mežsaimniecības nozares atbalstam. Tai skaitā nozīmīga daļa atbalsta kokmateriālu uzmērīšanu. KpDC uztur un attīsta ne tikai sev piederošanas sistēmas, bet arī kokmateriālu uzmērīšanā izmantotās sistēmas.

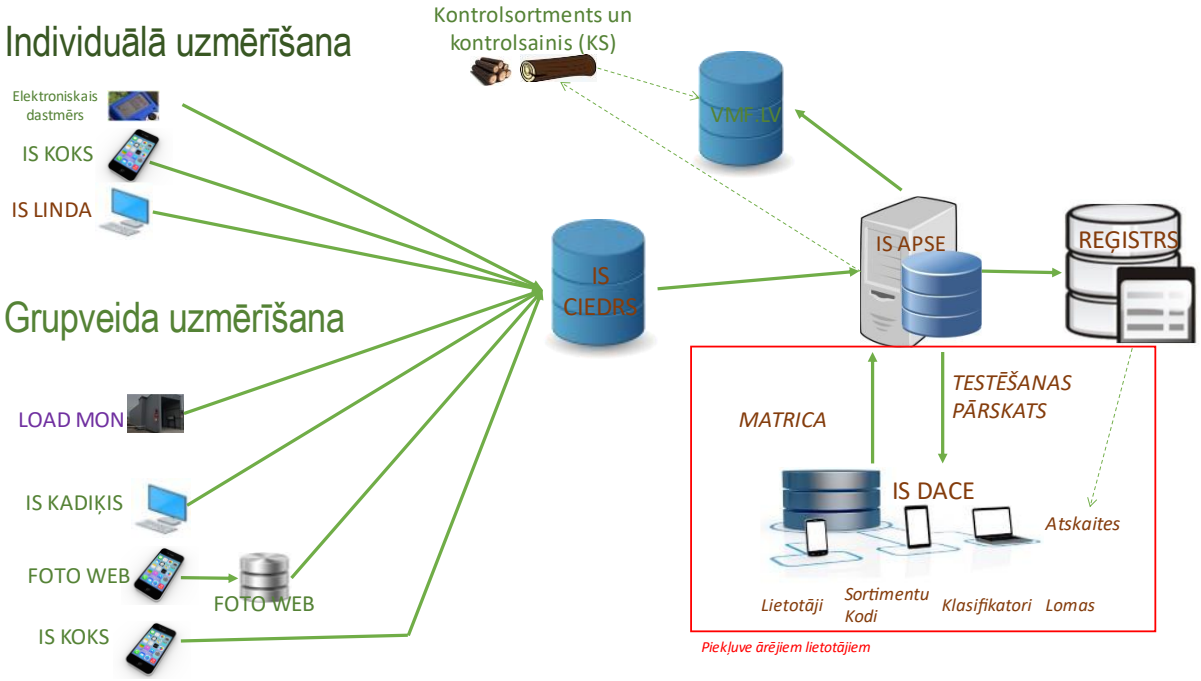
2.1.1.attēlā redzama koksnes mērīšanas datu plūsmas shēma.

3.8.1. IS Ciedrā ienāk dati no kokmateriālu uzmērīšanas ievades sistēmām – Elektroniskais dastmērs, IS Linda, IS Kadiķis, Foto Web, Load Mon.

3.8.2. No IS Ciedrs dati tiek nosūtīti uz IS Apse.

3.8.3. No IS Apse tiek nosūtīti koksnes mērījumu dati uz IS Dace un un klientu sistēmām pēc Matricā definētajām pieejamībām.

3.8.4. Kontroles funkciju nodrošināšanai dati tiek nosūtīti uz Kontrolsortimenta un kontrolsaiņa sistēmām.



Attēls 1. Kokmateriālu mērīšanas datu plūsma

3.9. KpDC nodrošina IS pakalpojumu uzņēmumiem, kas nodrošina kokmateriālu uzmērīšanu. Tai skaitā - sistēmas uzturēšanu un izmaiņu izstrādi.

3.10. Sistēmu uzturēšana:

3.10.1. IS Apse un uzturēšanu un izmaiņu veikšanu tiek nodrošināta ar uzņēmuma resursiem.

3.10.2. IS Ciedrs, IS Linda un IS Dace uzturēšanā un izmaiņu izstrādē tiek nodrošināts arī ārpakalpojums.

3.11. Datu bāzes un infrastruktūra tiek uzturēta Eiropas līmeņa atbilstošā ārējā datu centrā. Infrastruktūras pieejamība un darbības nepārtrauktību līgumiski nodrošina SLA starp uzņēmumu un datu centru.

3.12. Tiek nodrošināta serveru datu kopēšana un glabāšana Bite datu centrā.

3.13. Pieslēgumu internetam nodrošina ārējie pakalpojuma sniedzēji.

3.14. Datu pārraides šifrēšanai tiek izmantots drošs SSL sertifikāts.

3.15. Darbinieku darbs ar sistēmām tiek aizsargāts, nodrošināto iekšējo datortīklu (VPN).

3.16. Uzņēmums izmanto iekšējo datu tīklu, kuru nodrošina ārējie pakalpojuma sniedzēji.

4. Drošības pārvaldība

4.1. Uzņēmumā regulāri tiek pilnveidots dokumentu un pasākumu kopums, kuru īstenošana nodrošina IS drošības politikas mērķa sasniegšanu. Jekburš KpDC darbinieks var ierosināt veikt izmaiņas IS drošības politikā, ierosinājumus iesniedzot KpDC vadītājam.

4.2. Uzņēmumā nodrošina pastāvīgu drošības politikas īstenošanas koordinēšanu un pārraudzīšanu.

4.3. Gadījumos, kad uzņēmuma darbinieki neievēro "Drošības politikas" izvirzītās prasības, uzņēmuma vadība var ierosināt disciplinārās atbildības procesu saskaņā ar normatīvajiem aktiem.

4.4. Uzņēmumā ir skaidri definēts atbildības sadalījums par IS drošību.

4.5. Uzņēmuma vadītājs:

4.5.1. Atbild par IS drošību.

4.5.2. Nosaka un apstiprina IS drošības politiku.

4.5.3. Nodrošina nepieciešamos līdzekļus un atbalstu IS drošības politikas ieviešanai, uzturēšanai un pilnveidošanai.

4.5.4. Nosaka pienākumu un atbildības sadalījumu attiecībā uz IS drošību.

4.5.5. Nosaka kontroles mehānismu IS drošības pārvaldībai.

4.6. Atbildīgā personas par IS drošības pārvaldību ir IS drošības pārvaldnieks, kura funkcijas veic IT Projekta asistente:

4.6.1. Nodrošina nepieciešamo IS drošības dokumentu uzturēšanu un īstenošanu.

4.6.2. Sagatavo procedūras IS drošības politikas realizācijai un uzturēšanai.

4.6.3. Organizē IS risku analīzi.

4.6.4. Veic noteikto drošības prasību ievērošanas uzraudzību.

4.6.5. Informē iesaistītās personas par un drošības incidenta izmeklēšanas gaitu to novēršanu.

4.7. Noteikti sekojoši informācijas un tehnisko resursu pārvaldnieki:

4.7.1. IS Apse – IT Projekta vadītājs;

4.7.2. IS Ciedrs – IT Projekta vadītājs;

4.7.3. IS Dace – IT Projekta vadītājs;

4.7.4. IS Linda – IT Pakalpojumu vadītājs.

4.8. Informācijas un Tehnisko resursu pārvaldnieks:

4.8.1. Nosaka drošības prasības informācijas resursam.

4.8.2. Nosaka pieejas tiesību mehānismu informācijas resursam.

4.8.3. Atbild par piekļuves kontroli informācijas resursam.

4.8.4. Apkopo drošības riskus savā pārvaldībā esošajam informācijas un tehniskajam resursam.

4.8.5. Veic drošības incidenta izmeklēšanu.

4.8.6. Savas komptences ietvaros, veic drošības incidenta novēršanu.

4.8.7. Atbild par IS tehnisko resursu iegādi, izstrādi, darbību un uzturēšanu;

4.8.8. Nodrošina IS tehniskos un loģiskos aizsardzības pasākumus;

4.8.9. Atbild par IS pieejas tiesību pārvaldību;

4.8.10. Nodrošina IS darbības atjaunošanas pasākumus, ja Sistēmas darbība ir traucēta.

4.9. Incidentu pārvaldnieks, kura pienākumus pilda IS galvenais lietotājs:

4.9.1. Apkopo informāciju par informācijas drošības notikumiem un incidentiem.

4.9.2. Nosūta incidentus novēršanai atbildīgajām personām.

4.9.3. Kontrolē informācijas drošības notikumu un incidentu novēršanu.

4.10. Izstrādātāji, kuru pienākumus pilda programmēšanas sistēminženieris vai uzņēmums, ar kuru noslēgts līgums par ārpakalpojumu:

4.10.1. Nodrošina izstrādes, testa un produkcijas vides nodalīšanu;

4.10.2. Izmanto izstrādes un testa vidi;

4.10.3. Nodrošina, ka neautorizētas personas nevar piekļūt izejas kodam;

4.10.4. Nodrošina, ka izejas kods pēc iespējas netiek glabāts produkcijas sistēmās;

4.10.5. Izstrādi veic saskaņā ar šajā politikā noteikto.

4.10.6. Pēc nepieciešamības, novērš IS drošības incidentus.

4.11. Lietotāji - ziņo par Sistēmas informācijas drošības notikumiem un incidentiem.

5. Tiesiskais regulējums

5.1. IS ir ievērotas Latvijas Republikas normatīvo aktu prasības informācijas tehnoloģiju un informācijas drošības jomā.

5.2. Ja nav noteikts citādi, visa uzņēmuma izstrādātā programmatūra, apmācību materiāli, dokumenti un citi materiāli ir iestādes intelektuālais īpašums.

5.3. Darbā ar IS resursu ir jāievēro visas tā ražotāja noteiktās autortiesību, programmatūras licenču un lietošanas prasības.

6. IS drošības principi

6.1. IS lietotāju konti:

6.1.1. IS lietotāji, kas veic Sistēmas administrēšanas darbu, izmanto tam īpašus lietotāju kontus (turpmāk – Sistēmas administratora konti), kas netiek izmantoti ikdienas darbību veikšanai.

6.1.2. Piekļuve IS administratora līmenī un datubāzei tiek nodrošināta tikai no reģistrētām IP adresēm.

6.1.3. Katrs lietotāja konts ir saistīts ar konkrētu fizisko personu.

6.1.4. Kā piekļuves ierobežošanas līdzeklis IS tiek izmantota lomu pārbaude katrā darbībā.

6.1.5. IS Dace lietotāju piekļuve tiek piešķirta, balstoties uz noslēgto savstarpējo vienošanos/līgumu ar IS pārvaldītāju par organizācijas profila izveidi. IS lomas ir tiesības mainīt lietotājam ar administratora tiesībām.

6.1.6. IS Apse loma tiek piešķirta tikai un vienīgi no sistēmas administratora puses. Lietotājs nevar mainīt lomu sistēmā.

6.1.7. IS lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju - kļūdas apraksts un kļūdas identifikators.

6.1.8. Izveidojot jaunu organizācijas lietotāja kontu, tiek nodrošināta e-pasta adreses pārbaude. Nav iespējams ievadīt vērtību, kas nav e-pasta adrese.

6.1.9. IS lietotāja profilā tiek atspoguļota informācija tikai par organizāciju, kuras lietotāja profils ir izveidots.

6.1.10. Viens lietotājs ar savām pieejas tiesībām var lietot IS tikai, kā vienas organizācijas pārstāvis.

6.1.11. Reizi gadā tiek pārskatīti IS lietotāji.

6.2. Prasības parolēm:

6.2.1. IS piekļuve ir aizsargāta ar lietotāja vārdu un paroli.

6.2.2. IS lietotāju paroļu garums nav mazāks par 8 simboliem, satur vismaz vienu lielo burtu, vismaz vienu viens mazo burtu, vienu ciparu vai simbolu.

6.2.3. IS lietotāja parole ievadīšanas brīdī netiek pilnībā attēlota lietotājam.

6.2.4. Visas paroles tiek glabātas kriptētā veidā tā, lai arī sistēmas administratoram tās nav pieejamas. Ja sistēmas administratoram jāatjauno parole, tad tam jānotiek izmantojot konkrētas funkcijas izsaukumu, kas uzģenerē jauno paroli un nosūta to uz klienta reģistrēto e-pastu.

6.2.5. Iekārtām, t.sk. infrastruktūras iekārtām, kas nodrošina sistēmas funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles.

6.3. Izsekojamība:

6.3.1. IS auditācijas pierakstus, kas apkopo apskates informāciju veido un uzglabā vismaz 6 mēnešus pēc ieraksta izdarīšanas. Pārējos auditācijas pierakstus uzglabā vismaz 12 mēnešus.

6.3.2. IS auditācijas pierakstos ietver informāciju par pieslēgšanos vai atslēgšanos no sistēmas, datu atlasi, kā arī konta izveidi, grozīšanu vai dzēšanu, fiksējot notikuma laiku, kas sakrīt ar faktiskā notikuma koordinēto pasaules laiku (UTC), interneta protokola adresi, no kuras veikta darbība, aprakstu, kā arī informāciju par darbības iniciatoru – identifikatoru, pieslēguma metadatus.

6.3.3. Jebkura piekļuve sistēmai ir izsekojama līdz konkrētam IS lietotāja kontam vai interneta protokola (IP) adresei.

6.3.4. Katra sistēmas darbība logojas, tajā skaitā arī katra darbība, kas tiek veikta pa tiešo datubāzē no IS uzturētāju puses.

6.3.5. Atbildīgā persona par IS drošības pārvaldību nodrošina Sistēmas auditācijas pierakstu satura plānveida uzraudzību un analīzi, lai konstatētu incidentus.

6.4. Atjauninājumi:

6.4.1. IS pārvaldnieki veic pieejamo programmatūras atjauninājumu izvērtēšanu un testēšanu testa vidē.

6.4.2. IS jābūt uzliktiem visiem pieejamajiem nepieciešamajiem programmatūras atjauninājumiem.

6.5. Datubāzes līmenī:

6.5.1. Piekļuve tiek nodrošināta caur API (application programming interface) izmantojot sistēmas piešķirto lietotāja atslēgu.

6.5.2. Piekļuve sistēmu līmenī tiek nodrošināta ar tiešu pieslēgumu datu bāzei, izmantojot katrai sistēmai unikālu lietotāja vārdu un drošu paroli, kas atbilst 5.2 punktā aprakstītajam. Piekļuve ir iespējama tikai ar KpDC piešķirto IP adresi.

6.5.3. Piekļuve sistēmu uzturēšanai un izstrādei tiek nodrošināta ar tiešu pieslēgumu datu bāzei, izmantojot DBVS (datu bāzu vadības sistēmas), izmantojot katram lietotājam unikālu lietotāja vārdu un drošu paroli, kas atbilst 5.2 punktā aprakstītajam.

6.5.4. Piekļuve nav publiski pieejama.

6.6. Dati no IS tiek nosūtīti tikai norādītajiem adresātiem.

6.7. IS katru gadu tiek veikti drošības auditi pēc OWASP standartiem, kas apliecina datu pieejamības drošību.

7. IS aizsardzības pasākumi

7.1. Visi KpDC darbinieku tehniskie resursi, kas ikdienā tiek izmantoti, lai pieslēgtos sistēmai, ir aprīkoti ar pretvīrusu funkcionalitāti.

7.2. Fiziski piekļūt iekārtām, kas nodrošina IS darbību, atļauts vienīgi iestādes pilnvarotām personām vai šo personu pavadībā.

7.3. Plūsma starp informācijas sistēmu un tās lietotājiem, kā arī starp informācijas sistēmu un citām informācijas sistēmām tiek kontrolēta, izmantojot ugunsmūra risinājumu.

7.4. IS Apse un IS Ciedrs piekļuve tiek nodrošināta tikai no KpDC biroja IP adreses.

7.5. IS Linda piekļuve tiek nodrošināta ar KpDC WPN pieslēgumu.

7.6. Veicot Sistēmas izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu produkcijas vides glabāto datu integritātei. Tādēļ šādiem nolūkiem ir izveidota sistēmas izstrādes un testa vide.

7.7. Sistēmas izstrādes kods tiek glabāts KpDC GIT HUB resursā. Pieeja šim resursam ir tikai pilnvarotajam KpDC izstrādātājam.

7.8. Uz darbinieku datoriem nav pieejama sensitīva informācija. Visi dati tiek glabāti Eiropas līmeņa datu centrā DEAC.

8. IS drošības risku analīze un pārvaldība

8.1. Drošības riska pārvaldības plāns izstrādāts KpDC informācijas un tehnisko resursu risku pārvaldībai.

8.2. Risku analīzes mērķi Iestādē ir:

8.2.1. Apzināt Sistēmas risku līmeni.

8.2.2. Noteikt kādas darbības veicamas Sistēmas risku pārvaldībai:

8.2.2.1. Riska pieņemšana;

8.2.2.2. Riska pārvaldīšana;

8.2.2.3. Riska mazināšanas pasākumi.

8.3. Risku analīze ir jāveic visā IS dzīves ciklā ar šajā plānā noteikto regularitāti.

8.4. Risku analīzes veikšanā izmanto IS drošības apdraudējumu uzskaitījumu.

8.5. Risku analīzes veikšanu nodrošina, iesaistot atbildīgās personas par Sistēmas drošības pārvaldību.

8.6. Riska mazināšanas pasākumi tiek noteikti, pamatojoties uz to izmaksu un iespējamo zaudējumu samērojamību.

8.7. Katram riska mazināšanas pasākumam IS tiek noteikta atbildīgā persona un iespējamais izpildes termiņš.

8.8. Atbildīgā persona par Sistēmas drošības pārvaldību kontrolē risku mazināšanas pasākumu ieviešanu.

8.9. Risku analīze tiek veikta, balstoties uz dokumentā “IS drošības risku analīzes noteikumi” (KPDC.DP.7_IS_drosibas_risku_analizes_noteikumi) aprakstīto metodiku.

8.10. Balstoties uz IS drošības risku analīzes rezultātiem, tiek sagatavoti drošības risku mazināšanas pasākumi.

8.11. Katras nākamās risku analīzes laikā Atbildīgā persona par Sistēmas drošības pārvaldību novērtē katru riska mazināšanai veikto pasākumu lietderību.

8.12. Gadījumā, ja riska mazināšanas pasākums ir bijis nelietderīgs (piemēram, attiecīgais riska līmenis nav samazinājies), nosaka citu risku mazināšanas pasākumu.

8.13. IS drošības risku mazināšanas pasākumu plānu pārskata vismaz reizi gadā, kā arī šādos gadījumos:

8.13.1. Ja izmaiņas IS var ietekmēt Sistēmas drošību;

8.13.2. Ja ir mainījušies vai atklāti jauni IS drošības apdraudējumi;

8.13.3. Ja pieaug IS drošības incidentu skaits vai noticis nozīmīgs Sistēmas drošības incidents.

8.14. Ja, pārskatot plānu, konstatēta atbilstoša nepieciešamība, to aktualizē.

9. Drošības kritēriji

9.1. IS nepārtrauktās darbības laiks ir 24 stundas 7 dienas nedēļā.

9.2. Atbalsts tīkla pieslēguma punktiem ir jānodrošina 365 (366) dienas gadā.

9.3. Drošības incidentu iestāšanās gadījumā, tiek veiktas darbības, saskaņā ar KpDC IS drošības incidentu vadības noteikumiem un IS darbības nepārtrauktības atjaunošanas plānu.

10.IS drošības politikas izpildes kontrole

10.1. Pēc nepieciešamības, bet ne retāk, kā reizi gadā, tiek organizēts IS drošības audits, kas nodrošina IS atbilstību drošības politikai.

10.2. Pēc nepieciešamības, tiek organizētas IS incidentu vadības procedūras pārbaudes.

10.3. IS drošības pārvaldnieks iepazīstina KpDC darbiniekus ar IS drošības politiku.

10.4. IS drošības pārvaldnieks organizē un kontrolē visus Uzņēmuma IS resursu, to īpašnieku, aizbildņu un lietotāju uzskaiti.

10.5. Reizi gadā IS drošības pārvaldnieks organizē risku pārskatīšanu.

11.Noslēguma jautājumi

11.1. IS drošības politiku pārskata vismaz reizi gadā, ka arī šādos gadījumos:

11.1.1. ja izmaiņas sistēmā var ietekmēt sistēmas drošību;

11.1.2. ja mainījušies vai ir atklāti jauni sistēmas drošības apdraudējumi;

11.1.3. ja pieaug sistēmas drošības incidentu skaits vai noticis nozīmīgs sistēmas drošības incidents.

11.2. Ja, pārskatot politiku, konstatēta atbilstoša nepieciešamība, to aktualizē.