Informācijas sistēmu drošības pārbaudes vadlīnijas

VARAM, E-pārvaldes departaments; eparvalde@varam.gov.lv

Ievads

Pēdējo gadu laikā mēs ikdienas dzīvē arvien vairāk izmantojam elektronisko datu apstrādi. Valsts pārvaldes sektors nav izņēmums. Informācijas tehnoloģijas tiek izmantotas gan valsts organizāciju darbības atbalstam, gan pakalpojumu sniegšanai valsts iedzīvotājiem. Ar Ministru kabineta 2006.gada 19.jūlijā rīkojumu Nr.542 ir apstiprinātas "Informācijas sabiedrības attīstības pamatnostādnes 2006. – 2013.gadam". Dokumentā tiek uzsvērta nepieciešamība attīstīt informācijas sabiedrību, it sevišķi e-pārvaldi, jo tas pozitīvi ietekmē valsts pārvaldes pakalpojumu kvalitāti un pieejamību, kā arī sekmē efektīvāku, ekonomiskāku, demokrātiskāku un atklātāku pārvaldes darbu. Balstoties uz šīm pamatnostādnēm valsts pārvalde, lai īstenotu valsts funkciju izpildi un iedzīvotājiem sniegtu pakalpojumus pēc iespējas efektīvāk, attīsta un veido informācijas sistēmas.

Informācijas sistēmu uzkrāto datu izmantošana nenoliedzami sniedz būtiskus uzlabojumus daudzās dzīves jomās, tomēr līdz ar priekšrocībām parādās jauni apdraudējumi, kas var ietekmēt infromācijas pieejamību, veselumu un konfidencionalitāti. Lai varētu kontrolēt to ietekmi ir nepieciešamība pievērst papildus uzmanību informācijas sistēmu drošībai. Jo vairāk kāda iestāde izmanto informācijas sistēmas, jo vairāk ir dažādu informācijas drošības apdraudējumu, ar kuriem tai ir jāsastopas.

Informācijas sistēmu drošības pārbaudes vadlīnijām (turpmāk - Vadlīnijas) ir rekomendējošs raksturs. Vadlīnijās izmantoti materiāli no Amerikas Nacionālā standartu un tehnoloģiskā institūta.

Vadlīniju izstrādes mērķis

Vadlīnijas ir veidotas ar mērķi definēt valsts iestāžu pārziņā esošās informācijas sistēmu minimālās drošības prasības.

Vadlīnijas vispārējā līmenī nosaka minimālo drošības kontroļu kopu, kas iestādei jānodrošina informācijas sistēmai, to kopumam un informācijas tehnoloģiju infrastruktūrai.

Vadlīnijās aprakstītās minimālās drošības prasības var piemērot iestāžu funkciju atbalsta informācijas sistēmām (grāmatvedības, lietvedības, personāla, utt. informācijas sistēmām).

Jāņem vērā, ka izstrādātās vadlīnijas nav uztveramas kā paraugs, bet gan kā ceļvedis individuālu un iestādei piemērotu informācijas sistēmu drošības kontroļu pārvaldības ieviešanā. Šajā procesā ir nozīmīgi ņemt vērā informācijas sistēmas sarežģītību, veiktos risku analīzes rezultātus, pieejamos resursus un vajadzības, kas dažādās iestādēs var būtiski atšķirties. Drošības prasību ieviešanai ir jābūt samērīgai ar piejamo resursu un piešķirto līdzekļu apjomu.

Vadlīniju pielietošana

Valsts iestādēm, lai ievērotu normatīvo aktu prasībās noteikto informācijas drošību, jānosaka atbilstošākos un piemērotākos informācijas aizsardzības līdzekļus, kas būtu efektīvi un finansiāli izdevīgi attiecībā pret informāciju, ko tā aizsargā. Izvēlēties atbilstošāko drošības aizsardzības līdzekļu kopumu, kas atbilstu iestādes noteiktām drošības prasībām nav viegls uzdevums, tai pašā brīdī, svarīgs uzdevums, kas demonstrē iestādes izpratni par informācijas drošību un, ka tā ar lielu atbildības sajūtu spēj nodrošināt informācijas sistēmās uzkrāto datu konfidencionalitāti, veselumu, un pieejamību.

Lai palīdzētu institūcijām to pārziņā esošajām informācijas sistēmām izvēlēties piemērotākos informācijas sistēmu aizsardzības līdzekļus - ievests jēdziens minimālās prasības. Minimālās informācijas sistēmu drošības prasības – bāze informācijas drošību aizsardzības kontroļu izvēlei. Iestāde atbilstoši tās noteiktām drošības prasībām, lai samazinātu drošības apdraudējumus var paugstināt informācijas drošības līmeni, papildinot minimālās prasības ar papildus kontrolēm.

Auditorija

Vadlīnijas paredzētas:

1.Personām, kuras pārrauga informācijas sistēmu vai pārvalda informācijas drošību un ir atbildīgas par informācijas drošību iestādē (iestādes vadība, IT nodaļas vadītāji, informācijas drošības pārvaldnieki utt.);

2.Personām, kuras attīsta informācijas sistēmas (programmu un projektu vadītājiem, informācijas komunikāciju tehnoloģiju attīstītājiem, informācijas sistēmu analītiķiem un izstrādātājiem, sistēmu integrātoriem);

3.Personām, kuras ir atbildīgas par informācijas drošības ieviešanu un atbalsta funkcijām (atbildīgie par iestādes doto uzdevumu izpildi, informācijas resursu īpašnieki, pārraugiem, informācijas īpašniekiem, informācijas sistēmu drošību inženieriem, informācijas sistēmu administratoriem utt.);

4.Personām, kas ir atbildīgi par informācijas sistēmu un informācijas sistēmu drošības novērtēšanu un monitorēšanu (auditors, inspektori, sistēmu novērtētāji, neatkarīgie novērtētāji).

Saturs

1.Sadaļa

Drošības prasības informācijas sistēmai

1.Saime: Piekļuves kontrole Klase: Tehnoloģijas

1.1 .Piekļuves kontroles politika un procedūras

Kontrole: Iestāde izstrādā, apstiprina un pārskata vai papildina vismaz vienu reizi gadā vai pēc būtiskām izmaiņām:

1.1.1.Piekļuves kontroles politiku pie informācijas sistēmas, kurā nosaka mērķus, apjomu, lomas, atbildības, vadības atbildību, sadarbību ar citām struktūrvienībām vai institūcijām kā arī atbilstību normatīvajiem aktiem, un nozares politikas plānošanas dokumentiem;

1.1.2.Procedūras, lai atvieglotu piekļuves kontroles politikas īstenošanu.

1.2. Lietotāju kontu pārvaldīšana

Kontrole: Iestāde pārvalda informācijas sistēmu lietotāju kontus (pilnvarotas personas/grupas, izveidoto personificēto darba vietu, kura satur lietotāja identifikācijas un personificētu informāciju darbam ar informācijas sistēmu. Informācijas sistēmas saturošā informācija ir pieejama lietotājam tikai pēc tā pilnvaru pārbaudes (autorizācijas)), tai skaitā:

1.2.1.Lietotāju kontus iedala pēc tā tipa (lietotāji, grupa, sistēma/s, aplikācijas, viesis/anonīms, un pagaidu lietotāju konti);

1.2.2.Izstrādā īpašus nosacījumus darbam ar informācijas sistēmas saturošo informāciju vienas vai vairāku grupu ietvaros;

1.2.3.Identificē lietotājus, kuri ir pilnvaroti darbam ar informācijas sistēmu, un specificē to piekļuves tiesības;

1.2.4.Pilnvaro, kontu:

1.2.4.1.aktivizēšanai, pārveidošanai, bloķēšanai un dzēšanai;

1.2.5.Autorizē, kontrolē un monitorē viesis/ anonīms lietotājus, kā arī pagaidu kontus;

1.2.6.Informē lietotāju kontu pārvaldnieku (administrātoru), gadījumos, kad lietotāju konti vairs nav nepieciešami, vai informācijas sistēmas lietotāji pārtrauc lietot sistēmu, kā arī gadījumos, ja tie tiek rotēti citos amatos, vai arī nosaka jaunus piekļuves tiesību līmeņus informācijas sistēmā;

1.2.7.Deaktivizē: (i) pagaidu lietotāju kontus, kuri vairs nav nepieciešami, un (ii) kontus, kuru lietotāji ir beiguši darba tiesiskās attiecības vai pārcelti citos amatos;

1.2.8.Piekļuvi informācijas sistēmai nodrošina (i) darba pienākumu veikšanai; un (iii) cits pamatojums atbilstoši iestādes noteiktajiem mērķiem/funkcijām, un

1.2.9.Regulāri auditē lietotāju kontus [Iestādes definē laika periodu].

1.3. Piekļuves nodrošināšana

Kontrole: Piekļuvi informācijas sistēmai (loģisku) nodrošina atbilstoši izstrādātai piekļuves kontroles politikai.

Papildus vadlīnijas: Piekļuves kontroles politika (piemēram, lietotāja autorizācijas politika, lomu politika) un piekļuvi realizējošie mehānismi (piemēram, piekļuves kontroles saraksti (ACL), piekļuves kontroles matricas, kriptogrāfija), izmanto, lai kontrolētu lietotāju (vai to inicētos procesus) un objektu (piemēram, iekārtas, datu bāzes, procesus, programmas, citas informācijas sistēmas) piekļuvi informācijas sistēmai. Lai nodrošinātu papildus drošību piekļuves kontrolēm (novērst noteikto bāzes kontroļu apiešanu), iestāde var iestrādāt papildus kontroles aplikāciju līmenī.
Ja kriptogrāfiskā atslēgu izmanto kā piekļuves kontroli, tad kriptogrāfijas metodēm jābūt izstrādātām saskaņā ar iestādes vadlīnijām. Piekļuvei pie klasificētas informācijas, kriptogrāfijas mehānismus izmanto atkarībā no informācijas klasifikāciju līmeņa.

1.4. Nesekmīgi informācijas sistēmas lietošanas mēģinājumi

Kontrole: Informācijas sistēmā:

1.4.1.Nosaka pieļaujamo nesekmīgo piekļuves mēģinājumu maksimālo skaitu noteiktā laika periodā [Pielietojums: iestāde nosaka maksimālo piekļuves skaitu], un;

1.4.2.Automātiski [izvēle: slēdz lietotāju kontu/mezglu [Pielietojums: iestāde definē laika periodu] slēdz kontu/mezglu līdz administrators to atbloķēs; novilcina nākamās pieslēgšanās mēģinājumu uz noteiktu laika periodu

[Pielietojums: iestāde definē algoritmu]], ja maksimālais nesekmīgo piekļuves mēģinājumu skaits ir pārsniedzis noteikto ierobežojumu. Minēto kontroli piemēro neatkarīgi no tā, vai piekļuves mēģinājums tiek veikts lokālajā datu pārraides tīklā vai publiskajā datu pārraides tīklā.

Papildus vadlīnijas: Aizsardzības mehānisms neveiksmīgiem pieslēgšanās mēģinājumiem var tikt īstenots gan operētājsistēmas gan aplikāciju līmenī.

1.5 Informācijas sistēmas brīdinājuma informācija

Kontrole: Informācijas sistēma:

1.5.1.Pirms uzsākot darbu ar informācijas sistēmu, lietotājs jābrīdina par lietošanas sekām, ko var izraisīt informācijas sistēmas lietošana neparedzētiem mērķiem. Brīdinājumā ietver informāciju, kurā norāda: (i) lietotājs piekļūst informācijas sistēmai; (ii) informācijas sistēmas lietošana var tik uzraudzīta un veiktās darbības var tikt reģistrētas, un pēc tam tikt auditētas; (iii) tiek veikta lietotāja identitātes pārbaude, (iiii) informācijas sistēmas nesankcionēta lietošana ir aizliegta un lietotājam var tikt piemēroti normatīvos aktos paredzētie sodi, un; (iv) piekrītot izmantot informācijas sistēmu, lietotājs tiek informēts,par to, ka tā veiktās darbības informācijas sistēmā tiks kontrolētas. Iestādes informācijas sistēmu lietotājus var brīdināt iekļaujot šo normu informācijas sistēmu lietošanas noteikumos;

1.5.2. Brīdinājuma informāciju izgaismo uz ekrāna līdz brīdim, kamēr lietotājs veiks visas tās nepieciešamās darbības, kas nepieciešamas reģistrācijai informācijas sistēmā;

1.5.3.Publiski pieejamām informācijas sistēmām: (i) brīdinājuma informāciju izgaismo, kamēr lietotājs nav uzsācis darbu ar informācijas sistēmu, (ii) uz ekrāna redzamā vietā izvieto norādes, kuras informē lietotāju, ka informācijas sistēma tiek monitorēta, visas veiktās darbības tiek reģistrētas un auditētas atbilstoši privātuma nosacījumiem, un (iii) paziņojumā ietver informāciju, kā var kļūt par informācijas sistēmas autorizētu lietotāju.

Papildu vadlīnijas: Brīdinājuma informāciju var veidot interaktīvi kopā ar pieslēgšanās saskarni.

1.6. Aktivātes, kurām nepieprasa lietotāju identifikāciju vai autentifikāciju

Kontrole: Iestāde:

1.6.1.Auditē visas darbības, kuras tiek veiktas bez identifikācijas un autentifikācijas un;

1.6.2.Dokumentē informācijas sistēmas drošības plānā tādas lietotāja aktivitātes, kam nav nepieciešama identifikācija un autentifikācija.

Papildu vadlīnijas: Šī kontrole ir paredzēta sevišķiem gadījumiem, kad iestāde nosaka, pie kādiem apstākļiem lietotāja identifikācija un autentifikācija nav nepieciešama. Tas nenozīmē, ka šādas iespējas var tikt dotas informācijas sistēmā. Iestādes identificē tās aktivitātes, kas normalā situācijā pieprasa lietotāju identifikāciju un autentifikāciju, bet noteiktos gadījumos (piem., ārkārtas situācijās) ļauj identifikācijas un autentifikācijas mehānismus apiet. Šāds risinājums var būt, piemēram, programmatoriska funkcija, kas dot iespēju apiet pieslēgšanās funkcionalitāti. Šo kontroli neizmanto gadījumos, kad lietotāja identifikācija un autentifikācija ir jau notikusi un netiek atkārtota, bet situācijās, kad identifikācija un/ vai autentifikācija vēl nav veikta.

1.7. Attālinātā (remote) piekļuve

Kontrole: Iestāde:

1.7.1.Nosaka mehānismus ar kādiem drīkst veikt attālināto piekļuvi informācijas sistēmai;

1.7.2.Katram attālinātam piekļuves mehānismam nosaka ierobežojumus, drošības prasības un izstrādā ieviešanas vadlīnijas;

1.7.3.Monitorē un žurnalē nesankcionētus attālinātos piekļuves mēģinājumus informācijas sistēmai;

1.7.4.Katru attālināto piekļuves pieprasījumu, pirms ar to izveido savienojumu ar informācijas sistēmu, autorizē.

Papildus vadlīnijas: Attālinātās piekļuves mehānismi: iezvanpieeja, platjoslas un bezvadu. Virtuālais privātais tīkls (VPN) ir visefektīvākais veids, kā nodrošināt informācijas slepenību un veselumu pārraidē izmantojot publiskos datu pārraides tīklus.

1.8. Bezvadu piekļuve

Kontrole: Iestāde:

1.8.1. Nosaka ierobežojumus, drošības prasības un izstrādā vadlīnijas bezvadu piekļuvei pie informācijas sistēmas un iestādes informācijas tehnoloģiju infrastruktūras;

1.8.2.Monitorē nesankcionētu bezvadu piekļūšanas mēģinājumus informācijas sistēmai un informācijas tehnoloģiju infrastruktūrai;

1.8.3.Visus bezvadu pieslēgumu ar informācijas sistēmu autorizē.

Papildus vadlīnijas: Bezvadu tehnoloģijas ietver: satelīta, pakešu radio (UHF / VHF), 802.11x un Bluetooth. Bezvadu tīkli lietošanas autentifikācijas protokoli, kuri nodrošina kredinciāļu aizsardzību un kopēju autentifikāciju - piemēram, EAP/ TLS, PEAP. Jāņem vērā, ka bezvadu signāli var tikt izstaroti ārpus iestādes robežām un informācijas drošību kontrolējošām iekārtām.

1.9 Piekļuves kontrole no mobilajām iekārtām

Kontrole: Iestāde:

1.9.1.Izstrādā piekļūšanas ierobežojumus un norādījumus kā lietot mobilās iekārtas;

1.9.2.Mobilo iekārtu izmantošanai darbam ar informācijas sistēmu izstrādā vadlīnijas;

1.9.3.Monitorē neautorizētu mobilo iekārtu pieslēgumus iestādes informācijas sistēmai;

1.9.4.Specificē prasības mobilo iekārtu savienojumiem darbam ar informācijas sistēmām;

1.9.5.Neizmanto tādu informācijas sistēmas funkcionalitāti, kas nodrošina iespēju automātiski mobilā ierīcē izpildīt kodu bez lietotāja norādījuma;

1.9.6.Nosaka īpašus iestatījumu prasības mobilo iekārtu īpašniekiem, kuri tos izmanto vietās, kas var radīt būtisku apdraudējumu atbilstoši iestādes politikai un procedūrām, un;

1.9.7.Mobilajām iekārtām, kas izmantotas vietās, kas atbilstoši iestādes politikai un procedūrām var radīt būtisku apdraudējumu, veic pārbaudes un profilakses [Pielietojums: iestādes definē pārbaudes un profilakses pasākumus] .

Papildu vadlīnijas: Mobilās iekārtas ietver portatīvo datu nesējus (piemēram, USB atmiņas kartes, ārējie cietie diskdziņi) un portatīvās skatļošanas iekārtas un sakaru iekārtas ar informācijas uzglabāšanas iespēju (piemēram, piezīmjdators/portatīvie datori, personālie digitālie asistenti, mobilie telefoni, digitālās kameras, un audio ierakstu iekārtas). Iestādes kontrolē mobilās iekārtas un to izmantošanai ir tiesīga noteikt ierobežojumus. Mobilo iekārtu

izmantošanas ierobežojumos un norādījumos ietver, piemēram, konfigurācijas iestatījumus, iekārtu identifikācijas un autentifikācijas obligāto aizsardzības programmatūru (piemēram, ļaunprātīgu kodu atklāšanas programmatūru, ugunsmūri), skenēšanas iekārtas ļaunprātīgu kodu atklāšanai, atjauninātu antivīrusu programmatūru, prasību veikt operētājsistēmas veseluma pārbaudi, kā arī noteikt tādas funkcionalitātes atslēgšanu, kā, piemēram, bezvadu internetu, infrasarkano un bluetooth raidītāju/uztvērējus un atslēgt funkcionalitāti, kas nodrošina iespēju automātisku izpildīt kodu „Autorun" un „AutoPlay".

Personāla mobilajām iekārtām, ko izmanto darba pienākumu pildīšanai ārpus iestādes, sanitarizē datoru cieto diskdzini, ierobežo aplikāciju izmantošanu vai iestata specifiskas iestatījumus. Visas mobilās iekārtas, kas tika izmantotas ārpus iestādes datu pārraides tīklam, pieslēdz karantīnas datu pārraides tīklam, kurā pārbauda uz datorvīrusu esamību un aplikāciju jauninājumiem. Mobilo iekārtu aizsardzība ietver sevī arī informācijas nesēju aizsardzību.

1.10. Ārējo informācijas sistēmu izmantošana

Kontrole: Iestādes nosaka kārtību un nosacījumus, saskaņā ar kuriem izveido sadarbību ar tām iestādēm, kuru pārziņā tiek uzturētas informācijas sistēmas, un kas nodrošina pilnvarotām personām:

1.10.1.Piekļuvi ārējām informācijas sistēmām;

1.10.2.Apstrādāt, uzglabāt, un/vai pārsūtīt iestādes informāciju, izmantojot ārējās informācijas sistēmas;

Papildu vadlīnijas: Ārējās informācijas sistēmas vai to komponentes nav iestādes tiešā uzraudzībā un parasti tā netiek pilnvarota novērtēt to drošības aizsardzības kontroļu efektivitāti vai veikt drošības atbilstības pārbaudes. Ārējās informācijas sistēmas ietver (i) komercstruktūru vai sabiedrisko iestāžu (piemēram, viesnīcas vai lidostas, autoostas utt.) datorus vai komunikāciju iekārtas, (iii) informācijas sistēmas, kuras pieder vai, kuras uztur nevalstiskas organizācijas un (iv) valsts pārvaldē esošās informācijas sistēmas, ko uztur iestādes. Informācijas sistēmas, kuru darbību nodrošina iestāde savām struktūrvienībām, nevar tikt uzskatītās kā ārējas sistēmas. Šādu sistēmas izmantošanai neslēdz līgumus, bet iestāde izdod iekšējos normatīvos aktus, kurā nosaka sadarbības nosacījumus kā arī pilnvaro atbildīgās personas. Tādējādi iestāde var piemērot stingrākus drošības ierobežojumus nekā to nosaka normatīvie akti.
Šī kontrole neattiecas uz ārējām informācijas sistēmām, kura nodrošina piekļuvi publiski pieejamai informācijas sistēmai (piemēram, piekļūšana www.likumi.lv publicētai informācijai). Iestāde nosaka kārtību un nosacījumus, kā izmantot ārējās informācijas sistēmas atbilstoši iestādes drošības politikai un procedūrām.

Kārtībā un nosacījumos nosaka minimumu; (i) no kādām ārējās informācijas sistēmu saskarnēm var piekļūt pie iestādes informācijas sistēmas, un (ii) maksimāli atbilstoši klasificē informāciju, ko var apstrādāt, uzglabāt un nosūtīt ārējai informācijas sistēmai.

1.11. Publiski pieejama informācija

Kontrole: Iestāde:

1.11.1.Pilnvaro personas, kuras ievieto informāciju publiski pieejamās informācijas sistēmās;

1.11.2.Pilnvarotas personas apmāca, lai tās varētu novērtēt vai publiski pieejama informācija nesatur konfidenciālu informāciju;

1.11.3.Pirms ievada informācijas sistēmā publiski pieejamu informāciju, to pārbauda vai tā nesatur konfidenciāla rakstura informāciju;

1.11.4.Regulāri pārbauda vai publiski pieejamā informācija nesatur informāciju, kas nav paredzēta publiskai apskatei [Pielietojums: Iestādes definē biežumu], un

1.11.5.Gadījumā, ja tiek konstatēta informācijas sistēmā publiskai apskatei neparedzēta informācija, to dzēš.

Papildu vadlīnijas: Publiskai apskatei neparedzēta informācija ir jebkura informācija, par ko plašai sabiedrībai netiek dota iespēja iepazīties atbilstoši LR normatīviem aktiem. Piemēram informācija par privāto dzīvi aizsargā Personu datu aizsardzības likums un tā ir nepubliskojama informācija. Šo kontroli paredz tām iestādes informācijas sistēmām, kas pieejama brīvi plašai sabiedrībai, un parasti piekļuve tai tiek nodrošināta bez identifikācijas vai autentifikācijas.

2.Saime: Drošības apmācības klase: Procesi

2.1. Drošības apmācības, izglītošanas politika un procedūras

Kontrole: Iestāde izstrādā, izplata un pārskata/atjaunina [Pielietojums: iestādes definē periodu]:

2.1.1.Drošības apziņas veicināšanas un izglītošanas politiku, kurā nosaka mērķus, apjomu, lomas, atbildības, vadības apņemšanos, sadarbību ar citām iestādes struktūrvienībām institūcijām un atbilstību likumiem;

2.1.2.Procedūras, lai atvieglotu drošības apziņas un izglītošanas politikas īstenošanu.

Papildus vadlīnijas: Drošības apzināšanas, izglītošanas politikas un procedūru kontrole nepieciešama, lai efektīvi īstenotu un uzlabotu izvēlētās drošības kontroles.

2.2. Drošības apziņas veicināšana

Kontrole: Iestāde nodrošina pamatdrošības jautājumiem veltītas apzināšanas apmācības visu sistēmu lietotājiem (iekļaujot augstākā līmeņa vadītājus, kā arī līgumdarbiniekus), kā arī gadījumos, kad tiek veiktas izmaiņas sistēmā.

Papildus vadlīnijas: Iestādes nosaka atbilstošu drošībai veltītu apmācību programmu un metodoloģiju atbilstoši tai informācijas sistēmai ar, kuru lietotāji ir pilnvaroti strādāt. Apmācību materiālā iekļauj bāzes zināšanas, kas nepieciešamas, lai nodrošinātu informācijas sistēmas drošību un lietotāja uzvedību atbilstoši pieņemtai iestādes drošības prasībām un attiecīgi reaģētu uz aizdomīgiem drošības incidentiem. Apmācību materiālā iekļauj informāciju, kas nepieciešamas drošības procesu realizācijai, kas atbilst iestādes informācijas drošības politikai. Drošības apziņas veicināšanai var izmantot, piemēram, elektroniskos bukletus, vadību izsūtītos e-pastus, kurā ietver informāciju par atgādinājumu ievērot informācijas drošību, izlecošos ielogošanās saskarnes „logus", kā arī sanāksmes, kurās tiek apspriesti ar drošību saistītie atgadījumi un sekas.

2.3 Drošības apmācības

Kontrole: Iestāde personālam, atbilstoši to ieņemamajiem amatiem un atbildībām, rīko ar informācijas drošību saistītas apmācības: (i) piešķirot pirmreizējo piekļuvi informācijas sistēmai, vai uzdodot veikt jaunus pienākumus, (ii) pēc veiktām izmaiņām sistēmā, un; (iii) vismaz reizi gadā.

Papildu vadlīnijas: Iestāde nosaka atbilstošu drošības apmācību saturu ieņemamajiem amatiem un atbildībām, un īpašas prasības, kas nepieciešamas autorizētam personālam darbam ar informācijas sistēmu. Iestāde apmācības veic informācijas sistēmu pārvaldniekiem, sistēmas un tīkla administratoriem, personālam, kas veic neatkarīgas pārbaudes un novērtē atbilstību noteiktām prasībām, drošības kontroles novērtētājiem un personālam, kam piesķirta piekļuve sistēmas līmeņa programmatūrai. Ar drošību saistītās apmācības ir pietiekamas, lai droši veiktu uzticētos pienākumus. Iestādes drošības apmācības programmā iekļauj pārvaldību, procesus, tehnisko atbalstu un atbildības, kas attiecas uz fizisko, personāla, un tehnisko aizsardzības līdzekļu, preventīvo un fizisko aizsardzību.

2.4. Drošības apmācību dokumentēšana

Kontrole: Iestāde:
2.4.1.Dokumentē informāciju par mācībām;

2.4.2.Saglabā individuālās apmācību rezultātus [Pielietojums: iestādes nosaka periodu].

Papildu vadlīnijas: iestāde organizē padziļinātas, ja nepieciešams ar drošību saistītās mācības.

3.Saime: Žurnalēšana klase: Tehnoloģijas

3.1. žurnalēšanas politika

Kontrole: Iestāde izstrādā, izplata un pārskata/atjaunina [Pielietojums: Iestādes nosaka biežumu]:
a.Žurnalēšanas politiku, kurā nosaka mērķus, apjomu, laika intervālu, lomas, atbildības, vadības atbildību, sadarbību ar citām struktūrvienībām un institūcijām un atbilstību normatīvajiem aktiem; un
b.Procedūras, lai atvieglotu žurnalēšanas politikas īstenošanu.

3.2. Notikumu žurnāls

Kontrole: Iestāde:

3.2.1.Informācijas sistēmas notikumu žurnālā aktivitātes reģistrē pamatojoties uz riska analīzes novērtējumu un iestādes mērķiem [Pielietojums: Iestādes definē auditējamo vienību sarakstu];

3.2.2.Notikumu žurnāla saturu nosaka sadarbojoties ar iestādes struktūrvienību informācijas resursu īpašniekiem;

3.2.3.Racionāli izvērtē vai notikumu žurnāla saturs ir uzskatāms par pietiekošu, lai to varētu izmantot notikušo drošības incidentu izmeklēšanā un ietekmes novērtēšanai; un

3.2.4.Informācijas sistēmas notikumu žurnāla saturu nosaka, pamatojoties uz pašreizējo informāciju par draudiem un aktuālo risku novērtējumu: [Auditēšanu veic atbilstoši iestādes biežumam (vai situācijā, kad nepieciešams)].

Papildus vadlīnijas: Iestādei nosaka informācijas sistēmas notikumu žurnāla saturu atbilstoši to nozīmīgumam un drošības nepieciešamībai. Nosaka vispārējās informācijas sistēmu prasības, lai nodrošinātu, ka notikumu žurnāla saturs atbilstu aktuālai situācijai. Piemēram, iestāde var noteikt, ka informācijas sistēma ģenerē atskaiti katram failu piekļūšanas gadījumam (sekmīgs un nesekmīgs), bet neaktivizē šo iespēju gadījumos, kad tas sāk spēcīgi noslogot informācijas sistēmas veiktspēju. Ģenerēt notikumu žurnāla sarakstu var arī pakešu līmenī, tas ir, reģistrēt notikumus datu pārraides tīklā.

3.2. Notikumu žurnāla saturs

Kontrole: Informācijas sistēma ģenerē notikuma žurnālā ierakstus, kas satur pietiekamu informāciju, lai vismaz noteiktu, kāda veida notikums tas ir (skatīts, labots, dzēsts, izveidots utt), kad noticis (datums un laiks) , kur noticis, avots, rezultāts (sekmīgs vai nesekmīgs), kā arī jebkura lietotāja identifikācijas informācija, ar kuru saistīts notikums.

3.3. Notikuma žurnāla ierakstu kapacitāte

Kontrole: Iestāde nodrošina atbilstošu kapacitāti (atmiņas apjomu) notikuma žurnāla ierakstu uzglabāšanai un kontrolē to apjomu, lai tā nepārsniegtu noteikto ierobežojumu.

3.5. Reaģēšana uz žurnalēšanas kļūmēm

Kontrole: informācijas sistēma:

3.5.1.Brīdinājumus par žurnalēšanas kļūmēm realizē tā, lai iestādes atbildīgās amatpersonas par to tiktu savlaicīgi informētas, un

3.5.2.Veic sekojošas darbības: [Pielietojums: Iestādes noteikti pasākumi, kas jāveic (piemēram, aptur informācijas sistēmas darbību, pārraksta vecos žurnāla ierakstus (iepriekš izveidojot rezerves datu kopiju žurnāla ierakstiem), apstādina žurnāla ierakstu ģenerāciju)].

Papildus vadlīnijas: Notikumu žurnāla ierakstu kļūmes ir, piemēram, programmatūras / aparatūras kļūdas, nepilnības žurnalējamo ierakstu iegūšanas mehānismos, kā arī notikumu žurnāla neatbilstoša kapacitāte.

3.6. Notikumu žurnāla ierakstu pārskati, analīze un atskaites

Kontrole: Iestāde:

3.6.1.Pārskata un analizē informācijas sistēmu notikumu žurnāla reģistrētos ierakstus [Pielietojums: Iestāde definē biežumu], lai atklātu neatbilstības vai netipiskas aktivitātes, un sniegtu atskaiti iestādes atbildīgajām amatpersonām, un;

3.6.2.Patstāvīgi pārskata informācijas sistēmas notikumu žurnāla saturu atbilstoši veiktām pārbaudēm un analīzēm. Kā arī tad, kad parādās vai mainās apdraudējumi iestādes procesiem, aktīviem, indivīdiem un citām organizācijām vai valstij, pamatojoties uz drošības iestāžu vai citu uzticamu avotu sniegto informāciju.

3.7. Laika zīmogs

Kontrole: informācijas sistēmā sinhronizē iekšējo sistēmas laiku, lai ģenerētu laika zīmogus notikuma žurnāla ierakstiem.

Papildus vadlīnijas: Informācijas sistēmā laika zīmogi ietver datumu un laiku. Laiku var sinhronizēt atbilstoši universālajam koordinētajam laikam (UTC), Griničas laiks (GMT) vai vietējā laika UTC starpību. Latvijā administrātori var sinhronizēt informācijas sistēmas laiku ar Latnet serveriem (ntp.latnet.lv).

3.8. Notikumu žurnāla aizsardzība

Kontrole: Informācijas sistēmas notikumu žurnāla saturošo informāciju un žurnalējamos rīkus aizsargā no neautorizētas piekļuves, modifikācijas un dzēšanas.

3.9. Notikumu žurnāla satura arhivēšana

Kontrole: Iestāde arhivē žurnāla saturu [Pielietojums: atbilstoši žurnāla arhivēšanas politikai], lai nodrošinātu atbalstu drošības incidentu izmeklēšanai un izpildītu kontrolējošo institūciju prasības attiecībā uz informācijas saglabāšanu.

Papildu vadlīnijas: Iestādes uzglabā žurnāla saturu līdz brīdim kamēr netiks kontatēts, ka tie vairs nav nepieciešami administratīviem, tiesu, revīzijas, vai citiem nolūkiem. Pieejamību notikumu žurnālam jānodrošina atbilstoši LR normatīvajiem aktiem.

3.10. Notikumu žurnāla ierakstu ģenerēšana

Kontrole: informācijas sistēma:

3.10.1.Iestāde nosaka atbildīgās personas, kuras nosaka kādus ierakstus jāreģistrē notikumu žurnālā;

3.10.2.Notikumu žurnālā ierakstus reģistrē atbilstoši definētam sarakstam.

4.Saime: Drošības pārbaudes un novērtēšana Klase: Pārvaldība

4.1. Drošības pārbaudes un novērtēšanas politika un procedūras

Kontrole: Iestāde izstrādā, izplata un pārskata/ atjaunina [Pielietojums: Iestādes definē biežumu]:

4.1.1.Drošības pārbaužu veikšanas un riska novērtēšanas politiku, kurā nosaka mērķus, uzdevumus, pienākumus, vadības atbildību, sadarbību starp iestādes struktūrvienībām un atbilstību likumiem, un

4.1.2.Procedūras, lai atvieglotu drošības pārbaužu veikšanu un riska novērtēšanas politikas ieviešanu.

4.2. Drošības atbilstības pārbaude

Kontrole: Iestāde:

4.2.1.Pirms nodot informācijas sistēmu ekspluatācijā tai veic drošības atbilstības pārbaudi;

4.2.3.Periodiski veic drošības pārbaudes [Pielietojums: Iestādes definē periodu];

4.2.4.Nozīmē atbildīgo personu (no vadošo darbinieku vides), kas būs atbildīga par informācijas sistēmas drošības atbilstības pārbaudi;

4.2.5.Izstrādā drošības pārbaužu prasību plānu, kurā apraksta novērtējumu sfēru, kurā iekļauj:

4.2.5.1.Drošības kontroles un atbilstoši novērtējumam nepieciešamos uzlabojumus;

4.2.5.2.Novērtēšanas procedūras, kuras tiks izmantotas, lai noteiktu drošības kontroļu efektivitāti; un;

4.2.5.3.Novērtējuma vidi, personālu, kas iesaistīti drošības atbilstības pārbaudē un nosaka tā lomas un pienākumus;

4.2.5.4.Novērtē informācijas sistēmas drošības kontroles [Pielietojums: Iestādes definē biežumu], lai noteiktu, cik lielā mērā kontroles ir ieviestas korekti, vai darbojas kā ieplānots, un nodrošina to aizsardzības līmeni, kā to nosaka informācijas sistēmas drošības prasības;
4.2.5.5.Izstrādā drošības pārbaužu novērtējuma atskaiti, kurā dokumentē novērtējuma rezultātus;

4.2.5.6. Rezultātus, kas tika iegūti drošības pārbaužu pasākuma laikā, rakstiski iesniedz iestādes atbildīgām personām.

Papildu vadlīnijas: Iestāde novērtē informācijas sistēmas drošības kontroles šādos gadījumos: (i) drošības novērtējuma atbilstības vai neatbilstības; (ii) normatīvajos aktos noteiktajā kārtībā; (iii) pastāvīgi monitorējot, un; (iv) testējot/novērtējot informācijas sistēmu kā daļu no sistēmas izstrādes dzīves cikla procesa. Drošības pasākumu atbilstības novērtējuma ziņojumā dokumentētos rezultātus pietiekami detalizē, lai iestādes atbildīgās personas būtu informētas vai drošības kontroles īstenotas pareizi, darbojas kā tas ir bija iecerēts, un sniedz vēlamo rezultātu atbilstoši informācijas sistēmas drošības prasībām.

4.3. Pieslēgumi citu iestāžu informācijas sistēmām

Kontrole: Iestāde:

4.3.1.Pieslēgumu citu iestāžu pārziņā esošajām informācijas sistēmām atrunā līgumos vai rīkojas atbilstoši normatīvajos aktos noteiktajai kārtībai;

4.3.2.Katru savienojumu, to saskarņu parametrus, drošības prasības un savienojuma veidus atbilstoši dokumentē;

4.3.3.Pieslēgumus pie informācijas sistēmas uzrauga atbilstoši drošības prasībām.

Papildus vadlīnijas: Šī kontrole attiecas uz slēgumiem starp starpsistēmu saskarnēm un neattiecina uz lietotāju atbalsta programmatūru, piemēram, e-pastu un interneta pārlūkošanu. Iestādes pirms savienojuma izveides rūpīgi novērtē iespējamos apdraudējumus, kas var rasties slēdzot informācijas sistēmas ar sistēmām, kurām ir atšķirīgas drošības prasības un drošības kontroles. Atbildīgās personas par drošību nosaka kādi apdraudējumi var rasties izveidojot slēgumus ar citām informācijas sistēmām, kā arī nosaka kādas drošības kontroles ir jāievieš.

4.4.Rīcības plāns ievainojamību vai trūkumu novēršanai un mazināšanai

Kontrole: Iestāde:

4.4.1.Informācjas sistēmai izstrādā rīcības plānu ievainojamību vai trūkumu novēršanai un mazināšanai, kas atklātas informācijas sistēmu drošības kontroļu novērtējuma laikā;

4.4.2.Atjauno rīcības plānu ievainojamību vai trūkumu novēršanai un mazināšanai [Pielietojums: Iestādes definē periodu], pamatojoties uz drošības novērtējuma laikā iegūtiem datiem un draudu ietekmes analīzi.

4.5.Informācijas sistēmas darbības monitorēšana

Kontrole: Iestāde nosaka informācijas sistēmu darbības monitorēšanas stratēgiju, kurā ietver:

4.5.1.Konfigurācijas pārvaldības procesus informācijas sistēmai un to saistītiem komponentiem;

4.5.2.Informācijas sistēmas un to procesu vides konfigurācijas ietekme uz drošību;

4.5.3.Drošības kontroles novērtē atbilstoši iestādes darbības nepārtrauktības stratēģijai;

4.5.4.Vienreiz gadā informē atbildīgās par informācijas drošību iestādes par drošības stāvokli iestādē;

Papildus vadlīnijas: Informācijas sistēmas darbības monitorēšanas stratēģija ļauj iestādei uzturēt informācijas sistēmas drošu darbību dinamiskā vidē ar mainīgiem apdraudējumiem, ievainojamībām, tehnoloģijām un biznesa procesiem. Drošības kontroļu darbības monitorēšanu nodrošina izmantojot automātiskus līdzekļus atbilstoši riska pārvaldībai un iestādes izpratnei attiecībā uz drošības stāvokli informācijas sistēmā. Darbības monitorēšanas stratēģija var ietvert drošības novērtējuma ziņojumus, rīcības plānus un mērķus. Labi veidota darbības monitorēšanas stratēģija būtiski samazina pūles veicot drošības pārbaudes informācijas sistēmai.

5.Saime: Konfigurācijas pārvaldība Klase: Procesi

5.1. Konfigurācijas pārvaldības politika un procedūras

Kontrole: Iestāde izstrādā, izplata un pārskata / atjaunina [Pielietojums: Iestāde definē periodu]:

5.1.1.Konfigurācijas pārvaldības politiku, kurā nosaka mērķus, apjomu, lomas, atbildības, vadības atbildību, sadarbību ar citām iestādes struktūrvienībām un institūcijām, un atbilstību normatīvajiem aktiem;

5.1.2.Procedūras, lai atvieglotu konfigurācijas pārvaldības politikas īstenošanu.

5.2. Bāzes konfigurācija

Kontrole: Iestāde nodrošina informācijas sistēmas bāzes konfigurācijas aizsardzību un to attiecīgi dokumentē.

Papildus vadlīnijas: Informācijas sistēmas bāzes konfigurācijā ietilpst tās sastāvdaļas, datu pārraides savienojumi un to parametri. Bāzes konfigurācija satur informāciju par informācijas sistēmas tehnisko infrastruktūru (piemēram, standarta programmatūras slodze, darbstaciju, serveru, operētājsistēmu/instalētās programmas ar esošo versiju numuriem un atjauninājumiem utt.), datu pārraides tīkla topoloģijas komponentiem, un loģisko komponenšu izvietojumu informācijas sistēmas arhitektūrā. Bāzes konfigurāciju dokumentē atbilstoši uz aktuālo datumu. Konfigurācijā iekļauj informāciju par sistēmā veiktajām izmaiņām. Bāzes konfigurāciju aprakstu atjauno pēc katrām veiktajām izmaiņām informācijas sistēmā.

5.3. Konfigurāciju ietekmes analīze uz drošību

Kontrole: Iestāde

5.3.1.Pirms veic izmaiņas informācijas sistēmā, iestāde izvērtē potenciālo drošības risku analīzi.

Papildu vadlīnijas: Personām, kas veic drošības risku analīzi, ir jābūt nepieciešamajām prasmēm un tehniskām zināšanām, lai spētu novērtēt ietekmi uz informācijas sistēmu un to iespējamām sekām. Drošības ietekmes analīzē var ietvert, piemēram, informācijas sistēmas dokumentāciju izvērtēšanu, piemēram, drošības plānu, lai saprastu, kādas drošības kontroles tika veiktas sistēmā un to, kā tā varētu ietekmēt drošības kontroli.

5.4. Informācijas sistēmu komponenšu un to sastāvdaļu konfigurācija

Kontrole: Iestāde:

5.4.1.Nosaka un dokumentē obligātos konfigurācijas iestatījumus informācijas tehnoloģiju komponentēm, ko izmanto informācijas sistēmā [Pielietojums: iestādes nosaka drošus konfigurācijas iestatījumus];

5.4.2.Visus konfigurācijas iestatījumu izņēmumus, atsevišķām informācijas sistēmas sastāvdaļām vai to komponentēm, identificē un dokumentē;

5.4.3.Konfigurācijas parametrus kontrolē un uzrauga atbilstoši konfigurācijas politikai un procedūrām.

Papildu vadlīnijas: Konfigurācijas parametri var tikt veikti kontu failiem un direktorijām, pakalpojumu iestatījumos, portiem, protokoliem un datu savienojumiem. Iestāde nosaka obligātos konfigurācijas parametrus un izstrādā drošas konfigurēšanas vadlīnijas vai arī tās iegūst no informācijas tehnoloģiju izstrādātājiem un piegādātājiem . Vadlīnijās ietver norādījumus un procedūras kā droši konfigurēt informācijas sistēmas un to komponentes.

5.5. Minimālā funkcionalitāte

Kontrole: Iestāde konfigurē informācijas sistēmas darbināšanas vidi tā, lai nodrošinātu tikai būtisku funkciju izpildi un īpaši aizliedz vai ierobežo nevajadzīgo funkciju darbināšanu, piemēram, portus, protokolus un citus: [Pielietojums: Iestādes definē aizliegto un ierobežoto funkciju sarakstu, portus, protokolus, un pakalpojumus].

Papildus vadlīnijas: Dažas funkcijas un pakalpojumus, ko sniedz pēc noklusējuma, lai atbalstītu būtisku funkciju darbību var nebūt nepieciešami. Turklāt, reizēm ir ērti nodrošināt vairākus pakalpojumus ar vienu informācijas sistēmu, bet to darot palielinās risks pārējiem pakalpojumiem. Ja iespējams, iestādes iespēju robežās katram pakalpojumam nodrošina atsevišķu informācijas sistēmu (piem., e-pastam un web, bet ne abus). Iestādes izvērtē nevajadzīgu fizisku un loģisku portu, protokolu (piemēram, USB, FTP, IPv6, HTTP) nepieciešamību, jo tas rada draudus nesankcionēti izmantot sistēmu. Iestādes var izmantot tīkla skenēšanas rīkus, ielaušanās atklāšanas un novēršanas sistēmas, ieejas un izejas punktu aizsardzību, piemēram, ugunsmūri, lai identificētu un novērstu aizliegtu funkciju, portu, protokolu, un pakalpojumu lietošanu.

6.Saime: Darbības nepārtrauktības plānošana Klase: Procesi

6.1. Darbības nepārtrauktības politika un procedūras

Kontrole: Iestāde, izplata un pārskata/atjaunina [Pielietojums: Iestādes definē periodu]:

6.1.1.Darbības nepārtrauktības politiku, kurā nosaka mērķus, apjomu, lomas, atbildības, vadības atbildību, sadarbību ar citām iestādes struktūrvienībām un institūcijām, un atbilstību likumiem, un;

6.1.2.Procedūras, lai atvieglotu darbības nepārtrauktības politikas īstenošanu

6.2.Darbības nepārtrauktības plāns

Kontrole: Iestāde:

6.2.1.Izstrādā ārkārtas rīcības plānu attiecībā uz informācijas sistēmu, kurā:

6.2.1.1.Identificē būtiskas darbības funkcijas, kurām jānodrošina nepārtrauktība;

6.2.1.2.Nodrošina objektu atjaunošanu, atjaunošanas prioritātes, un metrikas;

6.2.1.3.Nozīmē par darbības nepārtrauktību atbildīgās personas, nosaka lomas, apkopo kontaktinformāciju;

6.2.1.4.Uztur būtiskas darbības funkcijas par spīti informācijas sistēmas traucējumiem vai atteicēm;

6.2.1.5.„Nepasliktinot" drošības pasākumus atjaunina informācijas sistēmu sākotnējā stāvoklī, un

6.2.1.6.Pārskata un apstiprina atbildīgās amatpersonas organizācijā;

6.2.2.Nodrošina personālu ar darbības nepārtrauktības plāna kopijām;

6.2.3.Koordinē darbības nepārtrauktības plāna aktvitātes atbilstoši incidentu apstrādes aktivitātēm;

6.2.4.Pārskata darbības nepārtrauktības plānu atbilstoši izmaiņām iestādē, informācijas sistēmā, vai darbības procesos vai atklājot problēmas, kas radušās darbības nepārtrauktības plāna īstenošanā, ieviešanā, izpildē, vai to testējot; un

6.2.5.Atjaunina darbības nepārtrauktības plāna izmaiņas;

Papildus vadlīnijas: Darbības nepārtrauktības plāns nepieciešams ārkārtas situācijās, kad sistēmas ir apdraudēta un nepieciešams atjaunot informācijas sistēmu un būtiskas darbības funkcijas.

6.3. Darbības nepārtrauktības apmācības

Kontrole: Iestāde periodiski rīko darbiniekiem darbības nepārtrauktības apmācības atbilstoši to lomām un atbildībām [Pielietojums: Iestādes definē biežumu].

6.4. Darbības nepārtrauktības plāna testēšana un pārbaude

Kontrole: Iestāde:

6.4.1.Testē un pārbauda darbības nepārtrauktības plānu [Pielietojums: Iestādes definē periodu], lai noteiktu [Pielietojums: Iestādes definētas pārbaudes un / vai mācības] cik plāns ir efektīvs un kādā mērā iestāde ir gatava to realizēt ārkārtas situācijās, un;

6.4.2. Novērtē, testē/pārbauda darbības nepārtrauktības plāna rezultātus un inicē koriģējošas aktivitātes.

Papildu vadlīnijas: Lai noteiktu iespējamo trūkumus darbības nepārtrauktības plānā var izmantot šādus scenārijus, piemēram, soli pa solim pārbauda sarakstu, modelē situācijas.

6.5. Informācijas sistēmu bojājumiecietība

Kontrole: Iestāde:

6.5.1.Nodrošina datu rezervēšanas kopiju veidošanu lietotāju līmeņa informācijai [Pielietojums: iestādes definē atjaunošanas periodu, kurā atjauno informāciju];

6.5.2.Nodrošina datu rezervēšanas kopiju veidošanu informācijas sistēmas līmeņa informācijai [Pielietojums: Iestādes definē periodu , kurā atjauno informāciju un atjaunošanas punktu];

6.5.3.Nodrošina rezerves kopiju veidošanu ar sistēmas drošību saistītai dokumentācijai [Pielietojums: Iestāde definē atjaunošanas periodu, kurā atjauno informāciju], un

6.5.4.Nodrošina datu rezerves kopijām konfidencionalitāti, pieejamību un veselumu.

Papildus vadlīnijas: Sistēmas līmeņa informācijā ietver, piemēram, sistēmas stāvokļa informāciju, operētājsistēmas un lietojumprogrammas, un licences. Lai

nodrošinātu datu rezerves kopiju integritāti var izmantot elektronisko parakstu un šifrēšanas hash funkcijas. Iestāde atbilstoši risku novērtējumam var izmantot arī datu rezerves kopiju šifrēšanu.

6.6. Informācijas sistēmas darbības atjaunošana

Kontrole: Iestāde nodrošina informācijas sistēmas atjaunošanu pēc bojājumiem, vai atteicēm.

Papildu vadlīnijas: Atjaunošana ir darbības nepārtrauktības pasākums, lai atjaunotu iestādei būtiskas darbības funkcijas.

7.Saime: Identifikācija un autentifikācija Klase: Tehnoloģijas

7.1. Identifikācijas un autentifikācija politika un procedūras

Kontrole: Iestāde izstrādā, izplata un pārskata/atjaunina [Pielietojums: Iestādes definē biežumu]:

a.Identifikācijas un autentifikācijas politiku, kurā nosaka mērķus, apjomu, lomas, atbildības, vadības atbildību, sadarbību ar citām iestādes struktūrvienībām, un atbilstību likumiem, un;

b.Procedūras, lai atvieglotu identifikācijas un autentifikācijas politikas ieviešanu.

7.2. Identifikācija un autentifikācija (iestādes lietotājiem)

Kontrole: informācijas sistēmās unikāli identificē un autentificē iestādes lietotājus (vai lietotāju ierosinātos vai procesus, kuri norit sistēmās):

7.3. Identifikātoru pārvaldība

Kontrole: Iestāde pārvalda lietotāju un iekārtu informācijas sistēmu identifikātorus:

7.3.1.Lietotāja vai iekārtu identitifikātoru piešķiršanai nozīmē pilnvarotas personas;

7.3.2.Indivīdu un iekārtu identifikātoriem jābūt unikāliem;
7.3.4.Lietotāju identifikātoru var piešķirt lietotāju grupai;

7.3.5.Identifikātorus izsniedz uz noteiktu laika periodu [Pielietojums: Iestādes nosaka periodu], un;

7.3.6.Pēc noteikta perioda identifikātoru bloķē [periodu nosaka iestāde]

7.3.7.Atjauno lietotāja identifikatoru [Pielietojums: Iestādes nosaka neaktivitātes periodu].

Papildu vadlīnijas: Visizplatītākie iekārtu identifikātori ir MAC vai IP adreses. Iekārtām var piešķirt arī unikālus identifikatorus. Lietotāju identifikātoru pārvaldību nepiemēro viesu un anonīmajiem kontiem. Parasti kā lietotāju identifikātoru izmanto lietotāja vārdus vai unikālus ciparu kodus.

7.4. Paroļu pārvaldība

Kontrole: Iestāde pārvalda informācijas sistēmu lietotāju un iekārtu paroles:

7.4.1.Pirms lietotājiem un iekārtām piešķir paroles tos identificē;

7.4.2.Paroles sarezģītību nosaka iestāde;

7.4.3.Nodrošina, ka paroles ir pietiekoši noturīgas pret atklāšanu;

7.4.4.Izstrādā administratīvas procedūras, kurā nosaka kā tiks izplatītas paroles, vai gadījumos, ja paroles tiek nozaudētas/kompromitētas vai anulētas;

7.4.4.Visas paroles, kas uzstādītas informācijas sistēmā pēc noklusējuma nomaina;

7.4.5.Ja nepieciešams parolēm nosaka minimālo un maksimālo izmantošanas un atklaizmantošanas laiku;

7.4.6.Paroles maina/atjauno [Pielietojums: Iestādes nosaka laika periodu konkrētam autentifikātoru veidam];

7.4.7.Paroļu saturu sargā no neautorizētas atklāšanas un modifikācijām un to aizsardzībai izmanto specifiskus aizsarglīdzekļu mērus;

7.4.8.Pieprasīt, lai lietotāji rūpējas par paroļu drošību;

Papildu vadlīnijas: Lietotāji kā alternatīvu parolēm var izmantot, piemēram, tokenus, biometrija kontroles, publisko atslēgu infrastruktūras (PKI) sertifikātus un kodu kalkulātorus. Vairums ražotāju informācijas sistēmas komponentes

piegādā ar jau sākotnēji iestatītu paroli. Pēc noklusējuma iestatītās paroles ir viegli atklājami un labi zināmi, tādēļ tie rada lielu risku informācijas drošībai. Tādēļ tās ir jānomaina uzreiz pēc uzstādīšanas reālā vidē. Lai nodrošinātu paroles slepenību, tās var glabāt informācijas sistēmā šifrētā veidā vai arī kā hash funkcijas.

Kontroles uzlabojumi:

1.Informācijas sistēmā kā autentificēšanās mehānismu izmanto paroli:

1.2.Paroles sarežģītība [Pielietojums: Iestādes definē prasības attiecībā uz lielo un mazo burtu jutīgumu, rakstzīmju skaitu, lielo burtu skaitu, mazo burtu skaitu, speciāliem simboliem, iekļauj minimālās prasības priekš katra tipa];

1.3.Nosaka minimālo paroles garumu [Pielietojums: Iestāde definē paroles garumu];

1.4.Paroles glabā un pārsūta šifrētā veidā;

1.5.Parolēm nosaka minimālo un maksimālo lietotošanas termiņu;

[Pielietojums: Iestādes definē minimālo un maksimālo lietošanas periodu],

Un;

1.6.Paroli neizmanto atkārtoti [Pielietojums: Iestādes definē izmantošanas skaitu].

7.5. Droša autentifikācija

Kontrole: informācijas sistēmā nodrošina, ka informācija, kas tiek izmantota autentifikācijas procesa laikā ir aizsargāta no neuztorizētas piekļūšanas.

7.6. Kriptogrāfijas algoritmi

Kontrole: Kriptogrāfijas algoritmus informācijas sistēmā izmanto atbilstoši normatīviem aktiem;

7.7.Identifikācija un autentifikācija (citu iestāžu lietotājiem)

Kontrole: Informācijas sistēmā identificē un autentificē citu iestāžu lietotājus (vai procesus, ko inicē citu iestāžu lietotāji).

8.Saime: Incidentu apstrāde Klase: Procesi

8.1. Incidentu apstrādes politika un procedūras

Kontrole: Iestāde izstrādā, izplata un pārskata/atjaunina [Pielietojums: Iestādes definē periodu]:

8.1.1.Incidentu apstrādes politiku, kurā nosaka mērķus, apjomu, lomas, atbildības, vadības atbildību, sadarbību ar citām struktūrvienībām, un atbilstību likumiem, un;

8.1.2.Procedūras, lai atvieglotu incidentu apstrādes politikas īstenošanu

8.2. Incidentu apstrādes apmācības

Kontrole: Iestāde:

8.2.1.Apmāca personālu atbilstoši to pienākumiem apstrādāt incidentus informācijas sistēmā, un;

8.2.2.Nodrošina incidentu apstrādes personāla kvalifikācijas celšanu [Pielietojums: Iestādes definē biežumu].

Papildu vadlīnijas: incidentu apstrādes mācībās lietotājus apmāca, lai tie prastu identificēt un ziņot par aizdomīgām darbībām, ko rada gan ārēji gan iekšējie apdraudējuma aģenti.

8.3. Incidentu apstrādes aktivitātes

Kontrole: Iestāde:

8.3.1.Incidentu apstrādes aktivitātes ietver identifikāciju un analīzi, novēršanu un atjaunošanu;

8.3.2.Incidentu apstrādes aktivitātes koordinētas kopā ar nepārtrauktības plānošanas aktivitātēm; un

8.3.3.Pieredzi, kas iegūst no iepriekšējiem incidentu apstrādes aktivitātēm, dokumentē un to izmanto treniņa un testēšanas uzdevumos kā arī mācībās.

8.4. Incidentu pārraudzība

Kontrole: Iestāde izmeklē un dokumentē katru informācija sistēmu drošības incidentu.

Papildu vadlīnijas: Informācijas sistēmu drošības incidentu dokumentācijā uztur uzskaiti par katru incidentu, statusu, un citu noderīgu informāciju, kas nepieciešama, lai varētu izmeklēt incidentu iemeslus.

8.5. Ziņošana par incidentiem

Kontrole: Iestāde:

8.5.1.Lai spētu laicīgi reaģēt uz incidentiem, personālam nosaka par aizdomīgiem drošības incidentiem ziņot atbildīgam personālam [Pielietojums: iestādes nosaka laika periodu], un

8.5.2.Atbildīgām iestādēm informāciju par incidentiem, kas saistīta ar drošību, ziņo saskaņā ar instrukciju.

8.6. Atbalsts incidentu apstrādei

Kontrole: Iestāde nodrošina atbilstošus resursus incidentu apstrādei. Informācijas sistēmas lietotājiem nodrošina konsultācijas un palīdzību kā rīkoties gadījumos, kad rodas ar drošību saistītios incidenti un kā ziņot par tiem.

Papildu vadlīnijas: Iestādes var izveidot palīdzības dienestu vai palīdzības grupu, kas reģistrētu un apstrādātu incidentus.

8.7. Incidentu novēršanas plāns

Kontrole: Iestāde:

8.7.1.Izstrādā incidentu novēršanas plānu, lai:

8.7.1.1.Spētu adekvāti reaģēt uz incidentiem;

8.7.1.2.Apraksta iestādes un to struktūru sadarbspēju;

8.7.1.3.Apraksta augstā līmenī, kāda ir incidentu novēršanas loma iestādē;

8.7.1.4.Nosaka kā tiks publicēti pārskati par incidentiem;

8.7.1.5.Nosaka metrikas un rādītājus, lai novērtētu kā iestāde spēj reaģēt uz incidentiem;

8.7.1.6.Nosaka nepieciešamos resursus un vadības atbalstu, lai efektīvi nodrošinātu incidentu novēršanu atbilstoši iestādes brieduma spējām;

8.7.1.7.Nosaka par incidentu novēršanu atbildīgās amatpersonas;

8.7.2.Nodrošina pieejamību incidentu pārvaldības plānam [Pielietojums: Iestāde definē darbinieku sarakstu, kuri apstrādā incidentus (identificē pēc vārda / vai amata)];

8.7.3.Pārskata incidentu pārvaldības plānu [Pielietojums: Iestādes definē biežumu];

8.7.4.Koriģē incidentu pārvaldības plānu, informācijas sistēmas / organizatoriskas izmaiņu vai problēmu laikā kā arī īstenojot, izpildot, vai testējot plānu un;

8.7.5.Sniedz informāciju par izmaiņām incidentu pārvaldības plānā (Iestāde nosaka incidentu apstrādes personālu (identificē tos pēc vārda/ vai amata)un struktūrvienības).

Papildu vadlīnijas: Ir svarīgi, ka iestādē ir noteikta formāla, mērķtiecīga, un saskaņota pieeja reaģējot vai apstrādājot incidentus. Iestādes mērķi, stratēģija palīdz noteikt nepieciešamos resursus apstrādāt incidentus.

9.Saime: Uzturēšana Klase: Process

9.1. Sistēmas uzturēšanas politika un procedūras

Kontrole: Iestāde izstrādā, izplata, pārskata/atjauno [Iestādes nosaka biežumu]:

9.1.Informācijas sistēmas uzturēšanas politiku, kurā nosaka mērķus, apjomus, lomas, atbildības, vadības atbildību, sadarbību starp citām iestādes struktūrvienībām, un atbilstību likumiem, un;

9.2.Procedūras, lai atvieglotu informācijas sistēmas uzturēšanu politikas Īstenošanu.

9.2.Uzturēšanas uzraudzība

Kontrole: iestāde:

9.2.1.Plāno, veic izmaiņas, dokumentē, pārskata ierakstus par sistēmas uzturēšanu un novērš kļūmes, labo atklātos defektus informācijas sistēmā vai to komponentēs atbilstoši ražotāja vai pārdevēja noteiktai specifikācijai/vai iestādes noteiktām prasībām;

9.2.3.Oficiālas iestādes amatpersonas pilnvaro pasākumus, kas saistīti ar informācijas sistēmas vai to komponenšu apkopi vai remontu;

9.2.5.Pēc tehniskās apkopes vai remonta pasākumiem pārbauda visas potenciāli ietekmējamās drošības kontroles, lai pārliecinātos, ka kontroles joprojām darbojas pareizi;

9.2.6. Datu nesēju bojājuma gadījumā jāpārliecinās, ka dati no datu nesēji nav atjaunojami un tā remonta gadījumā dati nenokļūs trešo personu rīcībā.

9.2.7.Kontrolē visas uzturēšanas aktivitātes, neatkarīgi no tā vai to veic uz vietas vai attālināti;

9.2.8.Pirms nodod informācijas sistēmu vai tās komponentes tehniskai apkopei vai remontam, atbildīgās amatpersonas pārbauda vai tā nesatur konfidenciālu un sensitīvu informāciju. Ja tā satur, tad nodrošina visu iespējamo, lai nodrošinātu informācijas veselumu un konfidencionalitāti;

9.3. Uzturēšana izmantojot datu pārraides tīklu

Kontrole: Iestāde:

9.3.1.Pilnvaro, uzrauga un kontrolē ar uzturēšanu un diagnostiku saistītās aktivitātes izmantojot datu pārraides tīklus;

9.3.2.Uzturēšanas un diagnostikas rīku izmantošanu datu pārraides tīklā atļauj, ja to izmantošana ir noteikta iestādes informācijas sistēmas drošības plānā;

9.3.3.Uzturēšanas un diagnostikas pasākumi tiek identificēti un autorizēti;

9.3.4.Par visām uzturēšanas un diagnostikas aktivitātēm veic atbilstošus ierakstus;

9.3.5.Pēc uzturēšanas un diagnostikas pasākumu beigām, visas aktīvās datu pārraides sesijas pārtrauc;

9.4. Atbalsta personāls

Kontrole: Iestāde:

9.4.1.Uztur sarakstu ar iestādēm un personām, kas nodrošina uzturēšanas pakalpojumus;

9.4.2.Nosaka, ka personām, kuras atbalsta vai uztur informācijas sistēmu ir atbilstoša kompetence un pilnvaroti to darīt;

9.4.3. Nosaka informācijas neizspaušanas nosacījumus, ja atbalsta personālam ir nepieciešamība piekļūt konfidenciālai informācijai.

10.Saime: Informācijas nesēju aizsardzība Klase: Procesi

10.1. Informācijas nesēju aizsardzības politika un prcedūras

Kontrole: Iestāde izstrādā, izplata un pārskata / atjaunina [Pielietojums: Iestādes definē biežumu]:

10.1.1.Informācijas nesēju aizsardzības politiku, kurā nosaka mērķus, darbības jomas, uzdevumus, pienākumus, vadības atbildību, sadarbību starp sturktūrvienībām, un atbilstību normatīviem aktiem, un;

10.1.2.Procedūras, lai atvieglotu informācijas nesēju aizsardzības politikas īstenošanu.

10.2. Piekļuve pie informācijas nesējiem

Kontrole: Iestāde nodrošina ierobežotu piekļuvi nesējiem [Pielietojums: Iestādes nosaka kāda veida digitāliem un nedigitāliem nesējiem] [Pielietojums: Iestādes noteiktām personām], pielietojot atbilstošu pasākumus [Pielietojums: Iestādes definē drošības pasākumus].

Papildus vadlīnijas: Informācijas nesēji ir gan digitālie mediji (piemēram, disketes, magnētiskās lentes, ārējie/noņemamie diskdziņi, zibatmiņas /USB diski, kompaktdiski, digitālie video diski), un ne-digitālie mediji (piemēram, papīrs, mikrofilmas). Šī kontrole attiecas arī uz mobiliem skaitļošanas un sakaru iekārtām ar informācijas uzglabāšanas iespēju (piemēram, piezīmjdatori/ portatīvie datori, personālie digitālie asistenti, mobilie telefoni, digitālās kameras un audio ierakstu iekārtas). Iestādes novērtē katra informācijas nesēja izmantošanas risku un iespējamo kaitējumu, kā arī nosaka atbilstošus ierobežošanas pasākumus. Iestādes dokumentē, politikas un procedūras un kādi īpaši pasākumi, tiek veikti, lai nodrošinātu ierobežotu piekļuvi.

10.3.Informācijas iznīcināšana

Kontrole: Iestāde:

10.3.1.Informācijas sistēmu, uz digitāliem un nedigitāliem nesējiem, saturošu informāciju iznīcina vai padara par atkārtoti neizmantojamu, ja tā vairs nav nepieciešama;

10.3.2.Iznīcināšanas mehānismus izmanto atbilstoši informācijas klasifikācijai vai sensivitātei;

10.Saime: Fiziskā un vides aizsardzība Klase: Procesi

10.4. Fiziskā un vides aizsardzības politika un procedūras

Kontrole: Iestāde izstrādā, izplata un pārskata/atjaunina [Pielietojums: Iestādes definē periodu]:

10.4.1.Fiziskās vides aizsardzības politiku, kurā nosaka mērķus, apjomu, lomas, atbildību, vadības atbildību, sadarbību starp struktūrvienībām, un atbilstība likumiem, un

10.4.2.Procedūras, lai atvieglotu fiziskās vides aizsardzības politikas ieviešanu.

10.5.Fiziskās piekļuves aizsardzība

Kontrole: Iestāde:

10.5.1.Sagatavo un uztur to personāla sarakstu kam piešķirta pielaide objektam, kurā izmitināta informācijas sistēma (izņemot tos objektus, kuri ir publiski pieejami);

10.5.2.Nosaka autorizācijas līdzekļus;

10.5.3.Anulē pielaidi personām, kam piekļuve vairs nav nepieciešama.

Papildu vadlīnijas: Autorizācijas līdzekļi, piemēram, identifikācijas kartes, kodu kartes un viedkartes.

10.6. Fiziskā piekļuves kontrole

Kontrole: Iestāde:

10.6.1.Īsteno fizisko piekļuves kontroli objektiem, kurā izmitināta informācijas sistēma (tostarp ieejas /izejas punktiem);

10.6.2.Pārbauda personas pirms tām nodrošina fizisko piekļuvi pie informācijas sistēmas;

10.6.3.Kontrolē ar fiziskās piekļuves vai aizsardzības rīkiem piekļūšanu telpām, kurā izvietota informācijas sistēma;

10.6.4.Publiski pieejamās vietas kontrolē atbilstoši iestādes riska novērtējumam;

10.6.5.Nosaka drošas atslēgas, kodu kombinācijas;

10.6.6.Regulāri veic fiziskās piekļuves iekārtu pārbaudi [Pielietojums: Iestāde definē biežumu], un;

10.6.7.Piekļuves atslēgas anulē, ja tās ir nozaudētas vai to kodu kombinācijas ir apdraudētas vai ar personām ir pārtrauktas darba attiecības.

10.7. Fiziskās piekļuves uzraudzība

Kontrole: Iestāde:

10.7.1.Uzrauga fizisko piekļuvi informācijas sistēmai, lai spētu adekvāti reaģēt uz gadījumiem, kas saistīti ar fizisko drošību;

10.7.2.Pārskata fiziskās piekļuves žurnālus [Pielietojums: Iestāde definē biežumu], un;

10.7.3.Pārskatu rezultātus un atklātās nepilnības koriģē atbilstoši incedentu apstrādes kārtībai.

10.8. Apmeklētāju kontrole

Kontrole: Katru apmeklētāju iestāde reģistrē un papildus noskaidro apmeklētāja vizītes mērķi pirms tiem atļauj atrasties telpās, kurās izmitināta informācijas sistēma. Kontrole neattiecas uz tām vietām, kurā informācijas sistēma ir publiski pieejama.

10.9. Apmeklētāju reģistrēšana

Kontrole: Iestāde:

10.9.1.Ievieš apmeklētāju reģistra žurnālu, kurā fiksē katru objekta apmeklējuma mērķi (izņemot tiem objektiem, kas atzīti par publiski pieejamiem) un

10.9.2.Pārbauda apmeklētāju reģistra žurnālu [Pielietojums: Iestāde definē biežumu].

Papildu vadlīnijas: Apmeklētāju piekļuves žurnālā iekļauj, piemēram, vārdu un uzvārdu, pārstāvētas iestādes nosaukumu, datumu, laiku un apmeklējuma mērķi.

10.10. Rezerves elektroenerģijas padeve

Kontrole: Iestāde nodrošina un uztur automātisku rezerves elektroenerģijas padeves sistēmu, kas aktivizējas, tiklīdz tiek pārtraukta elektroenerģijas padeve vai rodas traucējumi elektrolīnijās.

10.11. Ugunsdrošība

Kontrole: Iestāde nodrošina un uztur uguns novēršanas un detektēšanas iekārtas/sistēmas, ko darbina no neatkarīgiem enerģijas avotiem.

Papildu vadlīnijas: Ugunsdzēšanas un detektēšanas iekārtas/sistēmas ir, piemēram, izsmidzināšanas sistēmas, rokas ugunsdzēšanas aparāti, stacionāras ugunsdzēsības šļūtenes, un dūmu detektori. Datu centros un serveru telpās kā arī telpās, kurās atrodas skaitļošanas mašīnas izmanto tikai un vienīgi gāzveida vai pulverveida ugunsdzesēšanas šķidrumus.

10.12. Temperatūras un mitruma kontrole

Kontrole: Iestāde:

10.12.1.Nodrošina atbilstošu temperatūras un mitruma līmeni objektā, kurā izmitināta informācijas sistēmas infrastruktūra [Pielietojums: Iestādes definē pieņemamo līmeni], un;

10.12.2.Uzrauga temperatūras un mitruma līmeni [Pielietojums: Iestādes definē periodiskumu].

10.13.Ūdens noplūdes novēršana

Kontrole: Iestāde pasargā informācijas sistēmu no bojājumiem, ko var izraisīt ūdens noplūde, izmantojot pretūdensnoplūdes noslēgšanas vārstus. Atbilstoši nodrošina, ka pie tiem var piekļūt tikai pilnvarots personāls.

10.14. Piekļūšana pie perimetra iekārtām

Kontrole: Iestāde autorizē, uzrauga un kontrolē [Pielietojums: Iestādes, noteikta veida informācijas sistēmas komponenus] piekļuvi pie informācijas sistēmu perimetra iekārtām un uztur par tiem ierakstus.

Papildus vadlīnijas. Perimetra iekārtas ietver: ugunsmūri, maršrutizātori, datu pieķluves punkti utt.

Saime: Plānošana **Klase: Pārvaldība**

11.Drošības plānošanas politika un procedūras

Kontrole: Iestāde izstrādā, izplata un vienreiz gadā pārskata/atjaunina:

11.1.1.Drošības plānošanas politiku, kurā nosaka mērķus, apjomu, lomas, atbildības, vadības atbildību, sadarbību starp struktūrvienībām, un atbilstību likumiem, un

11.1.2.Procedūras, lai atvieglotu drošības plānošanas politikas īstenošanu.

11.2. Informācijas sistēmu drošības plāns

Kontrole: Iestāde:

11.2.1.Informācijas sistēmai izstrādā drošības plānu, kurā:

11.2.1.1.Nosaka iestādes struktūru un arhitektūru;

11.2.1.2.Skaidri un nepārprotami definē sistēmas darbības lauku;

11.2.1.3.Apraksta informācijas sistēmu uzdevumus un funkcijas;

11.2.1.4.Klasificē drošības prasības informācijas sistēmai;

11.2.1.5.Apraksta informācijas sistēmas vidi;

11.2.1.6.Apraksta sadarbību ar citām informācijas sistēmām;

11.2.1.7.Veic drošības pārbaudes informācijas sistēmai;

11.2.1.8. Atbilstoši noteiktām prasībām apraksta esošās un plānotās drošības kontroles;

11.2.1.9.Pārskata un apstiprina atļaujas tām personām, kuras ir atbildīgas par plāna izpildi;

11.2.2.Drošības plānu pārskatu [Pielietojums: Iestāde definē periodu], un;

11.2.2.Veic izmaiņas informācijas sistēmā pēc drošību kontroļu novērtējuma, kā arī problēmām, kas identificētas realizējot drošības plānuun atjaunina plānu.

11.3.Lietotāju uzvedības noteikumi

Kontrole: Iestāde:

11.3.1.Noteikumos apraksta lietotāja atbildību un no tiem sagaida atbilstošu uzvedību lietojot informācijas sistēmu;

11.3.2.Lietotājiem, pirms tiem tiek piešķirta piekļuve pie informācijas sistēmas, liek parakstīt apliecinājumu, ka lietotājs ir izlasījis uzvedības noteikumus un ar tiem iepazinies;

Papildus vadlīnijas. Informācijai, kas paredzēta informācijas sistēmas lietotājiem tiek veidota ērta un viegli lasāma, kā arī tai jānodrošina ērta pieejamība.

11.4.Privātuma ietekmes novērtēšana

Kontrole: Iestāde veic privātuma ietekmes novērtējumu informācijas sistēmā saskaņā ar personu datu aizsardzības likumu.

12.Saime: Personāla drošība Klase: Procesi

12.1.Personāla drošības politika un procedūras

Kontrole: Iestāde izstrādā, izplata un pārskata/atjaunina [Pielietojums: Iestādes definē periodu]:

12.1.1.Personāla drošības politiku, kurā nosaka mērķus, apjomu, lomas, atbildības, vadības atbildību, sadarbību starp struktūrvienībām, un atbilstība likumiem, un;

12.1.2.Procedūras, lai atvieglotu personāla drošības politikas īstenošanu.

12.2. Amatu novērtēšana

Kontrole: Iestāde:

12.2.1.Nosaka iespējamos drošības riskus visiem amatiem;

12.2.2.Nosaka vērtēšanas kritērijus personām, kas pretendē uz vakantām vietām; un;

12.2.3.Pārskata un novērtē riskus, kas saistīti ar amatiem [Pielietojums: Iestāde definē periodu].

12.3.Personāla uzraudzība

Kontrole: Iestāde:

12.3.1.Pirms piešķir personām piekļuvi pie informācijas sistēmas tās autorizē; un

12.3.2.Personas pārpārbauda saskaņā ar [Pielietojums: Iestādes definē sarakstus ar nosacījumiem, kā jāpārbauda, kur pārpārbauda, un pārpārbaudes biežumu].

12.4. Personāla atlaišana

Kontrole: Iestāde, izbeidzoties darba attiecībām:

12.4.1.Personai anulē piekļuvi informācijas sistēmai;

12.4.2.Personai piešķir apgaitas lapu;

12.4.3.Nodrošina iestādes personālam piekļuvi informācijai un informācijas sistēmām, ko iepriekš kontrolēja atlaistā persona.

12.5.Personāla rotācija

Kontrole: Gadījumos, ka darbinieki tiek norīkoti vai pārcelti citos amatos, iestāde pārskata loģisko un fizisko piekļuvi informācijas sistēmām/ iekārtām [Pielietojums: Iestāde nosaka rotācijas aktivitātes, [Pielietojums: Iestādes definētā laika posmā pēc darbinieka rotācijas].

12.5.Piekļuves līgums (saistību raksts)

Kontrole: Iestāde:

12.5.1.Ar visiem darbiniekiem, kam nepieciešama piekļuve informācijas sistēmai un tai uzglabātai informācijai slēdz piekļuves līgumus;

12.5.2.Pārskata/atjauno piekļuves līgumus [Pielietojums: Iestādes definē periodu].

12.6. Drošības prasību ievērošana ārpakalpojuma personālam

Kontrole: Iestāde:

12.6.1.Nosaka un izstrādā drošības prasības un atbildību ārpakalpojuma sniedzēju personālam;

12.6.2.Uzrauga ārpakalpojuma sniedzēja personāla atbilstību iestādes drošības prasībām.

12.7.Sankcijas

Kontrole: Iestāde pielieto sankcijas pret personām, kas neievēro informācijas drošības politiku un procedūras.

13.Saime: Risku novērtēšana Klase: Pārvaldība

13.1.Riska novērtēšanas politikas un procedūras

Kontrole: Iestāde izstrādā, izplata un pārskata/ atjaunina [Pielietojums: Iestādes definētas biežumus]:

13.1.1.Risku novērtēšanas politiku, kurā nosaka mērķus, apjomu, lomas, atbildības, vadības atbildību, sadarbību starp struktūrvienībām, un atbilstība likumiem, un;

13.1.2.Procedūras, lai atvieglotu riska novērtējumu politikas īstenošanu.

13.2.Informācijas klasifikācija

Kontrole: Iestāde:

13.2.1.Informāciju un informācijas sistēmas klasificē atbilstoši normatīviem aktiem, direktīvām, politikām, regulām, standartiem, vadlīnijām;

13.2.2.Informācijas klasificēšanas rezultāti tiek dokumentēti (kā arī pamatojums) drošības plānā;

13.3.3.Informācijas klasifikāciju veic iestādes oficiāli nozīmētas personas.

13.3.Risku novērtēšana

Kontrole: Iestāde:

13.3.1.Veic riska novērtējumu, tostarp varbūtību, ka risks var iestāties un to kaitējumu apjomu, kas var rasties informācijas nesankcionētas piekļuves, izmantošanas, izpaušanas, uzglabāšanas un pārraidīšanass, informācijas sistēmu un informācijas procesu modificēšanas vai iznīcināšanas gadījumā;

13.3.2. Risku novērtējuma rezultātus dokumentē [izvēle: drošības plānā; riska novērtējuma ziņojumā; [Pielietojums: Iestādes definē dokumentus]];

13.3.3.Pārskata riska novērtējuma rezultātus [Pielietojums: Iestādes definē biežumu], un;

13.3.4.Regulāri veic risku novērtējumu [Pielietojums: Iestādes nosaka periodu, bet vismaz vienu rezi gadā] kā arī tad, kad ir veiktas būtiskas izmaiņas informācijas sistēmā vai tajā darbības vidē, vai parādījušies jauni draudi vai atklātas ievainojamības, vai citi apstākļi, kas var ietekmēt drošību stāvokli sistēmā.

13.4.Ievainojamību atklāšana

Kontrole: Iestāde:

13.4.1.Ievainojamības meklē informācijas sistēmā un atbalsta aplikācijās, infrastruktūras konfigurācijās [Pielietojums: Iestādes definē biežumu un/vai pēc nejaušības principa saskaņā ar iestādes noteiktiem procesiem] un gadījumos, kad jauna veida ievainojamība potenciāli ietekmē sistēmas / programmu;

13.4.2.Izmanto tādus ievainojamību skenēšanas rīkus un paņēmienus, kas automātiski atklāj ievainojamības:

13.4.2.1.Uzskaita OS platformas un programmatūras trūkumus, un neatbilstošu konfigurāciju;

13.4.2.2.Kontroļu pārbaužu saraksti un testu procedūras ir caurredzami un standartizēti un;

13.4.2.3.Novērtē atklāto ievainojamību ietekmi;

13.4.3.Analizē ievainojamību skenēšanas atskaites ;

13.4.4.Novērš noteiktā laika periodā atklātās ievainojamības [Pielietojums: Iestāde definē reakcijas laikus] atbilstoši iestādes riska novērtējumam, un;

13.4.5. Lai palīdzētu novērst līdzīgas problēmas citās informācijas sistēmās nodrošina piekļuvi iestādes pilnvarotam darbiniekam informācijai, kas iegūta no ievainojamību skenēšanas procesa un drošības kontroles novērtējuma;

14.Saime: Informācijas sistēmu un pakalpojumu iepirkumi Klase: Pārvaldība

14.1. Sistēmu un pakalpojumu iepirkumu politika un procedūras

Kontrole: Iestāde izstrādā, izplata un pārskata/atjaunina [Pielietojums: Iestādes definē biežumu]:

14.1.1.Informācijas sistēmu un pakalpojumu iepirkumu politiku, kurā nosaka mērķus, darbības jomas, uzdevumus, pienākumiem, vadības atbildību, sadarbību starp struktūrvienībām, un atbilstību normatīvajiem aktiem, un;

14.1.2.Procedūras, lai atvieglotu informācijas sistēmu un iepirkumu politikas ieviešanu .

14.2. Resursu plānošana

Kontrole: Iestāde:

14.2.1.Plānotām informācijas sistēmām un biznesa procesiem nosaka informācijas drošības prasības;

14.2.2.Plāno nepieciešamos resursus, kas nepieciešami informācijas sistēmu aizsardzībai;

14.2.3.Iestādes informācijas drošību plāno atbilstoši budžetā iedalītiem finanšu līdzekļiem. Grāmatvedībā atvēlot speciālu šim nolūkam kontējumu.

14.3. Atbalsts visā ekspluatācijas stadijā

Kontrole: Iestāde:

14.3.1.Attīstot informācijas sistēmu ievēro informācijas drošības prasības;

14.3.2.Definē informācijas sistēmu drošības pasākumus visā sistēmas ekspluatācijas laikā;

14.3.2.Nozīmē par informācijas drošību atbildīgos darbiniekus.

14.4.Iepirkumu specifikācijas

Kontrole: Iepirkumu specifikācijas prasībās ietver vai ieliek atsauces no informācijas sistēmu tehniskajām specifikācijām un risku novērtējuma prasībām:

14.4.1. Funkcionālās drošības prasības/specifikācijas;

14.4.2.Ar drošību saistītās dokumentācijas prasības;

14.5. Informācijas sistēmu dokumentācija

Kontrole: Iestāde:

14.5.1.Uztur un nodrošina informācijas sistēmas dokumentācijas veselumu kā arī nodrošina, ka pie tās var piekļūt pilnvaroti lietotāji. Dokumentācijā, kas paredzēta administrātoriem apraksta:

14.5.2.Drošu konfigurēšanu, uzstādīšanu, un darbu ar informācijas sistēmu;

14.5.3.Kā lietot, izmantot un uzturēt drošības elementu / funkcijas; un

14.5.4.Konfigurācijas trūkumi (vājās vietas) un administratīvo (priviliģēto) funkciju izmantošana;

14.5.4.informācijas sistēmas atjaunošanas pasākumus;

14.5.5.Dokumentācijā, kas paredzēta lietotājiem:

14.5.6.Lietotājiem pieejamās drošības iespējas/funkcijas un kā tos droši un efektīvi izmantot;

14.5.7.Apraksta, kā droši darboties ar informācijas sistēmu;

14.5.8.Lietotāja atbildību lietotojot informāciju un informācijas sistēmu;

14.5.9.Apraksta kā iegūt informāciju par sistēmu, ja dokumentācija par informācijas sistēmu nav pieejama vai vispār nav.

14.6. Programmatūras lietošanas ierobežojumi

Kontrole: Iestāde:

14.6.1.Programmatūru izmanto atbilstoši noslēgtiem līgumiem un autortiesību tiesību dokumentiem;

14.6.2.Programmatūras licenču kontrolei un ar to saistīto dokumentāciju uzskaitei izmanto programmatūru vai žurnālus;

14.6.3.Kontrolē dc++, torrent utt. izmantošanu, lai novērstu nelegāla autordarbu izplatīšanu.

14.7. Lietotāja instalētās programmatūras

Kontrole: Iestāde nosaka kārtību, kas reglamentē programmatūras uzstādīšanu lietotājiem.

14.8. Informācijas sistēmu pakalpojumu saņēmēji

Kontrole: Iestāde:

14.8.1.Pieprasa, lai informācijas sistēmas pakalpojuma sniedzēji nodrošina pakalpojumus atbilstoši iestādes informācijas drošības politikai(prasībām), apkalpošanas līmeņa līgumiem un LR normatīviem aktiem;

14.8.2.Definē un dokumentē informācijas sistēmu pakalpojumu saņēmēju lomas un atbildības

14.8.3.Monitorē pakalpojumu saņēmēju drošības kontroļu atbilstību iestādes politikai un LR normatīviem aktiem.

15.Saime: Sistēmu un komunikāciju aizsardzība Klase: Tehnoloģijas

15.1. Sistēmu un komunikāciju aizsardzības politika un procedūras

Kontrole: Iestāde izstrādā, izplata un pārskata/atjaunina [Pielietojums: Iestādes definē biežumu]:

15.1.1.Sistēmu un komunikāciju aizsardzības politiku, kurā nosaka mērķus, apjomu, lomas, atbildības, vadības atbildību, sadarbību starp struktūrvienībām, un atbilstība likumiem, un;

15.1.2.Procedūras, lai atvieglotu sistēmas un komunikāciju aizsardzības politikas ieviešanu.

15.2. Aizsardzība no pakalpojuma atteicēm

Kontrole: Informācijas sistēmas aizsargā pret DDOS (izkliedētais pakalpojumu atteices uzbrukums): [Pielietojums: Iestādes nosaka sarakstu ar pakalpojumatteicēm vai izmanto atsauces uz avotiem].

15.3.Perimetra aizsardzība

Kontrole: informācijas sistēma:

15.3.1.Monitorē un kontrolē pieslēgumus perimetrā atrodošām un ārpus perimetra atrodošām sistēmām , un;

15.3.2.Pie ārējiem tīkliem vai sistēmām kā arī perimetra iekārtām slēdzas izmantojot meneģējamas pieslēgumu saskarnes atbilstoši iestādes drošības arhitektūrai.

15.4.Kriptogrāfisko atslēgu izveide un pārvaldība

Kontrole: Iestāde veido un pārvalda kriptogrāfiskās informācijas sistēmu atslēgas.

15.5.Kriptometožu pielietošanu

Kontrole: ja nepieciešams informācijas sistēmā ievieš kriptogrāfisko aizsardzību un kriptometodes atbilstoši LR likumdošanai.

15.6. Publisku informācijas sistēmu aizsardzība

Kontrole: Sabiedrībai pieejama informācijas sistēmas saturošai informācijai un lietojumprogrammām nodrošina veselumu un pieejamību.

15.7. Papildaprīkojums

Kontrole: informācijas sistēma:

15.7.1.Aizliedz tālvadības aktivizēšanu iekārtām: [Pielietojums: Iestādes definē izņēmumus, kad tālvadības aktivizācija ir atļauta], un;

15.7.2.Skaidri nosaka kādas iekārtas lietotājs var izmantot.

Papildus vadlīnijas: Papildiekārtas var būt, piemēram, kameras un mikrofoni.

16.Saime: Sistēmas un informācijas veselums **Klase: Procesi**

16.1. Sistēmas un informācijas veseluma politika un procedūras

Kontrole: Iestāde izstrādā, izplata un pārskata/atjaunina [Pielietojums: Iestāde definē periodu]:

16.1.1.Sistēmas un informācijas veseluma politiku, kurā norāda mērķus, apjomu, lomas, atbildības, vadības atbildību, sadarbību starp struktūrvienībām, un atbilstību likumiem, un;

16.1.2.Procedūras, lai atvieglotu sistēmas un informācijas veseluma politikas ieviešanu.

16.2.Ievainojamību sanācija (flaw remediation)

Kontrole: Iestāde:

16.2.1.Identificē, ziņo, un novērš informāciju sistēmas ievainojamības;

16.2.2.Pirms uzstāda programmatūras atjauninājumus tos testē uz iespējamām

blakusiedarbībām un novērtē ietekmi uz iestādes informācijas sistēmām;

16.2.3.Iestrādā ievainojamību novēršanas procedūras konfigurācijas pārvaldības procesos.

16.3.Aizsardzība pret ļaunprātīgu kodu

Kontrole: Iestāde:

16.3.1.Lai atklātu un likvidētu ļaunprātīgu koda izplatīšanās iespējas, datu pārraides tīkla ieejas un izejas punktos, informācijas sistēmās un darba stacijās

kā arī serveros un tīklā esošajās mobilajās iekārtās uzstāda atbilstošu programmatūru (antivīrusus utt.);

16.3.1.1.Programmatūru izmanto elektronisko pasta vēstuļu, programmatūras pielikumu, mājas lapu, ārējo datu nesēju pārbaudei uz datorvīrusu esamību vai

16.3.1.2.Lai novērstu iespēju izmantot informācijas sistēmas ievainojamības;

16.3.2.Regulāri atjaunina ļaunprātīgu kodu identificēšanas signatūras;

16.3.3.Konfigurē ļaunprātīgu kodu aizsardzības mehānismus, lai:

16.3.3.1.Periodiski un reālā laikā nodrošinātu informācijas sistēmas [Pielietojums: Iestādes definē biežumu] skenēšanu lejupielādējot, atverot vai izpildot failus;

16.3.3.1. [Izvēle (viens vai vairāki): Atklājot ļaunprātīgu kodu to bloķē, nosūta karantīnā, nosūta brīdinājumu administratoram; [Pielietojums: Iestāde definē darbības]];

Papildus vadlīnijas: Informācijas sistēmas ieejas un izejas punkti ir, piemēram, ugunsmūri, elektroniskā pasta serveri, web serveri, proxy serveri, un attālinātās piekļuves serveri. Ļaunprātīgi kodi ir, piemēram, datorvīrusi, Trojas zirgi, un spiegprogrammatūra. Pastāv vairākas tehnoloģijas un metodes, lai ierobežotu vai likvidētu sekas, ko rada ļaunprātīgais kods. Ieviešot konfigurācijas pārvaldības un programmatūras veseluma kontroli var efektīvi novērst neatļauta koda izpildi. Ļaunprātīgs kods var būt arī injicēts programmatūrā, piemēram, loģiskās bumbas, backdoor [„sētas durvis”]. Tradicionālie aizsardzības mehānismi nav būvēti, lai atklātu šādus kodu. Šādos gadījumos iestādēm ir jāpaļaujas uz riska mazināšanas pasākumiem un tajos jāiekļauj, piemēram, drošas kodēšanas praksi, uzticamu iepirkuma procesu, konfigurācijas pārvaldības un kontroles un pārraudzības praksi, lai palīdzētu nodrošināt, ka programmatūra ir izstrādāta kā tas tika iecerēts.

16.4. Drošības brīdinājumi, padomi un norādījumi

Kontrole: Iestāde:

16.4.1. Regulāri seko aktualitātēm informācijas drošības jomā.

16.4.2.Izstrādā iekšējos drošības brīdinājumus, padomus un norādījumus;

16.4.3.Nosaka laika posmu, kurā personālam jāziņo par atklātām neatbilstībām informācijas drošībā.

16.5.Datu uzglabāšana

Kontrole: Iestāde arhivē informācijas sistēmas datus atbilstoši LR normatīviem aktiem, rīkojumiem, norādījumiem, politiku, noteikumiem, standartiem un ekspluatācijas prasībām.

Papildu vadlīnijas: datus apstrādā un arhivēšanas prasības attiecas uz visu informācijas dzīves ciklu.