Pielikums

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas

SATURS

Lietotie termini un saīsinājumi

Apdraudējums - iemesli, kas var neļaut uzturēt informācijas sistēmas (IS) drošību atbilstoši noteiktajām informācijas resursu konfidencialitātes, pieejamības un integritātes prasībām. IS drošības apdraudējums ir ar nodomu (tīši) vai aiz neuzmanības veikta darbība vai notikums, kas var izraisīt sistēmas bojājumu, iznīcināšanu vai nonākšanu tādu personu rīcībā, kuras nav tam pilnvarotas, vai kuru dēļ piekļūšana sistēmas informācijas resursiem var būt traucēta vai neiespējama. Apdraudējumu iespējamību nosaka sistēmas ievainojamības.

Atlikušais risks – risks, kas saglabājas pēc tam, kad ir ieviesti drošības līdzekļi.

Autentiskums – īpašība, kas nodrošina, ka priekšmeta vai resursa identitāte ir tāda, kā tiek apgalvots.

Drošības līdzekļi vai pasākumi – prakse, procedūras vai mehānismi, kas var pasargāt no informācijas sistēmas apdraudējumiem, mazinot IS trūkumus vai ierobežojot drošības incidenta ietekmi.

Draudi - *(angliski „*threats")* jebkurš notikums, kura dēļ organizācijai var rasties zaudējumi. Draudi var būt visdažādākie – dažādas katastrofas, terorisms, budžeta finansējuma zaudējums, komunikāciju bojājumi, datu bojājumi, kļūdas, neuzticīga personāla darbība un citi.

Fiziskā aizsardzība –informācijas resursu aizsardzība pret fiziskas iedarbības radītu informācijas nesēju apdraudējumu (piemēram zādzība, sprieguma pazemināšanās, aparatūras bojājumi u.c.).

Loģiskā aizsardzība – datu vai Informācijas resursu aizsardzība, kuru realizē ar programmatūras līdzekļiem, piemēram, identificējot IS lietotāju, pārbaudot viņa pilnvaru atbilstību attiecīgajām darbībām IS, pasargājot informāciju no tīšas vai nejaušas maiņas vai dzēšanas.

Ievainojamība - informācijas sistēmas nepilnība, kas ļauj kādam noteiktam apdraudējumam īstenoties un ietekmēt sistēmas drošību.

Ietekme – informācijas drošības incidenta rezultāts.

Informācijas resursi (IR), Informācija – datu faili, datu bāzes, arhīvi u.c. informācija (neatkarīgi no datu nesēja veida).

> **Ierobežotas pieejas informācija** – iekšējās aprites informācija, kurai IR turētājs ir noteicis pieejas personu loku.
>
> **Vispārpieejamā informācija** – Informācija, kas ir brīvi pieejama visiem organizācijas darbiniekiem un jebkurai citai personai, kas šo Informāciju ir pieprasījusi.
>
> **Augsta riska informācija** – Informācija, kuru lietojot nevietā, nesankcionēti mainot, sabojājot vai padarot nepieejamu pilnvarotām personām kādu laika

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

periodu, var rasties nozīmīgi un ilgstoši zaudējumi un ciest Organizācijas reputācija.

Vidēja riska informācija – Informācija, kuru lietojot nevietā, nesankcionēti mainot, sabojājot vai padarot nepieejamu pilnvarotām personām kādu laika periodu, organizācijai var rasties jūtami zaudējumi un ciest Organizācijas reputācija.

Zema riska informācija – Informācija, kuru lietojot nevietā, nesankcionēti mainot, sabojājot vai padarot nepieejamu pilnvarotām personām kādu laika periodu, organizācijai nerodas nopietni zaudējumi vai būtiski darbības traucējumi.

Incidents – gadījums, kurā IS apdraudējumi ir negatīvi ietekmējuši informācijas sistēmas darbību, izmantojot tās trūkumus.

Informācijas resursu aizbildnis - persona, kuru norīkojis IR turētājs un kura ikdienā ir atbildīga par attiecīgo informācijas resursu vai to daļu.

Informācijas resursu turētājs (IR turētājs) – organizācijas darbinieks, kurš ir atbildīgs par Informācijas resursiem (to pieejamību, integritāti, konfidencialitāti, lietošanu un lietošanas sekām) un kura pienākumi ir noteikti organizācijas normatīvos.

Integrēta valsts informācijas sistēma — loģiska valsts informācijas sistēmu apvienība, kuras ietvaros vienotā informācijas laukā tiek uzturēti atsevišķu valsts informācijas sistēmu dati.

Integritāte – raksturo, cik lielā mērā Informācija tiek uzglabāta un/vai pārraidīta pilnīga, precīza, patiesa un aktuāla.

Informācijas sistēma/-as (IS) – datu ievadīšanas, uzglabāšanas un apstrādes datorizēta sistēma, kas paredz lietotāju pieeju tajā glabātajiem datiem vai informācijai.

IS drošības pārvaldnieks (ISDP) - organizācijas darbinieks, kas ir atbildīgs par organizācijas IS drošības pārvaldību.

IT - Informācijas tehnoloģijas

ĪUMEPLS - Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāts.

Klasificēšana – Konfidencialitātes, Pieejamības un Vērtības līmeņa piešķiršana.
Informācijas drošības kategorijas:

Konfidencialitāte – īpašība, ka informācija nav pieejama vai netiek atklāta nepilnvarotiem indivīdiem, sistēmām vai procesiem.

Pieejamība – raksturo, cik lielā mērā pilnvarotās personas var piekļūt nepieciešamajai Informācijai ne vēlāk kā noteiktā laikā pēc Informācijas pieprasīšanas brīža;

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

Vērtība – Informācijas resursa nozīmīgums organizācijai, ko nosaka, izvērtējot iespējamos zaudējumus, kurus var radīt Informācijas zaudēšana, sabojāšana vai nonākšana nepiederošu personu rokās.

Nepilnība - *(angliski „*vulnerability”*)* raksturo sistēmas ievainojamības pakāpi, realizējoties konkrētam draudam, piemēram, vāja administratīvā sistēma, nav precīzi definēti pienākumi, atbildība, netiek veikta piekļuves kontrole vai tā ir nepilnīga (gan fiziskā piekļuve, gan loģiskā), nav informācijas sistēmas drošības noteikumu u. c.

Risks – organizācijas varbūtēja nespēja pilnvērtīgi un kvalitatīvi veikt kādu savu saistību vai funkciju izpildi. Informācijas drošības kontekstā tiek aplūkoti tikai tie riski, kas ir saistīti ar IS funkcionēšanu.

Organizācija – valsts pārvaldes iestāde, kuras pārziņā atrodas noteiktas informācijas sistēmas.

Tehnoloģiskie resursi (TR) – programmatūra (izpildāms programmas kods un konfigurācijas faili, kas nodrošina IS funkcionēšanu), datori, datortīklu aparatūra, komunikāciju līnijas u.c. tehniskie līdzekļi, ko izmanto informācijas apstrādei, pārraidei un glabāšanai.

Tehnoloģisko resursu turētājs (TR turētājs) – organizācijas darbinieks, kurš ir atbildīgs par tehnoloģisko resursu uzturēšanu un drošību.

Valsts informācijas sistēma (VIS) - strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek nodrošināta valsts funkciju izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana.

Valsts informācijas sistēmas lietotājs (Lietotājs) - juridiskā vai fiziskā persona, kura noslēgusi līgumu ar valsts informācijas sistēmas pārzini par datu lietošanu vai kura uz pieprasījuma pamata saņem datus valsts informācijas sistēmas pārziņa vai normatīvajos aktos noteiktajā kārtībā.

Valsts informācijas sistēmas pārzinis — valsts institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada valsts informācijas sistēmas darbību.

Valsts informācijas sistēmas turētājs - valsts informācijas sistēmas pārzinis vai tā pilnvarota institūcija, kas uztur šīs sistēmas informācijas un tehnisko resursu funkcionalitāti un nodrošina informācijas apriti.

Valsts informācijas sistēmu reģistrs - valsts reģistrs valsts informācijas sistēmu uzskaitei un to funkciju identificēšanai.

Valsts informācijas sistēmu savietotājs — valsts informācijas sistēmu, standartu un pārvaldības kopums, ar kura palīdzību tiek nodrošināta vairāku valsts informācijas sistēmu pilna vai daļēja funkcionalitāte integrētas valsts informācijas sistēmas ietvaros.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas” informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā”

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, tiek realizēti tādi nozīmīgi informācijas tehnoloģiju projekti kā Valsts informācijas sistēmu savietotāja ieviešana. 2008.gadā ir plānots uzsākt vērienīgus projektus izglītības informatizācijas un e-veselības jomās.

Informācijas tehnoloģiju izmantošana nenoliedzami sniedz būtiskus uzlabojumus daudzās dzīves jomās, tomēr līdz ar priekšrocībām parādās jauni riski. –Lai tos varētu kontrolēt ir nepieciešamība pievērst papildus uzmanību informācijas sistēmu drošībai. Nepieciešamība investēt informācijas sistēmu drošībā pieaug proporcionāli IT izmantošanas intensitātei. Jo vairāk kāda organizācija izmanto informācijas sistēmas, jo vairāk ir dažādu risku, ar kuriem tai ir jāsastopas. Mūsdienās informācijas sistēmu drošība sāk veidoties kā nozīmīga informācijas tehnoloģiju apakšnozare. Ja vel dažus gadus senā vēsturē organizācijas visā pasaulē informāciju sistēmu drošībai tērēja 1 – 2 procentus no sava kopējā informācijas tehnoloģiju budžeta, tad šodien šie izdevumi veido 3 – 5 procentus, bet atsevišķās valstīs pat 15 procentus no iestāžu tēriņiem informāciju tehnoloģiju jomā.

Vadlīnijām ir rekomendējošs raksturs. Vadlīnijas neatceļ normatīvajos aktos noteiktās prasības. Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāts neuzņemas atbildību par jebkādiem tiešiem, netiešiem, saistītiem, izrietošiem vai īpašiem zaudējumiem, kuri radušies vai var rasties saistībā ar šo vadlīniju izmantošanu.

IS drošība kā IT apakšnozare

Informācijas sistēmu drošības kā informācijas tehnoloģiju apakšnozares aizsākumi meklējami salīdzinoši nesenā pagātnē, vēl tikai 25 gadus atpakaļ nebija nepieciešamības runāt par IS drošības jautājumiem. Ja pasaulē ar automašīnām brauc jau vairāk kā 100 gadus un ir tradīcijās un noteikumos iesakņojušies vienoti ceļu satiksmes noteikumi, kas bez lielām problēmām ļauj pārvietoties visās pasaules valstīs, tad neilgajā laika posmā, kopš IS drošības jautājums ir kļuvis aktuāls, diemžēl nav izdevies izstrādāt vienotu standartu, kas definētu informācijas sistēmu drošību. Mūsu rīcībā ir vairāki starptautiski standarti – ISO/IEC 17799:2005 (ISO/IEC 27002:2005), ISO/IEC 13335, CoBIT, ISF standarts, tomēr tiem ir tikai rekomendējošs raksturs, un to definīcijas ir ļoti plašas.

Latvijas Republikā informācijas sistēmu drošība organizācijas valsts informācijas sistēmās tiek noteikta ar Ministru kabineta 2005.gada 11.oktobra noteikumiem Nr.765

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

„Valsts informācijas sistēmu vispārējās drošības prasības" (turpmāk – Noteikumi). Līdz ar Valsts informācijas sistēmu likuma spēkā stāšanos spēku zaudēja Ministru kabineta 2000.gada 24.marta noteikumi Nr.106 „Informācijas sistēmu drošības noteikumi" darbība un pašreiz formāli sanāk, ka par informācijas sistēmu drošību ir jādomā tikai valsts informāciju sistēmu pārziņiem.

IS drošība un atbildības

Atbildība par informācijas sistēmu drošības nodrošināšanu jāuzņemas ikvienai publiskās pārvaldes organizācijai, neatkarīgi no tā vai tās pārziņā ir vai nav kāda valsts informācijas sistēma. Tikai palielinot informācijas sistēmu drošības līmeni katrā organizācijā atsevišķi, iespējams palielināt informācijas sistēmu drošības līmeni visās valsts informācijas sistēmās kopumā. Katrai valsts iestādei var būt atšķirīga pieeja tam, kā plānot un cik lielus finansu resursus ieguldīt informācijas sistēmu drošībā, jo būtiski atšķiras riski, ar kuriem tām ir jāsastopas. Tomēr katrai valsts organizācijai mūsdienās ir nepieciešama sava informācijas sistēmu drošības politika.

Kopumā var izdalīt trīs nozīmīgus argumentus IS drošības politikas nepieciešamībai katrā publiskās pārvaldes organizācijā:

1. veselais saprāts – instinktīvas rūpes par savu drošību. Ja manas organizācijas IS vide būs droša un sadarbības organizācijas IS vide būs droša, tad mūsu savstarpējā sadarbība būs droša;
2. normatīvo aktu bāze – Valsts informāciju sistēmu likums, Fizisko personu datu aizsardzības likums, Informācijas atklātības likums un no tiem izrietošie noteikumi;
3. reāla atbildība drošības incidenta gadījumā – saistoša ne tikai organizācijai, bet arī tās vadītājam. Sekas var skart arī citas informācijas sistēmas un sadarbības partnerus. Ļoti bieži drošības incidenta rezultātā tiek nodarīts ne tikai morālais, bet arī finansiālais kaitējums. Piemēram, likumā noteikto normu neievērošanas gadījumā var tikt piespriests administratīvais sods organizācijas vadītājam, cietusī puse var vērsties ar prasību tiesā un pieprasīt kompensāciju. Drošības incidentu gadījumā var tikt nodarīts arī nemateriāls kaitējums (kurš bieži ir nopietnāks par materiālo) būtiski iedragājot organizācijas reputāciju.

Jāņem vērā, ka valsts organizāciju informācijas sistēmu vājās vietas var tikt izmantotas arī politiskos nolūkos, kā tas notika 2007.gada maijā Igaunijā, kad, atbildot uz „Bronzas kareivja" pārvietošanu Tallinā, Igaunijas informācijas sistēmas piedzīvoja plaša mēroga hakeru uzbrukumus.

Vadlīniju izstrādes mērķis

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīniju izstrādes mērķis ir palīdzēt organizācijām ieviest normatīvo aktu noteiktajām prasībām atbilstošu informācijas sistēmu drošības politiku un tai pakārtotos normatīvus. Vadlīniju izstrāde balstīta uz Noteikumiem un Latvijā pieņemto LVS ISO/IEC 17799:2005 standartu, kas

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

vispārējā līmenī nosaka, ko vajadzētu saturēt IS drošības politikai un pakārtotiem drošības pārvaldības dokumentiem.

Šobrīd Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāts strādā pie Noteikumu grozījumiem un papildinājumiem, lai noteikumi attiektos uz sistēmu pārziņiem kopumā, nevis tikai uz atsevišķām valsts informācijas sistēmām. Tādēļ vadlīnijas ir veidotas ar mērķi aptvert sistēmu pārziņu pārvaldībā visas esošās informācijas sistēmas un definēt to drošības prasības.

Jāņem vērā, ka izstrādātās vadlīnijas nav uztveramas kā paraugs, bet gan kā ceļvedis individuālas un organizācijai piemērotas IS drošības pārvaldības ieviešanā. Šajā procesā nozīmīgi ņemt vērā organizācijas struktūru, pieņemamo riska līmeni, pieejamos resursus un vajadzības, kas dažādās organizācijās var būtiski atšķirties.

Veiksmīgai informācijas sistēmu drošības pārvaldības modeļa ieviešanai ir jāsākas organizācijas vadības līmenī. Ja vadība neizpratīs IS drošības politikas nepieciešamību, tā nepiešķirs adekvātus finansiālos un cilvēkresursus tās realizācijai. Tādā gadījumā IS drošības pārvaldības modeli ieviest nebūs iespējams.

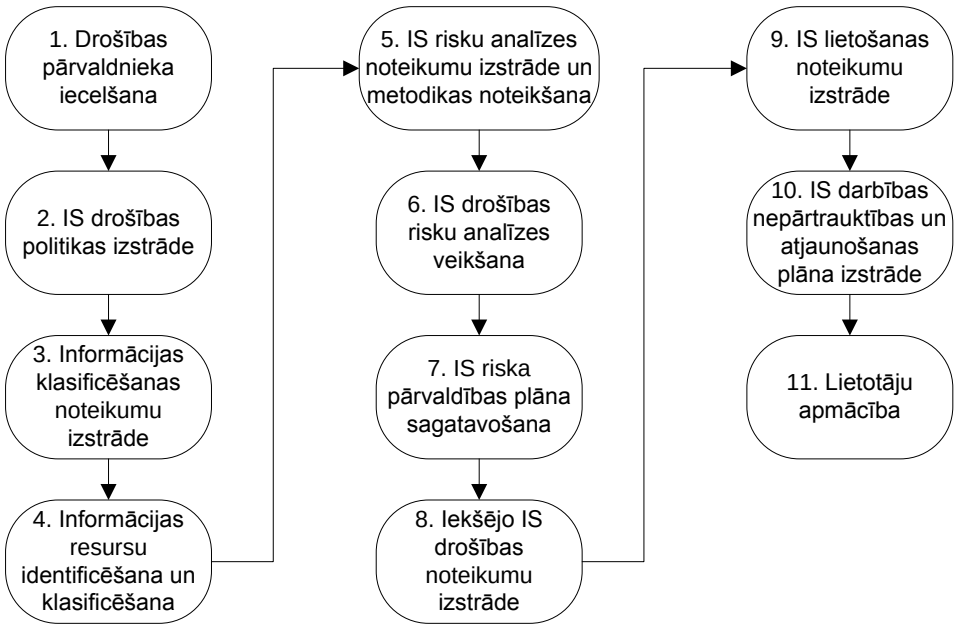
Bieži tiek diskutēts, vai IS drošības uzlabošana ir tehnoloģisks vai organizatorisks process. , Pareizāk būtu informācijas sistēmu drošības nodrošināšanu uztvert kā abu šo procesu mijiedarbību. Pastāv vairākas problēmas, kuras, izmantojot tikai tehnoloģiskus vai tikai organizatoriskus līdzekļus, nav efektīvi atrisināmas. Piemēram, darbinieka uzvedības kontrole. Lai gan teorētiski ar tehnisko līdzekļu palīdzību būtu iespējams veikt kontroli, praktiski šāds risinājums prasītu nesamērojami lielus finansiālos līdzekļus. Darbiniekam ne tikai apzinīgi jāattiecas pret saviem darba pienākumiem, viņam jābūt arī zināšanām, kā pareizi rīkoties, lai neapdraudētu informācijas sistēmu drošību. Informācijas sistēmu drošības politika, galvenokārt, ir zināšanu avots kā izturēties konkrētā situācijā, vai kā vadība vēlētos, lai darbinieks izturas.

IS drošības pārvaldības ieviešana un saistītie procesi

Drošības pārvaldības ieviešanai var būt divas pieejas. Pirmā no tām – kā šablonu izmantot jau gatavus drošības politikas un pakārtotos drošības pārvaldības dokumentus. Šī pieeja ir ātra un lēta, bet, diemžēl, formāla un līdz ar to arī neefektīva. Otra pieeja - izmantojot vadlīnijas, ieviest savu drošības politiku, kas atbilstu organizācijas struktūrai, resursiem un mērķiem. Šāda veida drošības politikas ieviešana būtu sarežģītāka, laikietilpīgāka un dārgāka, bet rezultātā ievērojami uzlabotos organizācijas IS drošība.

IS drošības pārvaldības ieviešanai jāsākas ar IS drošības organizācijas izveidi. 1.attēlā ir atspoguļots IS drošības pārvaldības ieviešanas process.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas” informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā”



1. attēls. IS drošības pārvaldības ieviešanas process

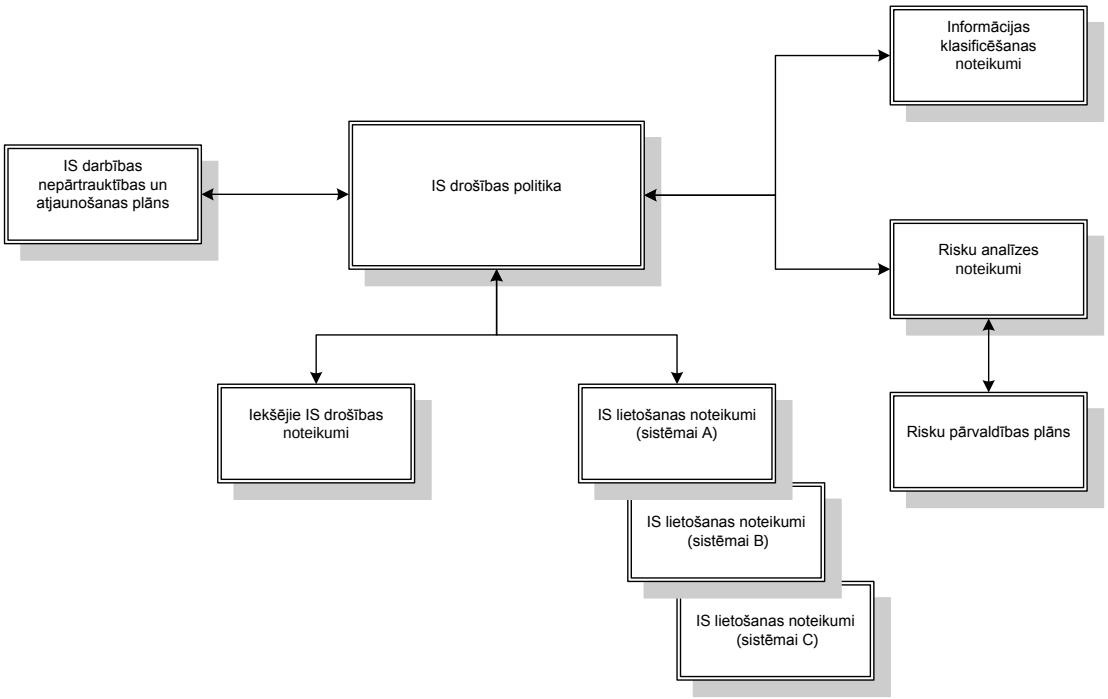
Piezīme: IS drošības pārvaldības ieviešanas process ir attēlots kā viens otram secīgi sekojoši atsevišķi pasākumi. Praksē šie paši pasākumi bieži tiek īstenoti vienlaicīgi.

Organizācijas primārais uzdevums ir pienākumu sadale, definējot atbildības, kuras tiek fiksētas darbinieku amatu aprakstos.

Pēc pienākumu sadalījuma definēšanas ir jāizstrādā sākotnējā IS drošības politika, no kuras tad arī izriet pārējās komponentes - noteikumi un procedūras, kas ir veids kā tiek kontrolēta politikas realizēšana, ieviešana un atjaunošana.

2.attēlā ir atspoguļoti minimāli nepieciešamie dokumenti, kuri ir jāizstrādā, lai organizācijā ieviestu IS drošības pārvaldību.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"



2. attēls. IS drošības pārvaldības minimāli nepieciešamie dokumenti

Svarīgi atcerēties!

Atbilstoši Noteikumi, drošības politiku, iekšējo sistēmas drošības noteikumus, sistēmas lietošanas noteikumu, sistēmas drošības riska pārvaldības plānu un sistēmas atjaunošanas plānu apstiprina Valts informācijas sistēmas pārzinis. **Tātad, minētie dokumenti ir jāizdod iekšējo normatīvo aktu veidā.**

IS drošības pārvaldības ieviešanas procesu laikā veicamie uzdevumi detalizēti aprakstīti turpmākajās nodaļās, bet procesu un atbildīgo sadalījums nodaļā 2.1., kā arī katras nodaļas sākumā.

Vadlīnijas sastāv no sekojošām nodaļām, kas apskata IS drošības pārvaldības ieviešanas modeli:

1. Nodaļa. IS drošības politikas izstrāde un īstenošana
2. Nodaļa. Informācijas sistēmu drošības organizācija
3. Nodaļa. Informācijas klasificēšanas noteikumu izstrāde un ievērošana
4. Nodaļa. Informācijas sistēmu drošības risku analīze
5. Nodaļa. Informācijas sistēmu drošības riska pārvaldības plāna izstrādāšana un izpilde
6. Nodaļa. Iekšējo informācijas sistēmu drošības noteikumu izstrāde un ievērošana
7. Nodaļa. Informācijas sistēmu lietošanas noteikumu izstrāde un ievērošana
8. Nodaļa. Informācijas sistēmu darbības nepārtrauktības un atjaunošanas plāna izstrāde un izpilde
9. Nodaļa. Biežāk uzdotie jautājumi
10. Nodaļa. Saites uz Interneta resursiem
11. Nodaļa. Pielikumi ar dokumentu paraugiem

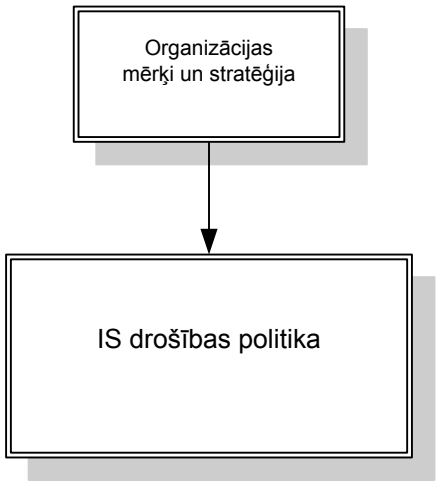
Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

1. IS drošības politikas izstrāde un īstenošana

Lai noteiktu organizācijas informācijas sistēmu (IS) drošības principus, ir jāizstrādā kopēja IS drošības politika, kas aptvertu sistēmas pārziņa pārvaldībā esošās informācijas sistēmas, nosakot atbildīgos IS drošības jomā un paužot organizācijas vadības nostāju, kāpēc organizācijas rīcībā esošā informācija ir svarīga tās mērķu īstenošanai un kā tiek nodrošināta informācijas un tehnoloģisko resursu aizsardzība.

Drošības politikas mērķis ir definēt organizācijas vadības nostāju un atbalstu informācijas drošības nodrošināšanai, atbilstoši organizācijas vajadzībām, saistošai likumdošanai un drošības normām.

IS drošības politikas nostādnes tiek noteiktas atbilstoši organizācijas definētajiem mērķiem un stratēģijai (skatīt 3.attēlu).



3. attēls. Organizācijas mērķi un IS drošības politika

IS drošības politika ieņem centrālo vietu organizācijas IS drošības organizācijā un no tās izriet visi ar IS drošību saistītie noteikumi, kārtības, procedūras, plāni un rīkojumi. IS drošības politikas nostādnes ir jāzina jebkuram organizācijas darbiniekam.

Ar ko sākt?
Galvenā atbildība par IS drošības politikas izstrādi un ieviešanu gulstas uz organizācijas vadības, kā arī informācijas drošības pārvaldnieka pleciem. Pastāv kļūdains uzskats, ka par IS drošības pasākumu noteikšanu un ieviešanu ir atbildīga tikai IT nodaļa.

Organizācijas vadībai un informācijas resursu turētājiem ir jāatceras, ka IT speciālisti var palīdzēt formulēt, ieviest un uzraudzīt IS drošības pasākumus, bet galvenais iniciators un procesa virzītājs ir organizācijas vadība, kurai sākotnēji ir jāpieņem lēmums par sekojošiem jautājumiem:

1. Kāda būs organizācijas IS drošības struktūra (*skatīt 2. nodaļu*)?
2. Kā tiks sadalīta atbildība par IS drošības pasākumu ieviešanu un uzturēšanu starp dažādām organizācijas struktūrvienībām?

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

3. Vai ir apzināti iespējamie riski un novērtēti to mazināšanai nepieciešamie pasākumi?
4. Vai IS drošības pasākumu realizēšanai tiek piešķirti adekvāti finansu un cilvēku resursi?
5. Vai organizācija rūpējas par IS drošību tikai, lai formāli izpildītu ārējo normatīvu prasības vai arī ir reāla izpratne IS drošības pasākumu lietderību un nepieciešamību?

Drošības politikas dokumenta sagatavošana ir jāuztic organizācijas IS drošības pārvaldniekam, kas to veic sadarbojoties ar informācijas resursu un tehnoloģisko resursu turētājiem, bet apstiprināšanai ir jānotiek vadības līmenī. IS drošības pārvaldnieks ir atbildīgs par visu nepieciešamo darbu inicializāciju, koordinēšanu un IS drošības politikas realizēšanu dzīvē (skatīt 1.tabulu).

Process	**Procesa virzītājs**	**Procesa izpildītājs**	**Sasniedzamais rezultāts**	**Dokumenta izstrādātājs**	**Dokumentu apstiprina**
IS drošības politikas izstrāde	Organizā-cijas vadība vai IS drošības komiteja	Drošības pārvaldnieks	Izstrādāta IS drošības politika	Drošības pārvaldnieks sadarbībā ar IR un TR turētājiem	Organizā-cijas vadība vai IS drošības komiteja

1.tabula. IS drošības politikas izstrādes procesa iesaistītās un atbildīgās personas

Pēc drošības politikas izstrādes un dokumenta apstiprināšanas, ar tā saturu ir jāiepazīstina visi organizācijas darbinieki. Iesaistītām trešajām pusēm, drošības politikas nostādnes un prasības ir jāietver savstarpējos līgumos.

Svarīgi atcerēties!
Drošības politika definē organizācijas kopējo nostāju drošības jautājumos, bet specifiskas drošības prasības detalizētāk ir jāizskaidro pakārtotos dokumentos, tādos kā iekšējie informācijas sistēmu drošības noteikumi (*skatīt 6. nodaļu*), informācijas sistēmas lietošanas noteikumi (*skatīt 7. nodaļu*), u.c. Drošības politikas un pakārotie dokumenti jāuztur un jāatjaunina, pamatojoties uz regulāru drošības pārskatu un to analīzes rezultātiem.

Normatīvo aktu prasības
Atbilstoši Noteikumiem, IS drošības politikai ir jāsatur vismaz sekojošas sadaļas:

1. sistēmas drošības politikas mērķus un pamatnostādnes;
2. sistēmas raksturojumu un analīzi drošības jomā;
3. sistēmas drošības vadības organizācijas principus;
4. sistēmas drošības atbilstību normatīvajiem aktiem un standartiem;
5. sistēmas drošības principus un kritērijus (piemēram, sistēmas nepārtrauktās darbības laiks, sistēmas darbības atjaunošanas laiks, sistēmas drošības riska pieņemamais līmenis, sistēmas drošības incidenta atklāšanas laiks, pieļaujamais neveiksmīgo piekļūšanas mēģinājumu skaits).

➢ *Pielikums. IS drošības politikas dokumenta paraugu skatīt pielikumā Nr.1.*
Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

2. Informācijas sistēmu drošības organizācija

IS drošības politikas ieviešanu var iedalīt vairākos vienlīdz nozīmīgos posmos – izstrādāšana, ieviešana, uzturēšana.

Sākotnējā *izstrādāšanas posmā* būtiska loma ir organizācijas vadībai. Tās primārie uzdevumi ir:

- drošības organizācijas izveide;
- darbinieku lomu sadale;
- pilnvaru piešķiršana.

Ieviešanas posmā svarīgi, lai pieņemtie lēmumi nepastāvētu tikai kā mutvārdu vienošanās, bet tiktu dokumentēti - jānodrošina pienākumu fiksēšana amatu aprakstos un departamentu, nodaļu nolikumos.

2.1 Lomu sadalījums

Situācijā, kad visas lomas realizētas organizācijas ietvaros to sadalījums ir sekojošs: (*skatīt 4.attēlu*):

1. IS drošības pārvaldnieka pienākumi:
    a. informācijas klasifikācijas un risku analīzes procesa vadība;
    b. nepieciešamo IS drošības normatīvu izstrāde un uzturēšana;;
    c. noteikto drošības prasību ievērošanas kontrole;
    d. IT drošības incidentu pārvaldība;
    e. dalība IS darbības atjaunošanas un nepārtrauktības plānošanā;
    f. darbinieku apmācība informācijas drošības jomā.

2. IS drošības komitejas pienākumi:
    a. atbildība par informācijas drošības politikas definēšanu un tās saskaņošana ar organizācijas mērķiem;
    b. informācijas drošības politikas pārbaude un apstiprināšana;
    c. drošības incidentu analīze;
    d. resursu turētāju nozīmēšana;
    e. IS drošības risku pārvaldības plāna apstiprināšana.

Piezīme. Mazākām organizācijām drošības komiteju var neveidot, bet minētās funkcijas ir jāuzņemas organizācijas vadībai.

3. IS auditora pienākumi:
    a. IS izveides un darbības atbilstības pārbaude spēkā esošajai likumdošanai un organizācijas iekšējiem normatīviem;
    b. IS risku un nepilnību identificēšana,
    c. vadības informēšana par pārbaužu rezultātiem un rekomendācijām trūkumu novēršanai.

Piezīme. Bieži auditors ir trešās puses vai ārpakalpojumu sniedzēja pārstāvis.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

4. Informācijas lietotāja pienākumi:
    a. IS drošības noteikumu ievērošana,
    b. atbildīgs par visām darbībām, kuras ir veiktas ar viņa lietotāja vārdu IS;
    c. informēt informācijas drošības pārvaldnieku par visiem IT drošības incidentiem un aizdomīgiem notikumiem.

Piezīme. Valsts informāciju sistēmās informācijas lietotāju definētā loma ir valsts informāciju sistēmu lietotāji. Parasti informācijas lietotāji ir organizācijas darbinieki vai ārēji lietotāji.

Pēc resursu piederības tiek identificētas sekojošas lomas:

1. Informācijas resursu turētājs:
    a. atbild par rīcībā esošo informācijas resursu klasificēšanu;
    b. nosaka informācijas resursu lietošanas kārtību;
    c. apstiprina lietotāju pieejas tiesības;
    d. piedalās IS risku analīzes veikšanā, kas attiecās uz konkrētā IR turētāja pārziņā esošo IS;
    e. nosaka informācijas resursu drošības prasības.

Piezīme. Informācijas resursu turētājs cieši sadarbojas ar tehnoloģisko resursu turētāju.

2. Tehnoloģisko resursu turētājs:
    a. atbild par tehnoloģisko resursu fiziskās un loģiskās aizsardzības pasākumu nodrošināšanu;
    b. sadarbojas ar informācijas resursu turētāju, lai īstenotu datu aizsardzības prasības,
    c. piedalās IS risku analīzē,
    d. veic IS darbības atjaunošanas nodrošināšanu;

Piezīme. Ir novērots, ka dažādu iestāžu normatīvos terminoloģija atšķiras - tehnoloģisko resursu turētājs tiek saukts arī par tehnisko resursu turētāju.

3. Informācijas resursu aizbildnis ir persona, kuru norīkojis IR turētājs un kura ikdienā ir atbildīga par attiecīgo informācijas resursu vai to daļu.

Svarīgi atcerēties!
Informācijas resursu turētājs parasti ir struktūrvienības vadītājs, kas atbild par attiecīgajiem organizācijas procesiem, kurus veic izmantojot IS. Informācijas resursu turētājs ir tas kas nosaka nepieciešamo IT pakalpojumu kvalitātes un drošības prasības, bet tehnoloģisko resursu turētāji nodrošina IT pakalpojumu piegādi atbilstoši pieprasītajam kvalitātes līmenim.

Informācijas resursu turētāja pienākumos ietilpst nepieciešamā informācijas drošības līmeņa noteikšana, sistēmas attīstības plānošana. Savukārt, tehnoloģisko resursu turētāja loma analoģiska sistēmas administratora amatam. Tehnoloģisko resursu turētājs atbildīgs par informācijas resursu turētāja izvirzīto prasību tehnisko nodrošinājumu.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

2.tabulā attēloti IS drošības pārvaldības procesi un atbildīgās personas:

Nr.p.k.	Process	Procesa virzītājs	Procesa izpildītājs	Sasniedzamais rezultāts	Dokumenta izstrādātājs	Dokumentu apstiprina
1	Drošības pārvaldnieka iecelšana	Organizācijas vadība	Organizācijas vadība	Iecelts drošības pārvaldnieks, ar amata aprakstā definētiem uzdevumiem		
2	IS drošības politikas izstrāde	Organizācijas vadība	Drošības pārvaldnieks	Izstrādāta IS drošības politika	Drošības pārvaldnieks sadarbībā ar IR turētājiem un TR turētājiem	Organizācijas vadība
3	Informācijas klasificēšanas noteikumu izstrāde	Drošības pārvaldnieks	Drošības pārvaldnieks	Izstrādāti informācijas klasificēšanas noteikumi	Drošības pārvaldnieks	Organizācijas vadība
4	Informācijas resursu identificēšana un klasificēšana	Organizācijas vadība	Drošības pārvaldnieks	Identificēti organizācijai nozīmīgie informācijas resursi, vadības apstiprināti IR un TR turētāji.		

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

		Drošības pārvaldnieks	Drošības pārvaldnieks sadarbībā ar IR turētājiem	Izveidots informācijas resursu klasifikators. Informācijas resursiem ir noteiktas to klasifikācijas vērtības (konfidencialitāte, integritāte, pieejamība).		
5	IS risku analīzes noteikumu izstrāde un metodikas noteikšana	Drošības pārvaldnieks	Drošības pārvaldnieks	Izstrādāti IS risku analīzes noteikumi un noteikta IS risku analīzes metodika	Drošības pārvaldnieks	Organizācijas vadība
6	IS drošības risku analīzes veikšana	Drošības pārvaldnieks	Drošības pārvaldnieks sadarbībā ar IR un TR turētājiem	Veiktas IS risku analīzes un noteiktas nepieciešamās drošības prasības	Drošības pārvaldnieks	Organizācijas vadība
7	IS risku pārvaldības plāna sagatavošana	Organizācijas vadība	Drošības pārvaldnieks	Sastādīts IS risku pārvaldības plāns	Drošības pārvaldnieks	Organizācijas vadība

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

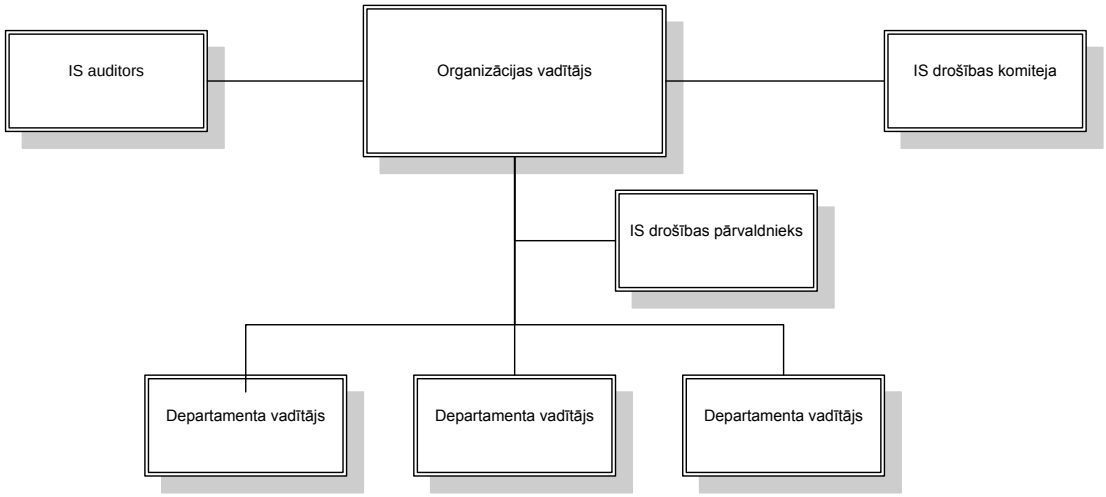
8	Iekšējo IS drošības noteikumu izstrāde	Drošības pārvaldnieks	Drošības pārvaldnieks sadarbībā ar IR un TR turētājiem	Izstrādāti iekšējie IS drošības noteikumi	Drošības pārvaldnieks	Organizācijas vadība
9	IS lietošanas noteikumu izstrāde	Drošības pārvaldnieks	Drošības pārvaldnieks sadarbībā ar IR un TR turētājiem	Izstrādāti IS lietošanas noteikumi	Drošības pārvaldnieks	Organizācijas vadība
10	IS darbības nepārtrauktības un atjaunošanas plāna izstrāde	Organizācijas vadība	Drošības pārvaldnieks sadarbībā ar IR un TR turētājiem	Izstrādāts IS darbības nepārtrauktības un atjaunošanas plāns	Drošības pārvaldnieks	Organizācijas vadība
11	Lietotāju apmācība	Drošības pārvaldnieks	Drošības pārvaldnieks	Apmācīti organizācijas darbinieki		

2. tabula. IS drošības pārvaldības procesi un atbildīgās personas

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

Katra loma cieši saistīta ar noteiktiem pienākumiem un atbildību. Vadība pilnvaro drošības pārvaldnieku, kura pārraudzībā ir ar IS drošību saistītu jautājumu koordinācija. Lielākās organizācijās visaptverošu jautājumu risināšanai tiek izveidota IS drošības komiteja, kuras sastāvā ietilpst organizācijas vadošie darbinieki, to skaitā arī drošības pārvaldnieks.

No funkcionālās struktūras skatoties nav svarīgi, kā pakļautībā strādā drošības pārvaldnieks. Bet tā kā nepietiekamu drošības pārvaldnieka pilnvaru gadījumā var tikt kavēta svarīgu lēmumu savlaicīga pieņemšana, drošības pārvaldniekam vajadzētu būt tiešā organizācijas vadītāja vai viņa vietnieka pakļautībā.



4. attēls. Optimālā IS drošības organizācija

Uzturēšanas posms saistīts ar IS kontroli, problēmu risināšanu un IS attīstības plānošanu. Drošības pārvaldnieks sadarbojoties ar informācijas resursu turētāju un tehnoloģisko resursu turētāju ir atbildīgs par IS drošības risku identificēšanu un kontroli. Papildus atbildība jāuzņemas arī iekšējā audita nodaļai, kura, izmantojot savus vai ārējos resursus, kontrolē, kā noteikumi un procedūras tiek ievērotas.

Svarīgs priekšnosacījums veiksmīga uzturēšanas posma realizācijai ir noteikto funkciju korekta izpilde. Tāpēc būtiska nozīme ir lietotāju apmācībai. Tikai apmācīti IS lietotāji zinās, kā atbilstoši rīkoties ikdienā un arī drošības incidentu gadījumā. IS drošības aizsargāšanas nolūkos ir svarīgi, lai drošības politikas prasības ievērotu gan iekšējie, gan ārējie sistēmas lietotāji.

Atbilstoši organizācijas struktūrai, resursiem un vajadzībām pienākumu apraksti var tikt mainīti.

2.2 Organizācijas IS ar ārējiem lietotājiem, vai IS pieslēgumiem

Nereti lomu pienākumi tiek realizēti ārpus organizācijas. Iespējama situācija, kad organizācija kādu no IS pārvaldības vai drošības funkcijām deleģē veikt ārējam pakalpojumu sniedzējam vai citai organizācijai. Palielinot uzsvaru uz elektronisko Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

datu apstrādi un ieviešot arvien jaunas informācijas sistēmas, šodien valsts organizācijas sastopas ar komplicētākiem gadījumiem, kas atšķirīgas no iepriekš aprakstītās standartsituācijas.

Svarīgi atcerēties!
Ja organizācija deleģē trešo pusi, atbildība par informācijas pieejamību, integritāti un konfidencialitāti gulstas uz informācijas resursu turētāja pleciem. Ir jādefinē drošības prasības ārējiem lietotājiem un jāpanāk to ievērošana savstarpējo līgumu ietvaros.

Ar visiem IS ārējiem lietotājiem, to pārziņiem (organizācijas, IS pieslēgumi) ir jāslēdz IS izmantošanas līgumi, kuros tiek minētas drošības politikā ietvertās prasības un prasības tās ievērot. Prasības var tikt definētas līdzīgi kā nodaļā 2.3. par ārpakalpojuma izmantošanu.

Līgumos ar ārējiem pakalpojumu sniedzējiem, lietotājiem obligāti ir jāiekļauj punkts, kādas būs soda sankcijas par drošības prasību neievērošanu!

2.3 Sistēmas turētāja funkcijas nodotas ārpakalpojumu sniedzējam

Sistēmas pārzinis savus uzdevumus, kuri nepieciešami sistēmas darbības nodrošināšanai var deleģēt vienam vai vairākiem ārpakalpojumu sniedzējiem.

Izvietojot IS ārpakalpojumu sniedzēja datu centrā ārpakalpojumu sniedzējs nekļūst par tehnoloģisko resursu turētāju – viņš pilda deleģētos pienākumus. Organizācijas nozīmētais tehnoloģisko resursu turētājs ir atbildīgā persona, kura regulāri seko līdzi un pārliecinās, ka ārpakalpojumu sniedzējs pilda noteiktās IS pakalpojumu pieejamības un IS drošības prasības, līdzīgi kā to darītu tehnoloģisko resursu turētājs, ja IS atrastos organizācijas datu centrā.

Svarīgi atcerēties!
Sistēmas pārzinim, kurš plāno saņemt ārpakalpojumu, IS drošības politikā un citos saistošos normatīvos ir jānosaka ārpakalpojuma izmantošanas prasības.

Ārpakalpojuma izmantošanas prasības nosaka:
1. kārtību, kādā tiek pieņemti lēmumi par ārpakalpojuma saņemšanu;
2. ārpakalpojuma līguma slēgšanas, izpildes uzraudzības un izbeigšanas kārtību;
3. kārtību kā tiek īstenota sadarbība ar ārpakalpojumu sniedzēju un saņemtā ārpakalpojuma apjoma un kvalitātes uzraudzība un saistīto risku pārvaldība;
4. atbildīgās personas un struktūrvienības, kas sadarbojas ar ārpakalpojumu sniedzēju, kā arī attiecīgo personu tiesības un pienākumus.
5. sistēmas pārziņa rīcību, ja ārpakalpojumu sniedzējs nepilda vai nevarēs pildīt ārpakalpojuma līguma noteikumus.

Sistēmas pārzinis slēdz ārpakalpojumu līgumu, kurā nosaka:
1. saņemamā ārpakalpojuma aprakstu;

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

2. precīzas ārpakalpojuma apjoma un kvalitātes prasības - minimālās prasības atbilstoši Iekšējiem IS drošības noteikumiem (*skatīt 6. nodaļu*);
3. pārziņa un ārpakalpojumu sniedzēja tiesības un pienākumus, to skaitā pārziņa tiesības pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti un dot ārpakalpojumu sniedzējam obligāti izpildāmus norādījumus jautājumos, kas saistīti ar ārpakalpojuma godprātīgu, kvalitatīvu, savlaicīgu un normatīvajiem aktiem atbilstošu izpildi;
4. soda sankcijas;
5. līguma laušanas nosacījumus.

Svarīgi atcerēties!
Ārpakalpojuma saņemšana neatbrīvo sistēmas pārzini no atbildības, kas noteikta likumā vai līgumā ar tās klientiem. Pārzinis ir atbildīgs par ārpakalpojumu sniedzēja veikumu tādā pašā mērā kā par savējo.

Līgumos ar ārpakalpojumu sniedzējiem obligāti ir jāiekļauj punkts, kādas būs soda sankcijas par drošības prasību neievērošanu!

2.4 Vienas organizācijas pārvaldībā integrētas vairākas Valsts informācijas sistēmas

Ja vienas organizācijas pārvaldībā ir savstarpēji integrētas vairākas valsts informācijas sistēmas, tad katrai IS var būt savs informācijas resursu turētājs, bet kopīgs tehnoloģisko resursu turētājs.

Raugoties no drošības standartu puses, ir nepieciešams izstrādāt vienotu IS drošības politiku, kas aptvertu visas sistēmas pārziņa pārvaldībā esošās informācijas sistēmas, bet Noteikumi paredz, ka ir nepieciešams izstrādāt tik drošības politikas, cik Valsts informācijas sistēmas ir pārziņa pārvaldībā.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

3. Informācijas klasificēšanas noteikumu izstrāde un ievērošana

Lai novērtētu, kura informācija organizācijai ir svarīga un kā to atbilstoši aizsargāt ir jāveic informācijas klasificēšana.

Klasificēšanas mērķis ir savlaicīgi, izmantojot vienotu metodiku, identificēt organizācijas rīcībā esošo informāciju, novērtēt tās nozīmību, iedalot to klasifikācijas grupās un nodrošināt katras informācijas grupas aizsardzību atbilstoši tās klasifikācijas līmenim.

Ar ko sākt?

Informācijas klasificēšanu veic saskaņā ar klasifikācijas noteikumiem, kurus izstrādā saskaņā ar organizācijas IS drošības politiku un ārējo normatīvu prasībām.

Informācijas klasificēšanas noteikumu izstrādes procesā iesaistītās un atbildīgās personas skatīt 3.tabulā.

Process	**Procesa virzītājs**	**Procesa izpildītājs**	**Sasniedzamais rezultāts**	**Dokumenta izstrādātājs**	**Dokumentu apstiprina**
Informācijas klasificēšanas noteikumu izstrāde	Drošības pārvaldnieks	Drošības pārvaldnieks	Izstrādāti informācijas klasificēšanas noteikumi	Drošības pārvaldnieks	Organizācijas vadība

3.tabula. Informācijas klasificēšanas noteikumu izstrādes process un atbildīgās personas

Informācijas klasificēšanas noteikumos ietvertiem klasifikācijas principiem un metodei ir jābūt skaidriem un ērti izmantojamiem. Kopumā klasificēšanas process ietver četrus posmus.

Sākotnēji organizācija identificē tai nozīmīgos informācijas resursus. IR vēlams piesaistīt konkrētām IS vai procesiem.

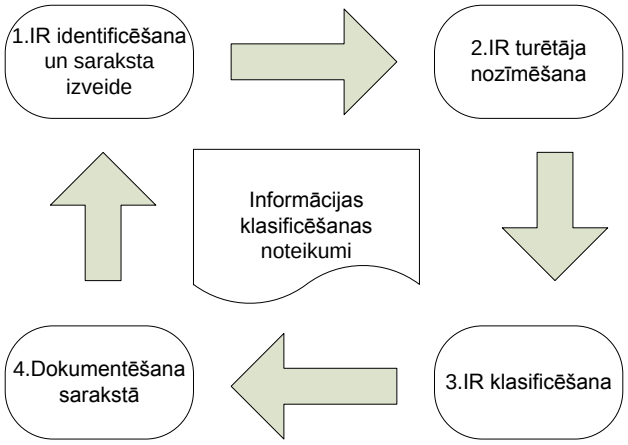
Otrajā posmā visiem identificētajiem resursiem nozīmē informācijas resursu (IR) turētājus, kas pamatā ir to struktūrvienību vadītāji, kuri savu pienākumu veikšanai izmanto šos IR.

Trešajā posmā IR turētāji sadarbojoties ar drošības pārvaldnieku klasificē savus IR saskaņā ar organizācijā noteiktiem klasifikācijas principiem vai metodi.

Ceturtā posmā visi klasifikācijas rezultāti tiek apkopoti vienotā sarakstā vai klasifikatorā.

Informācijas klasificēšanas procesu skatīt 5.attēlā.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"



5. attēls. Informācijas klasificēšanas process

Informācijas resursu turētāju nozīmē ar vadības lēmumu un tas ir organizācijas darbinieks, kas ir atbildīgs par viņam uzticēto informācijas resursu drošību un pamatā ir šo resursu galvenais lietotājs. Termins "turētājs" nenozīmē resursu piederību, bet nosaka, ka organizācijas darbiniekam ir noteikti zināmi pienākumi.

Turētāja pienākumus nosaka organizācijas normatīvos un tie ir:
- klasificēt īpašumā esošo informāciju;
- noteikt sistēmas lietošanas kārtību un piešķirt darbiniekiem tiesības piekļūt informācijai vai sistēmai un lietot to;
- veikt īpašumā esošo informācijas resursu vai sistēmas risku analīzi;
- nodrošināt, ka īpašumā esošā informācija vai sistēma ir atbilstoši aizsargāta;
- noteikt un apstiprināt izmaiņas sistēmā (ietverot arī IS drošību);
- iesaistīties sistēmas drošības pārbaudēs.

Drošības pārvaldniekam ir jānodrošina apmācības process, kas uzlabotu resursu turētāju zināšanas un iemaņas savu pienākumu sekmīgai izpildei. Resursu turētājs savu ikdienas pienākumu izpildi var uzticēt veikt aizbildnim, tomēr atbildību par resursa pārvaldību turētājs nevar nodot citam darbiniekam.

Svarīgi atcerēties!
Organizācijas, kuras izmanto kompleksas un sarežģītas IS var apvienot dažādos IR, kuri kopā nodrošina kādu noteiktu organizācijas funkciju vai pakalpojumu un noteikt šim pakalpojumam turētāju. Pakalpojuma turētājs ir atbildīgs par noteiktā pakalpojuma piegādes kvalitātes un drošības prasību noteikšanu un kontroli. Parasti starp pakalpojuma turētāju un pakalpojuma tehnisko piegādātāju (IT daļu vai ārpakalpojumu sniedzēju) tiek slēgti pakalpojuma līmeņa lūgumi *(SLA)*, kuros precīzi un izmērāmi nosaka gan funkcionālās gan drošības prasības pakalpojuma piegādei.

Klasifikāciju informācijas resursa turētājs veic sadarbībā ar organizācijas IS drošības pārvaldnieku, ņemot vērā klasifikācijas noteikumos noteikto metodi. Informācijas klasificēšana attiecas uz visu organizācijas rīcībā esošo informāciju

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

neatkarīgi no informācijas nesēja veida (papīrs, diskete, cietais disks, magnētiskā lente vai citi informācijas nesēji).

Tā kā informācijas drošību nosaka informācijas konfidencialitāte, integritāte un tās pieejamība, tad veicot informācijas klasifikāciju visa organizācijas rīcībā esošā informācija ir jāvērtē saskaņā ar šīm trim skalām.

- Konfidencialitātes līmeni (K) nosaka atkarībā no tā, kādi zaudējumi organizācijai var rasties informācijas nesankcionētas izmantošanas gadījumā;
- Vērtības līmeni (V) nosaka atkarībā no tā, kādi zaudējumi organizācijas var rasties, ja tās darbiniekiem nav pieejama pilnīga, precīza un atbilstoša informācija, t.i. nav nodrošināta integritāte;
- Pieejamības līmeni (P) nosaka atkarībā no tā, kādi zaudējumi organizācijai var rasties, ja tās darbiniekiem nav pieejama nepieciešamā informācija vai pakalpojums noteiktā vietā un laikā.

Katrai no vērtēšanas skalām ir jānosaka līmeņi un jāizvēlas atbilstoši apzīmējumi, piemēram, klasificējot informāciju pēc konfidencialitātes, var tikt lietoti 2 līmeņi ar attiecīgiem apzīmējumiem:

K1 – Ierobežotas pieejamības informācija;

K2 – Vispārpieejama informācija.

Konfidencialitātes līmeņi ņemti no „Informācijas atklātības likuma”.

Klasificējot informāciju pēc tās vērtības līmeņa, var tikt lietotas 3 kategorijas:

V1 – Augsta riska informācija;

V2 – Vidēja riska informācija;

V3 – Zema riska informācija.

Klasificējot informāciju pēc tās pieejamības līmeņa, var tikt lietotas 3 kategorijas:

P1 – Informācija ir pieejama 24 stundas diennaktī, 7 dienas nedēļā, ne vēlāk kā 2 stundu laikā;

P2 – Informācija ir pieejama organizācijas darba laikā, ne vēlāk kā 8 stundu laikā;

P3 – Informācija ir pieejama organizācijas darba laikā, ne vēlāk kā 2 dienu laikā;

<u>Svarīgi atcerēties!</u>
Veicot klasifikāciju nav vēlams izmantot vairāk kā piecus dažādus līmeņus, jo tad ir sarežģīti noteikt precīzus vērtējuma kritērijus katram līmenim.
Informācijas konfidencialitātes līmeni var noteikt kā primāru vai svarīgāku par pārējiem vērtēšanas kritērijiem, piemēram -, piešķirot informācijas resursiem augstāko konfidenciālas informācijas kategoriju (K1), pēc vērtības tie arī ir jāklasificē kā augsta riska informācijas resursi (V1).

<u>Informācijas resursu klasifikācijas anketa un saraksts</u>
Praktiski informācijas resursa klasifikāciju veic aizpildot klasifikācijas anketu. Klasifikācijas anketa tiek izstrādāta saskaņā ar klasifikācijas noteikumiem un tajā tiek

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas” informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā”

fiksēti klasifikācijas rezultāti, kurus apstiprina attiecīgā resursa turētājs (*skatīt Pielikumu Nr.2*).

Lai process būtu objektīvāks, klasifikāciju var veikt grupā, kurā ir iesaistīts IS drošības pārvaldnieks un arī IS uzturētāji. Tomēr, gala lēmums par informācijas klasifikācijas līmeni ir jāpieņem informācijas resursu turētājam, kas rakstiski apstiprina resursa klasifikāciju.

Datus no dažādām klasifikācijas anketām IS drošības pārvaldnieks apkopo vienotā klasifikācijas sarakstā. Informācijas resursu saraksts ir tabula, kurā uzskaitītas visas organizācijā esošās IS un to sastāvā esošie informācijas resursi. Katram informācijas resursam ir norādīts resursa turētājs un aizbildnis, kā arī fiksēti resursa klasifikācijas rezultāti.

Informācijas resurss	Konfidenci-alitāte	Vērtība	Pieejamība	Resursa turētājs
Grāmatvedības uzskaites sistēma	K1	V1	P1, nepārtraukti, maks. dīkstāve 2 h	galvenā grāmatvede
Līgumu datu bāze	K1	V2	P3, darba laikā, maks. dīkstāve 48 h	juridiskās daļas vadītājs
Vērtspapīru uzskaites programma	K1	V2	P3, darba laikā, maks. dīkstāve 48 h	klientu daļas vadītājs
Interneta mājas lapa	K2	V2	P2, nepārtraukti, maks. dīkstāve 8 h	marketinga daļas vadītājs

4. tabula. Informācijas klasifikācijas saraksts

Klasifikācijas uzturēšana un aktualizācija

IR turētājam ir pienākums ne retāk kā reizi gadā veikt sev atbildībā esošu IR klasifikācijas pārskatīšanu. Ja informācijas resursa klasifikācija ir veikta vairāk nekā pirms gada, tad IS drošības pārvaldnieks rakstiskā veidā sagatavo un nosūta IR turētājam priekšlikumu veikt attiecīgā IR klasifikācijas pārskatīšanu. Jaunu sistēmu izstrādes gadījumā projekta vadītājs ir atbildīgs, lai, uzsākot IS izstrādes vai iegādes un ieviešanas projektu, attiecīgā IS tiktu iekļauta IR sarakstā.

Svarīgi atcerēties!
Organizācija savos normatīvos balstoties uz risku analīzi nosaka arī klasificētas informācijas lietošanas noteikumus, kā arī obligātās fiziskās un loģiskās aizsardzības prasības, kuras tiek piemērotas atbilstoši informācijas klasifikācijas līmenim.

Nākamais IS drošības pārvaldības solis pēc resursu klasifikācijas ir risku analīze, kura palīdz identificēt un novērtēt iespējamos riskus, kuriem ir pakļauti organizācijas resursi un piemērot tiem atbilstošus drošības pasākumus.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

- <u>Pielikums.</u> *Informācijas klasificēšanas noteikumu paraugu skatīt pielikumā Nr.2.*

4. Informācijas sistēmu drošības risku pārvaldība

Risku pārvaldība jeb vadība ir viens no IT drošības un arī biznesa plānošanas pamatelementiem. Risku pārvaldība organizācijai ļauj apzināt tās pašreizējo situāciju un plānot tās attīstību. Katrai organizācijai ir mērķi, kurus tā vēlas sasniegt. Lai īstenotu mērķus, tiek noteikti uzdevumi, kuru veikšanai ir nepieciešami resursi. Neatkarīgi no organizācijas vadības gribas, pastāv ārējie un iekšējie draudi. Lai samazinātu draudu iespējas tiek izmantoti aizsardzības jeb drošības līdzekļi, bet, tā kā simtprocentīgi drošu sistēmu nav, ir iespējami arī zaudējumi. Minētā procesa analīze, vērtējot konkrētus jūsu organizācijas mērķus, uzdevumus, resursus, nepilnības, draudus, aizsardzības līdzekļus, potenciālos zaudējumus arī ir IS risku analīze.

Risku analīzes mērķis ir identificēt un novērtēt riskus, kuriem ir pakļautas sistēmas un to resursi, lai noteiktu un izvēlētos atbilstošus un pamatotus drošības pasākumus.

IS risku analīze ietver risku identificēšanu, to novērtēšanu un samazināšanu līdz pieņemamam līmenim.

Informāciju sistēmu risku analīze ir vadības rīks, lai novērtētu IS drošību un pamatotu nepieciešamos IS drošības pasākumus un izmaksas.

Ar ko sākt?

Drošības pārvaldniekam kopā ar organizācijas vadību ir jāizveido IS risku analīzes noteikumi, kuros būtu definēta kārtība kas un kādā veidā organizācijā veic risku analīzi, kas apstiprina rezultātus. Jānosaka prasības kādām sistēmām tiek veikta kārtējā risku analīze (visām projekta stadijā esošām IS un pārējām IS vismaz reizi gadā) un kritēriji ārkārtas risku analīzes veikšanai. Jānosaka tālākās darbības pēc risku analīzes.

Nākamais posms ir atbilstošas risku analīzes metodikas izvēle.

IS drošības risku analīzes procesā iesaistītās un atbildīgās personas skatīt 5.tabulā.

Process	**Procesa virzītājs**	**Procesa izpildītājs**	**Sasniedzamais rezultāts**	**Dokumenta izstrādātājs**	**Dokumentu apstiprina**
IS drošības risku analīzes veikšana	Drošības pārvaldnieks	IR un TR turētāji sadarbībā ar drošības pārvaldnieku	Veiktas IS risku analīzes, noteikti drošības pasākumi	Drošības pārvaldnieks	IR turētājs vai organizācijas vadība

5.tabula. tabula. IS drošības risku analīzes procesā iesaistītās un atbildīgās personas

Kādi ir ieguvumi no risku analīzes?

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

Pirmais lielākais ieguvums organizācijai no IS risku analīzes procesa ir pareiza atbildības sadalīšana. Parasti organizācijā par IS drošību atbild IS daļa un organizācijas vadība tikai piešķir vai nepiešķir līdzekļus konkrētam tehniskam risinājumam. Veicot IS risku analīzi, vadība, akceptējot riska analīzes rezultātus, uzņemas arī atbildību par esošās sistēmas stāvokli, savukārt, noraidot konkrēta drošības risinājuma finansēšanu, vadība ir informēta par risku, ko tā uzņemas. Risku analīze nodrošina, ka organizācijā tiek ieviesti un uzturēti tikai nepieciešamie drošības pasākumi.

Otrs nozīmīgs ieguvums no IS risku analīzes attiecināms uz IT darbiniekiem. Veicot riska analīzi un iegūstot IS resursu novērtējumu, kā arī drošības līdzekļu finansiālo pamatojumu, IT darbiniekiem rodas iespējas savlaicīgi plānot savas darbības un attīstību. IS risku analīze sniedz atbildes uz jautājumiem – kāds drošības risinājums nodrošina maksimāli labāko efektu, kādā secībā ieviest drošības risinājumus utt.

Riska analīze nav brīnumlīdzeklis, kas atrisinās organizācijas IS drošības problēmas, taču tā ļauj aptvert esošo situāciju organizācijā.

Svarīgi atcerēties!
Risks ir tieši proporcionāls nevēlamā notikuma **ietekmei** uz organizāciju un šādu negadījumu **iespējamībai** vai arī citiem vārdiem tas ir tieši atkarīgs no apdraudējuma varbūtības un ietekmes.

Risks = ietekme x iespējamība

4.1 IS risku analīzes metodika

Veicot risku analīzi liela nozīme ir darbinieku pieredzei, intuīcijai un prognozēšanas spējai. Tomēr, lai analīzes process būtu sistemātisks un tās rezultāti būtu salīdzināmi un atkārtojami ir jāizmanto organizācijai piemērota un procesa dalībniekiem izprotama IS risku analīzes metode/metodika. Izvēlētā metodika ir jādokumentē un jāveic darbinieku apmācība tās izmantošanā.

Ir daudz dažādu riska analīzes metodiku – gan kvalitatīvu, kas paredz sistēmu novērtēšanu vārdiski (sistēmas ir vidēji drošas, drošas, nedrošas, un zaudējumi – lieli, vidēji, niecīgi), gan kvantitatīvu, kuras izmantojot zaudējumus un risku jau novērtē skaitliski (latos, punktos, procentos). Piemēram, populārākās ir šādas metodikas[1] - ENISA, CRAMM, Ebios, ISF metodes: IRAM (*Information Risk Analysis Methodologies*) un SPRINT (*Simplified Process for Risk Identification*), kas pieejamas ISF biedriem.

Aplūkosim *kvalitatīvo* IS riska analīzes metodiku.
Kvalitatīvo metodiku var izmantot, ja organizācija ir ar pārskatāmu resursu daudzumu un tās speciālisti ir pietiekami kvalificēti, lai spētu novērtēt apskatāmo sistēmu.

[1] 10.nodaļā ir atrodamas Internet saites uz risku analīzes metodiku mājas lapām
Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

1) Pirmais solis ir novērtēt cik lielā mērā analizējamā IS var ietekmēt organizācijas darbību – tās mērķus un procesus. Novērtējumam ir jāizmanto dati no konkrētās IS informācijas resursu klasifikācijas.
2) Tālākais solis, kuru var atzīmēt kā svarīgāko procesā, ir identificēt iespējamos IS apdraudējumus.

Viens no variantiem ir izmantot apdraudējumu novērtējuma tabulu, (skatīt 6. tabulu). apdraudējumi ir sadalīti četrās grupās:

- dabas spēki (plūdi, vētra, zibens);
- kļūdas vai netīšas cilvēku darbības;
- tīšas cilvēku nesankcionētas darbības;
- iekārtu/programmatūras/līniju/servisa atteice (iekārtas avārija, ilglaicīgs elektrības pārāvums).

Apdraudējumi	**Sistēmai atbilst** (jā/nē)	**Iespējamība** 1 = zema 2 = vidēja 3 = augsta	**Ietekme** 1 = zema 2 = vidēja 3 = augsta	**Riska līmenis**	**Prioritāte**
Dabas spēki					
Sniega vētra					
…					
Cilvēku radīti apdraudējumi (netīši)					
Ugunsgrēks (iekšējs, neliels)					
...					
Cilvēku radīti (netīši)					
Viltošana, krāpšana					
Ļaunprātīga izmantošana (iekšēja)					
...					
Vides apdraudējumi					
Strāvas pārrāvumi					
...					

6. tabula. Apdraudējumu iespējamības un ietekmes novērtējums un riska aprēķins

Otrs veids kā identificēt IS apdraudējums ir intervēt atbildīgos darbiniekus un procesu dokumentēt. Lai intervijas strukturētu, iespējamos apdraudējumus var sadalīt tīšos un netīšos un vērtēt to ietekmi uz konkrētās IS integritāti, konfidencialitāti un pieejamību (skatīt 7. tabulu).

	integritāte	**konfidencialitāte**	**pieejamība**	
Netīši/Nejauši	- kļūdains vai atkārtots datu ievads - ievadlauku modifikācija	- nepārtraukt sesiju pēc darbā beigšanas - nenobloķēt darbstaciju - nosūtīt e-pastu citai personai - izdrukāt uz cita printera	- nejauši sabojāt datu nesēju - plūdi, ugunsgrēks - telekomunikāciju pārrāvums	Neparedzēts notikums (kļūda, nolaidība)

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

Tīši	- kļūdainu pārskatu sagatavošana - datu labošana	- piekļūt datiem bez autorizācijas; - neatļauti izpaust datus -nokopēt bez atļaujas	- datu iznīcināšana - DoS uzbrukums -sabotāža, terorisms	Neautorizēts notikums (krāpšana, ļaunprātīga izmantošana)
	Informācijas modificēšana, sabojāšana	*Informācijas izpaušana*	*Informācijas vai pakalpojumu nepieejamība*	

7. tabula. Apdraudējumu identificēšana

3) Nākamais solis ir novērtēt identificēto apdraudējumu ietekmi un iespējamību. Vērtēšanai var tikt pielietota skala no 1 līdz 3. Var izmantot arī citu skalu, piemēram četru, piecu vai desmit līmeņu skalu. Risku iegūst, sareizinot apdraudējuma ietekmi ar tā iestāšanās varbūtību (skatīt 6. tabulas priekšpēdējo kolonu).

4) Pēc risku aprēķina ir jāpieņem lēmums kādas darbības ir jāveic tālāk. Iespējamās stratēģijas var būt sekojošas:

- piemērot atbilstošus drošības pasākumus, lai samazinātu risku;
- apzināti un objektīvi pieņemt risku, pārliecinoties ka lēmums saskan ar organizācijas drošības politiku un riska akceptēšanas kritērijiem;
- izvairīties no riska, vispār neatļaujot darbības, kuras var izraisīt risku;
- novirzīt riskus citai organizācijai (apdrošinātājam, ārpakalpojuma sniedzējam).

Lēmuma pieņemšanai var izmantot risku pārvaldības matricu (skatīt 8. tabulu).

		Resursu ietekme uz organizāciju		
Nepilnības	*Augstas-3*	**3**	**6**	**9**
	Vidējas-2	**2**	**4**	**6**
	Zemas-1	**1**	**2**	**3**
		Zema-1	*Vidēja-2*	*Augsta-3*

8. tabula. Risku pārvaldības matrica

9 - drošības pasākumi ir jāpiemēro nekavējoties;
6 – ievērojams risks, drošības pasākumus ieteicams piemērot;
2 un 3 - pieņemams risks, nepieciešams sekot līdzi attīstībai;
1 – nenozīmīgs risks.

Katra konstatētā riska mazināšanai ir jāpiedāvā ieviest gan tehniskos, gan administratīvos drošības līdzekļus. Drošības pasākumus var arī klasificēt pēc to darbības veida:

- samazina apdraudējumu iespējamību;
- samazina apdraudējumu ietekmi;
- brīdina *(detect)* par apdraudējuma īstenošanos;
- palīdz atjaunot *(recover)* sistēmas darbību pēc incidenta.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

Novērtējot drošības pasākumus ir jāizvēlas efektīvākie drošības pasākumi - tie, kuri var kontrolēt lielāku skaitu apdraudējumu.

Pēc drošības pasākumu noteikšanas atlikušam riskam ir jābūt pieņemamam resursu turētājiem.

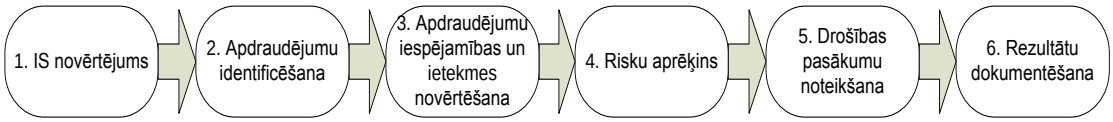
5) Risku analīzes rezultāti tiek noformēti rakstiski, aizpildot IS riska analīzes kopsavilkumu (*skatīt Pielikumā Nr.3*). IS riska analīzes kopsavilkumu paraksta IR turētājs, tādējādi apstiprinot atlikušos riskus un ieviešamo drošības līdzekļu termiņu plānu. IS riska analīzēs noteiktos drošības pasākumus apkopo kopējā organizācijas IS drošības risku pārvaldības plānā (*skatīt 5.nodaļu*), kuru iesniedz organizācijas vadībai apstiprināšanai.

Lai šādu metodiku varētu lietot, lēmuma pieņēmējam ir jābūt pietiekamai pieredzei IS drošības jomā un labi jāpazīst sistēma, lai varētu to pareizi novērtēt.

Bāzes metodikas rezultāti var kalpot arī par ieejas datiem detalizētākām risku analīzes metodēm vai tehniskām IS drošības pārbaudēm, kuras nepieciešamības gadījumā var tikt pielietotas padziļinātai sistēmas drošības risku novērtēšanai.

4.2 IS risku analīzes procesa piemērs

Tālāk, kā piemēru apskatīsim vienkāršu risku analīzes procesu, kurā visu analīzes procesu nosacīti var sadalīt sešos etapos vai soļos (skatīt 6.attēlu):



6. attēls. IS risku analīzes process

Solis 1: IS novērtējums;
Solis 2: Apdraudējumu identificēšana;
Solis 3; Apdraudējumu iespējamības un ietekmes novērtēšana;
Solis 4: Risku aprēķins;
Solis 5: Drošības pasākumu noteikšana;
Solis 6: Rezultātu dokumentēšana.

Solis 1: IS novērtējums.
Lai veiksmīgi īstenotu risku analīzi ir jābūt skaidrai izpratnei, kas tiks analizēts un kāda ir sistēmas ietekme uz organizācijas darbību. Jādod atbilde, kā tā tiešā vai netiešā veidā ir nepieciešama organizācijas mērķu izpildei, kāda ir tās loma būtiskos procesos, vai tā apstrādā organizācijai kritisku vai konfidenciālu informāciju. Lai vērtētu sistēmas ietekmi uz organizācijas darbību ir jāizmanto dati no informācijas klasifikācijas saraksta, kurā ir vērtēta sistēmas informācijas konfidencialitāte, integritāte un pieejamība (*skatīt Pielikumu Nr.2*).

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

Solis 2: Apdraudējumu identificēšana.
Šajā posmā identificē konkrētus sistēmas apdraudējumus. Identificējot apdraudējumus vēlams iekļaut sarakstā tos, kuri var radīt vislielāko ietekmi uz sistēmu. Jānorāda kādā veidā sistēma tiks ietekmēta, kāda tieši būs ietekme, kas to uzsāks (darbinieks, neautorizēta persona, dabas spēki, tehnoloģiska kļūme vai citi cēloņi). Apdraudējuma aprakstam ir jābūt īsam, bet konkrētam. Jāatceras, ka apdraudējumu iespējamību nosaka sistēmas ievainojamības.

Solis 3: Apdraudējumu iespējamības un ietekmes novērtēšana.
Kad apdraudējumu tabula ir izveidota un komanda piekrīt katrai apdraudējuma definīcijai, tad ir laiks novērtēt to iespējamību un ietekmi. Ja izmanto trīs līmeņu skalu tad, konkrēto apdraudējumu iespējamību vai ietekmi var noteikt kā zemu, vidēju vai augstu vai apzīmēt to ar skaitļiem no 1 līdz 3. Vērtējumus ierakstiet tabulā, kuru kā piemēru minējām apskatot risku analīzes metodes (skatīt 9. tabulu).

Apdraudējumi	**Iespējamība** 1 = zema 2 = vidēja 3 = augsta	**Ietekme** 1 = zema 2 = vidēja 3 = augsta	**Risks**	**Prioritāte**
…				
…				

9. tabula. Apdraudējumu iespējamības un ietekmes novērtējums un riska aprēķins

Solis 4: Risku aprēķins.
Kad ir veikts apdraudējumu iespējamības un ietekmes novērtējums, tad izmantojot iegūtos datus veic riska aprēķinu. Drošības risks ir tieši proporcionāls iespējamā apdraudējuma varbūtībai un ietekmei (risks = ietekme x iespējamība). Tātad, sareiziniet ietekmi un varbūtību un ierakstiet skaitli riska kolonnā. Kolonnā prioritāte ierakstiet 1 pretim riskam ar lielāko vērtību un secīgi atbilstošas prioritātes zemākiem riskiem.

Solis 5: Drošības pasākumu noteikšana.
Katras risku analīzes svarīgs posms ir drošības pasākumu izvēle, kas samazinātu draudu ietekmi vai sistēmas ievainojamību. Drošības pasākumu noteikšana ir jāsāk riskiem ar augstāko prioritāti. Izvēloties drošības pasākumus ir jāievēro samērīguma princips, t.i. potenciālai ietekmei ir jābūt lielākai par paredzētajām pasākuma izmaksām, ņemot vērā arī riska varbūtību. Katram drošības pasākumam jānosaka atbildīgais par pasākumu īstenošanu un to plānotais termiņš. Pēc drošības pasākumu noteikšanas atlikušam riskam ir jābūt pieņemamam resursu turētājam.

Solis 6: Rezultātu dokumentēšana.
Riska analīzes veicējiem rezultāti ir jāapkopo protokolā vai IS riska analīzes kopsavilkumā (*skatīt Pielikumā Nr.3*).
Savukārt, atsevišķās IS riska analīzēs noteiktos drošības pasākumus apkopo kopējā organizācijas IS drošības risku pārvaldības plānā. Plānā pasākumi tiek sakārtoti

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

prioritāšu secībā. Priekšroka tiek dota īsākā laikā īstenojamiem pasākumiem, kas var būtiski samazināt risku pēc iespējas lielākam būtisko informācijas sistēmu skaitam.

Normatīvo aktu prasības

Atbilstoši Noteikumiem sistēmas drošības risku analīzei ir jāsatur vismaz sekojošas sadaļas:

1. sistēmas drošības apdraudējumu uzskaitījumu, to īstenošanās varbūtības novērtējumu un tuvošanās pazīmju uzskaitījumu;
2. sistēmas drošības riska novērtējumu;
3. sistēmas drošības riska mazināšanas pasākumu un tajos izmantojamo līdzekļu uzskaitījumu;
4. sistēmas pārziņa, sistēmas datu subjektu un sistēmas lietotāju iespējamo zaudējumu vai kaitējuma novērtējumu, ja notiktu sistēmas drošības incidents;
5. sistēmas drošības riska mazināšanai veikto pasākumu lietderības novērtējumu.

- *Pielikums. Informācijas sistēmu riska analīzes noteikumu dokumenta paraugu skatīt pielikumos Nr.3.*

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

5. Sistēmas drošības risku pārvaldības plāna izstrādāšana un izpilde

Risku pārvaldības gaitā organizācijai ir jāpieņem lēmums kā tā plānveidīgi aizsargāsies pret iespējamām risku sekām, kādā veidā šie aizsardzības pasākumi tiks īstenoti un kuras ir atbildīgās personas.

Lai mērķtiecīgi un sistemātiski īstenotu izvēlētos apdraudējumu novēršanas pasākumus risku analīzes rezultātus ir nepieciešams apkopot darbību koordinējošā dokumentā vai IS drošības plānā. Plānam ir jānodrošina, ka aizsargpasākumi tiek īstenoti savlaicīgi un atbilstoši prioritātēm, kas izriet no IS riskiem. Plānam ir jābūt labi strukturētam un vadības apstiprinātam.

Ar ko sākt?
Riska analīzes veicējiem darba rezultāti rakstiski jānoformē saskaņā ar izvēlēto IS riska analīzes metodoloģiju. Tādejādi, risku analīzes rezultāti sniedz organizācijas vadībai informāciju par darbībām, kuras ir plānots veikt, lai samazinātu identificētos riskus konkrētām sistēmām. Visi risku analīzēs noteiktie obligāti ieviešamie drošības pasākumi ir jāapkopo vienotā dokumentā, kas arī veido kopējo organizācijas IS drošības riska pārvaldības plānu.

IS drošības riska pārvaldības plāna izstrādāšanas procesā iesaistītās un atbildīgās personas skatīt 10.tabulā.

Process	**Procesa virzītājs**	**Procesa izpildītājs**	**Sasniedzamais rezultāts**	**Dokumenta izstrādātājs**	**Dokumentu apstiprina**
IS riska pārvaldības plāna sagatavošana	Drošības pārvaldnieks	Drošības pārvaldnieks	Sastādīts IS drošības riska pārvaldības plāns	Drošības pārvaldnieks	Organizācijas vadība

10. tabula. IS drošības riska pārvaldības plāna izstrādāšanas procesā iesaistītās un atbildīgās personas

IS drošības riska pārvaldības plāns ietver (*skatīt 11.tabulu*):

1. drošības apdraudējumu uzskaitījumu;
2. pasākumus drošības riska mazināšanai, to izpildes termiņus (īsā, vidējā un ilgā laika posmā plānotās darbības), finansējumu vai izmaksas un par izpildi atbildīgo personu sarakstu.

Informācijas sistēma	Apdraudējumi	Drošības pasākumi	Izpildes termiņi	Izmaksas	Atbildīgā persona

11. tabula. IS drošības plāna paraugs

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

Organizācijai jāparedz noteikto pasākumu pārbaudes un izmaiņu procedūra. Drošības plānu aktualizē, pamatojoties uz atkārtotu IS drošības risku analīzi.

Plāna izpildi kontrolē IS drošības pārvaldnieks!

Svarīgi atcerēties!
Organizācija var veidot arī katrai kritiskai sistēmai savu IS drošības risku pārvaldības plānu. Tādā gadījumā dokumentā attiecībā uz katru sistēmu ir jāietver šādi jautājumi:

1. drošības mērķi attiecībā uz konfidencialitāti, integritāti un pieejamību;
2. riska analīzes pieeja šai sistēmai;
3. plānoto aizsargpasākumu saraksts ietverot prioritātes izvēlēto aizsargpasākumu īstenošanai un esošo aizsargpasākumu uzlabošanai un veids kā šie pasākumi darbosies praksē,
4. noteikto aizsargpasākumu ieviešanas un ekspluatācijas izmaksu aprēķins;
5. noteikto aizsargpasākumu ieviešanas un paveiktā darba kontrolei nepieciešamo cilvēku resursu aprēķins;
6. detalizēts īstenošanas darba plāns ietverot prioritātes, grafiku, budžetu, pienākumus, izpildes kritērijus un to kontroli.

Normatīvo aktu prasības
Atbilstoši Noteikumiem, sistēmas drošības riska pārvaldības plānam ir jāsatur vismaz sekojošas sadaļas:

1. sistēmas drošības apdraudējumu uzskaitījumu un sistēmas drošības riska izvērtējumu;
2. pasākumus sistēmas drošības riska mazināšanai, to izpildes termiņus, finansējumu un par izpildi atbildīgo personu sarakstu.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

6. Iekšējo informācijas sistēmu drošības noteikumu izstrāde un ievērošana

Lai aizsargātu organizācijas pārvaldībā esošās informācijas sistēmas ir jāizstrādā iekšējie informācijas sistēmu drošības noteikumi, nosakot pasākumus drošības risku mazināšanai.

Iekšējo informācijas sistēmu drošības noteikumu mērķis ir nodefinēt organizācijas informācijas sistēmu fiziskās un loģiskās aizsardzības, informācijas uzglabāšanas un pieejamības prasības, lai izvairītos no nevēlamiem apkārtējās vides, tehniskajiem un cilvēkfaktoriem.

Ar ko sākt?
IS drošības noteikumu izstrādi parasti veic drošības pārvaldnieks sadarbojoties ar tehnoloģisko resursu turētājiem, bet atsevišķu prasību definēšanā piesaistot arī informācijas resursu turētājus.

Iekšējo IS drošības noteikumu izstrādes procesā iesaistītās un atbildīgās personas skatīt 12.tabulā.

Process	**Procesa virzītājs**	**Procesa izpildītājs**	**Sasniedzamais rezultāts**	**Dokumenta izstrādātājs**	**Dokumentu apstiprina**
Iekšējo IS drošības noteikumu izstrāde	Drošības pārvaldnieks	Drošības pārvaldnieks sadarbībā ar IR un TR turētājiem	Izstrādāti iekšējie IS drošības noteikumi	Drošības pārvaldnieks	Organizācijas vadība

12. tabula Iekšējo IS drošības noteikumu izstrādes procesā iesaistītās un atbildīgās personas

Drošības pārvaldniekam ir jāatbild uz sekojošiem jautājumiem:

1. Kur ir izvietotas organizācijas IS un kā tiek nodrošināta to fiziskā aizsardzība - ugunsgrēks, plūdi, temperatūras svārstības, neatbilstoša elektro-padeve, elektromagnētiskā lauka iedarbība, tehnikas zādzība, pakalpojumu sniedzēju piekļuve datu centram u.c.?
2. Kā tiek nodrošināta IS loģiskā aizsardzība - lietotāju piekļuves kontrole, administratoru un ārpakalpojumu sniedzēju piekļuve, pretvīrusu aizsardzība, „ielaušanās no Interneta" mēģinājumu kontrole?
3. Kā un kādā veidā uzrauga informācijas sistēmu drošību?
4. Kā un kādā veidā tiek veikta incidentu pārvaldība (definē informācijas drošības incidentu, nosaka kam ir jāziņo par drošības incidentiem, nosaka atbildīgos par reakcijas darbību veikšanu, kārtību kādā tiek analizētas incidentu sekas un cēloņi, kārtību kādā nepieciešamības gadījumā tiek vākti pierādījumi)?
5. Kādā veidā tiek nodrošināta datu nesēju fiziskā un loģiskā aizsardzība?
6. Kādā veidā tiek nodrošināta antivīrusu aizsardzība?

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

7. Kādā veidā tiek veikta liekpasta (*spam*) un interneta izmantošanas kontrole?
8. Kādā veidā tiek veikta bezvadu iekārtu izmantošanas kontrole?
9. Kādas procedūras ir noteiktas rezerves kopiju izgatavošanai un informācijas atjaunošanai no tām – kāda informācija, informācijas sistēma, cik bieži tiek kopēta, kur tiek uzglabātas kopijas, cik bieži tiek veikta kopiju un atjaunošanas procedūru testēšana, vai informācija tiek šifrēta?
10. Cik senu vai jaunu informāciju varēs atjaunot no rezerves kopijām?
11. Kāds drošības līmenis tiek noteikts, informācijas sistēmu izstrādi un uzturēšanu uzticot ārējam pakalpojumu sniedzējam?
12. Kādas ir prasības organizācijai veicot jaunu informācijas sistēmu izstrādi, iegādi, ieviešanu un izmaiņu pārvaldīšanas procesu?
13. Kā un cik bieži organizācijas darbinieki tiek informēti vai apmācīti par drošības jautājumiem?

Ārpakalpojumu sniedzējiem, kuri veic organizācijas informācijas sistēmu izstrādi un uzturēšanu, drošības līmenim ir jābūt noteiktam ne zemākam par organizācijas iekšējos IS drošības noteikumos definēto. Noteiktajām drošības prasībām ir jābūt iekļautām sadarbības līgumos.

<u>Svarīgi atcerēties!</u>
Darbinieki tiek iepazīstināti ar iekšējiem IS drošības noteikumiem stājoties darbā. Par katrām izmaiņām IS drošības noteikumos, darbinieki ir regulāri jāinformē.

<u>Normatīvo aktu prasības</u>
Atbilstoši Noteikumiem, iekšējiem IS drošības noteikumiem ir jāsatur vismaz sekojošas sadaļas:

1. sistēmas informācijas resursu izveidošanas, papildināšanas, mainīšanas, apstrādes, pārraidīšanas, glabāšanas, atjaunošanas un iznīcināšanas kārtību;
2. sistēmas informācijas un tehnisko resursu lietošanas un tās kontroles kārtību;
3. kārtību, kādā tiek nodrošināta piekļūšana sistēmas informācijas un tehniskajiem resursiem;
4. sistēmas informācijas resursu rezerves kopiju izgatavošanas un glabāšanas kārtību, kā arī kārtību, kādā pārbauda, vai ar sistēmas informācijas resursu rezerves kopijām iespējams atjaunot sistēmas informācijas resursus;
5. datu nesēju lietošanas, pārvietošanas, glabāšanas un iznīcināšanas kārtību;
6. kārtību, kādā lieto un glabā informāciju vai datus, kas nepieciešami, lai piekļūtu sistēmas informācijas un tehniskajiem resursiem;
7. prasības sistēmas informācijas resursu aizsardzībai, kuru īsteno, izmantojot programmatūras līdzekļus (piemēram, sistēmas lietotāja atpazīšana un viņa pilnvaru atbilstības pārbaude attiecīgajām darbībām sistēmā, pasargājot sistēmas informācijas resursus no tīšas vai nejaušas bojāšanas vai iznīcināšanas);
8. prasības sistēmas tehnisko resursu aizsardzībai pret fiziskas iedarbības radītu sistēmas drošības apdraudējumu (piemēram, ugunsgrēks, plūdi, sprieguma pazemināšanās vai pārspriegums enerģijas pievades tīklā, sistēmas tehnisko resursu zādzība, gaisa mitrums vai temperatūra, kas neatbilst ekspluatācijas noteikumiem);

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

9. kārtību, kādā novēro sistēmas drošības apdraudējuma tuvošanās pazīmes;
10. kārtību, kādā atklāj un pārvalda sistēmas drošības incidentus;
11. kārtību, kādā sistēma darbojas, ja tās informācijas vai tehniskie resursi nav pieejami pilnā apjomā;
12. kārtību, kādā maina sistēmas tehniskos resursus;
13. sistēmas pārziņa darbinieku apmācības un zināšanu pārbaudes kārtību sistēmas drošības jomā.

- <u>Pielikums.</u> *Iekšējo IS drošības noteikumu dokumenta paraugu skatīt pielikumā Nr.4.*

7. Informācijas sistēmu lietošanas noteikumu izstrāde un ievērošana

Lai organizētu informācijas sistēmu lietotāju drošu darbu ar informācijas sistēmām, organizācijai ir jāizstrādā informācijas sistēmu lietošanas noteikumi.

Informācijas sistēmu lietošanas noteikumu mērķis ir nodefinēt kārtību, kādā organizācijas IS lietotāji tiek reģistrēti un atcelti, kādas ir to tiesības un pienākumi, lietojot informācijas sistēmas.

Ar ko sākt?
Lai izstrādātu IS lietošanas noteikumus, par pamatu tiek ņemta resursu klasificēšanas laikā iegūtā informācija (skatīt nodaļu *3. Informācijas klasificēšanas noteikumu izstrāde un ievērošana*) . Balstoties uz šo informāciju tiek apzinātas visas informācijas sistēmas un pastāvošā lietotāju reģistrācijas un atcelšanas kārtību. Šis brīdis ir atbilstošs, lai maksimāli unificēt lietotāju reģistrācijas procesus un optimizētu procesā iesaistīto personu darbības.

IS lietošanas noteikumu izstrādes procesā iesaistītās un atbildīgās personas skatīt 13.tabulā.

Process	**Procesa virzītājs**	**Procesa izpildītājs**	**Sasniedzamais rezultāts**	**Dokumenta izstrādātājs**	**Dokumentu apstiprina**
IS lietošanas noteikumu izstrāde	Drošības pārvaldnieks	Drošības pārvaldnieks sadarbībā ar IR un TR turētājiem	Izstrādāti IS lietošanas noteikumi	Drošības pārvaldnieks	Organizācijas vadība

13. tabula. IS lietošanas noteikumu izstrādes procesā iesaistītās un atbildīgās personas

Izstrādājot informācijas sistēmu lietošanas noteikumus, informācijas resursu turētājiem sadarbībā ar drošības pārvaldnieku ir jāatbild uz sekojošiem jautājumiem:

1. Kādā veidā IS lietotājam tiek izveidots, piereģistrēts, atcelts lietotāja vārds? Kurš par to atbild?
2. Kādā veidā ārējiem lietotājiem, ārpakalpojumu sniedzējiem tiek piešķirts izveidots, piereģistrēts, atcelts lietotāja vārds? Kurš par to atbild?
3. Kādas tiesības lietotājam vai grupām var tik noteiktas (piemēram, lasīšanas, rakstīšanas, u.c.)?
4. Kādas prasības ir noteiktas parolei – kādi un cik simboli jāizmanto, cik bieži tā jāmaina?
5. Kādas prasības ir izvirzītas E-pasta un interneta izmantošanai?
6. Kādas prasības ir noteiktas perifēriju iekārtu (USB atmiņas iekārtas, …) izmantošanai un kontrolei?

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

7. Kādā veidā tiek veikta datortehnikas aparatūras un papildus programmatūras izmaiņu pieprasīšana?
8. Kādā veidā tiek veikta datortehnikas bojājumu un programmu traucējumu pieteikšana?
9. Kādā veidā un kam ir jāziņo par drošības incidentiem?
10. Kā tiek organizēta lietotāju apmācība?
11. Kāda disciplinārā atbildība var iestāties, pārkāpjot noteikumus?

Svarīgi atcerēties!
Izstrādājot informācijas sistēmu lietošanas noteikumus, tajos ir jāapskata katras organizācijas pārvaldībā esošas informācijas sistēmas lietošanas organizēšana. Noteikumu normatīvais dokuments var tikt izstrādāts viens (aprakstot visas informācijas sistēmas kopā – ja neatšķiras lietošanas organizēšana) vai vairāki (katrai IS savi lietošanas noteikumi – ja atšķiras lietošanas organizēšana).

Papildus konkrētu informāciju sistēmu lietošanas noteikumiem var tik izstrādāti, piemēram, Interneta izmantošanas noteikumi, elektroniskā pasta izmantošanas noteikumi u.c.

Lietotājam tiek piešķirta piekļuve informācijas sistēmai tikai tad, kad lietotājs ir izlasījis IS lietošanas noteikumus un par to parakstījies. Komplicētākās sistēmās var tikt noteikta prasība, piemēram, pirms piešķirt piekļuvi informācijas sistēmai, lietotājam ir jāiziet noteiktas IS lietošanas apmācības.

Normatīvo aktu prasības
Atbilstoši Noteikumiem, IS lietošanas noteikumiem ir jāsatur vismaz sekojošas sadaļas:

1. IS lietotāju tiesības, pienākumi, ierobežojumi un atbildība
2. IS lietotāju reģistrācija un tās atcelšanas kārtība;
3. IS lietošanas kārtība;
4. IS lietotāju atbalsta kārtība;
5. IS informācijas un tehnisko resursu lietošanas un tās kontroles kārtību;
6. kārtību, kādā tiek nodrošināta piekļūšana sistēmas informācijas un tehniskajiem resursiem.

- *Pielikums. IS lietošanas noteikumu paraugu skatīt pielikumā Nr.5.*

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

8. Informācijas sistēmu darbības nepārtrauktības un atjaunošanas plāna izstrāde un izpilde

IS darbības nepārtrauktība un atjaunošana ir process, kuru ieviešot, var mazināt un paredzēt informācijas sistēmu darbības traucējumu negatīvo ietekmi uz organizācijas darbu, līdz pieņemamam līmenim, kombinējot preventīvus un darbību atjaunojošus tehnoloģiskos un administratīvos mehānismus.

Informācijas sistēmu darbības nepārtrauktības un atjaunošanas plāna mērķis ir definēt kritiskos organizācijas informācijas un tehnoloģiskos resursus, aizsargāt organizācijas biznesa procesus no informācijas sistēmu darbības traucējumu ietekmes un paredzēt secīgu un plānveidīgu rīcību, pārredzamā laika izteiksmē atjaunojot informācijas sistēmu darba spējas.

Ar ko sākt?
Lai izstrādātu IS darbības nepārtrauktības un atjaunošanas plānu, par pamatu tiek ņemta resursu klasificēšanas laikā iegūtā informācija (skatīt nodaļu *3. Informācijas klasificēšanas noteikumu izstrāde un ievērošana*), identificējot organizācijas darbībai kritiskās informācijas sistēmas un vērtējot to ietekmi uz biznesa procesiem.

IS darbības nepārtrauktības un atjaunošanas plāna izstrādes procesā iesaistītās un atbildīgās personas skatīt 14.tabulā.

Process	**Procesa virzītājs**	**Procesa izpildītājs**	**Sasniedzamais rezultāts**	**Dokumenta izstrādātājs**	**Dokumentu apstiprina**
IS darbības nepārtrauktības un atjaunošanas plāna izstrāde	Organizācijas vadība	Drošības pārvaldnieks, IR un TR turētāji	Izstrādāts IS darbības nepārtrauktības un atjaunošanas plāns	Drošības pārvaldnieks	Organizācijas vadība

14. tabula. IS darbības nepārtrauktības un atjaunošanas plāna izstrādes procesā iesaistītās un atbildīgās personas

Pārdomājot IS darbības nepārtrauktību un atjaunošanu, informācijas resursu turētājiem ir jāatbild uz sekojošiem jautājumiem:

1. Kādi riski var ietekmēt organizācijas IS darbības nepārtrauktību (skatīt nodaļu *4. Informācijas sistēmu drošības risku analīze*)?
2. Kādi tehnoloģiskie resursi un informācijas sistēmas ir iesaistītas kritiskos biznesa procesos?
3. Kā drošības incidenti var ietekmēt informācijas sistēmu darbību?

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

4. Kāds ir organizācijai pieļaujamais informācijas sistēmas dīkstāves laiks (no šī jautājuma izsmeļošākas un pārdomātākas atbildes ir atkarīga atbilstoša drošības risinājuma ieviešana)?
5. Kā tiks organizēta darbība drošības incidenta gadījumā – kas ir atbildīgie darbinieki, grupas par konkrētu sistēmu, kādas procedūras ir jāveic, lai atjaunotu informācijas sistēmu darbību, kur atrodas datu rezerves kopijas?
6. Kā tiks organizēta darbinieku apziņošana un atbildīgo personu apmācība IS darbības nepārtrauktības un atjaunošanas jomā?

Svarīgi atcerēties!
IS nepārtrauktības nostādnēm ir jābūt izstrādātām visaptverošām, balstoties uz risku analīzi. Katrai informācijas sistēmai var tikt izstrādāts savs darbības nepārtrauktības un atjaunošanas plāns, pārdomājot katra kritiskā biznesa procesa norisi.
Lai kritiskā brīdī savlaicīgi veiktu IS darbības atjaunošanu ir nepieciešams izstrādāt detalizētas informāciju sistēmu un tehnoloģisko resursu atjaunošanas instrukcijas.

Plānā aprakstītās darbības ir jāpārbauda un jāatjauno reizi gadā vai pie būtiskām informācijas sistēmu darbības un konfigurācijas izmaiņām.

Nododot informācijas sistēmu uzturēšanu ārpakalpojumu sniedzējam, IS darbības nepārtrauktība ir jāpārdomā kontekstā ar visām iesaistītajām pusēm. Informācijas sistēmas darbības nepārtrauktības un atjaunošanas plānošanas iniciators un atbildīgais ir informācijas resursu turētāja organizācija vai pārzinis. Maldīgs ir priekšstats, ka nododot informācijas sistēmu ārpakalpojumu sniedzējam atbildība no organizācijas pleciem ir noņemta.

Normatīvo aktu prasības
Atbilstoši Noteikumiem, IS darbības nepārtrauktības un atjaunošanas plānam ir jāsatur vismaz sekojošas sadaļas:

1. Pasākumus, kas veicami, lai nodrošinātu informācijas sistēmu nepārtrauktu darbību;
2. informācijas un tehnoloģisko resursu atjaunošanas pasākumus prioritārā secībā, kas veicami pēc drošības incidenta;
3. informācijas sistēmu atjaunošanas pasākumu procedūru aprakstu;
4. informācijas sistēmu atjaunošanas pasākumos iesaistīto atbildīgo personu kontaktu informāciju un darbības instrukcijas;
5. atbildīgo personu apmācības, nodarbību un sagatavotības pārbaužu plānu.

- *Pielikums. IS darbības nepārtrauktības un atjaunošanas plāna paraugu skatīt pielikumā Nr.6.*

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

9. Biežāk uzdotie jautājumi

Kas ir risku analīze?
Risku analīze ir process, kura laikā kolektīvi tiek identificēti un novērtēti iespējamie sistēmas apdraudējumi atkarībā no to ietekmes un iespējas īstenoties. Atkarībā no veiktā novērtējuma, komanda izvēlas atbilstošus drošības pasākumus ar mērķi samazināt risku līdz resursa turētājam pieņemamam līmenim. Risku pārvaldības mērķis nav novērst visus iespējamos riskus. Risku analīzi var uzskatīt par metodi ar kuras palīdzību organizācijas vadība var samazināt riskus līdz tai pieņemamam līmenim.

Kāpēc ir jāveic risku analīze?
Organizācijas vadībai pieņemot lēmumus par jauna projekta uzsākšanu, nozīmīgām izmaiņām vai nepieciešamību ieviest kādus drošības pasākumus ir nepieciešams argumentēts un ticams pamatojums to ieviešanai. Dokumentēta risku analīze sniedz šādu pamatojumu.
Otrkārt, efektīvs risku analīzes process nodrošina, ka organizācijā tiek ieviesti un uzturēti tikai nepieciešamie drošības pasākumi. Neviena drošības kontrole nav obligāta. Visu nosaka organizācijas mērķi un uzdevumi. Metodiski un sistemātiski veicot risku pārvaldību organizācija var noteikt optimālās drošības kontroles, kas arī sekmē pašas organizācijas kopējo mērķu sasniegšanu.
Treškārt, risku analīzes rezultāti noder ja ir noticis incidents un tiek vērtēts process par to kā tika pieņemti lēmumi par esošiem drošības pasākumiem.

Kad un kam ir jāveic risku analīze?
Risku analīze ir jāveic katru reizi kad tiek izlietoti organizācijas līdzekļi vai resursi – pirms projekta uzsākšanas, pirms nozīmīgu izmaiņu veikšanas, pirms nozīmīgu pasākumu plānošanas vai pat plāna iespējamības pārbaudes. Risku analīze ir jāveic tiem darbiniekiem, kas vislabāk pārzina konkrēto sistēmu vai procesu, kas pārzina procesa detaļas un ir saskarsmē ar to ikdienā. Risku analīzes procesu vēlams vadīt vai koordinēt darbiniekam, kas, savukārt, vislabāk pārzina organizācijā noteikto risku analīzes metodiku un var efektīvi organizēt analīzes procesu un noformēt tās gala rezultātus. Tāda kompetence ir organizācijas IS drošības pārvaldniekam.

Kas ir riska analīzes rezultāti?
Tipiskie riska analīzes nodevumi ir: identificēti konkrētās sistēmas apdraudējumi, identificētie svarīgākie riski, kuriem ir pakļautas IS un ieteiktie drošības pasākumi, kas samazina riskus līdz pieņemamam līmenim.

Kā mērīt risku analīzes efektivitāti?
Risku analīzes efektivitāti nosaka izvēlēto drošības pasākumu efektivitāte. Organizācijai ir jāspēj novērtēt ieguvumi no investīcijām IS drošībā.
Risku analīzei ir jābūt ātrai un efektīvai. To pamatā nosaka darbinieku iemaņas risku analīzes veikšanā un izvēlētās metodikas atbilstība mērķiem. Tā ir jāveic dažās dienās nevis nedēļām vai mēnešiem ilgi. Process jāorganizē tā lai tas darbiniekiem netraucētu veikt ikdienas pienākumus.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

10. Saites uz Interneta resursiem

1. SIA „Latvijas standarts”:
   www.lvs.lv

2. Starptautiskā standartizācijas organizācija:
   http://www.iso.org/iso/home.htm

3. IT pakalpojumu pārvaldības vadlīnijas ITIL:
   http://www.itil.co.uk

4. IT pārvaldības vadlīnijas CobiT:
   http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/Obtain_COBIT.htm

5. IS drošības pārvaldības resursi – bezmaksas lejupielādējami IS drošības materiāli, dokumenti un 20 kritiskāko tīkla un sistēmu drošības ievainojamību tops:
   http://www.sans.org

6. Neatkarīgais informācijas drošības forums - The information security forum (ISF):
   www.securityforum.org

7. ENISA risku analīzes metodikas apraksts:
   http://www.enisa.europa.eu/rmra/rm_home.html

8. CRAMM risku analīzes metodikas apraksts:
   www.cramm.com

9. Ebios risku analīzes metodikas apraksts:
   www.ssi.gouv.fr

Pielikums Nr.1
IS drošības politikas dokumenta paraugs

IS drošības politika

1. IS drošības politikas mērķi un pamatnostādnes

1.1. Organizācijas informācijas drošības politika (tālāk tekstā – drošības politika) ir izstrādāta un tiek īstenota saskaņā ar Organizācijas darbības mērķiem un uzdevumiem, Latvijas Republikā spēkā esošo likumdošanu, kā arī ņemot vērā starptautisko IS drošības standartu rekomendācijas.

1.2. Drošības politika ir izstrādāta ar mērķi nodrošināt tādu informācijas tehnoloģiju vidi, lai Organizācijas informācijas un tehnoloģiskie resursi būtu aizsargāti pret ārējiem un iekšējiem drošības riskiem un vienlaikus nodrošinātu Organizācijas nepārtrauktu un kvalitatīvu darbību atbilstoši normatīvajos aktos noteiktajām funkcijām.

1.3. Drošības politika nosaka galvenos drošības pamatnosacījumus informācijas tehnoloģiju videi un nosaka kārtību informācijas un tehnoloģisko resursu aizsardzības nodrošināšanai Organizācijā.

1.4. Drošības politika ir saistoša visiem Organizācijas darbiniekiem, kā arī tiem ārpakalpojumu sniedzējiem, kuri Organizācijai sniedz ar IT saistītus pakalpojumus.

1.5. Drošības politika neattiecas uz informācijas sistēmām, kuras nodrošina tādas informācijas apriti, kas ir atdzīta par valsts noslēpuma objektu.

2. Drošības politikas īstenošanas pamatprincipi

2.1. Organizācijā ir noteikts un patstāvīgi tiek pilnveidots dokumentu un pasākumu kopums, kuru īstenošana nodrošina drošības politikas mērķa sasniegšanu.

2.2. Risku ierobežošanas un darbības nepārtrauktības nodrošināšanas izmaksas ir samērojamas ar iespējamiem zaudējumiem, kas varētu rasties šo risku īstenošanās vai Organizācijas darbības pārtraukšanas gadījumos.

2.3. Organizācijā tiek sekmēta katra darbinieka izpratne par pienākumiem risku un darbības nepārtrauktības pārvaldīšanā un informācijas un tehnoloģisko resursu aizsardzības nodrošināšanā, veicot Organizācijas darbinieku regulāru izglītošanu.

2.4. Organizācijā tiek nodrošināta pastāvīga drošības politikas īstenošanas koordinēšana un pārraudzīšana.

2.5. Gadījumos, kad Organizācijas darbinieki neievēro IS drošības politikas izvirzītās prasības, Organizācijas vadība var ierosināt disciplinārās sodīšanas procesu saskaņā ar esošo likumdošanu.

3. Drošības organizācija

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

3.1. Organizācijas vadība. Organizācijas vadība kopumā ir atbildīga par informācijas drošības politikas īstenošanu, t.sk. atbildīga par IT drošības organizācijas izveidi un atbildības noteikšanu, kontroles noteikšanu un adekvātu resursu piešķiršanu IT drošības organizācijas pilnvērtīgai funkcionēšanai.

3.2. Informācijas drošības komiteja. Informācijas drošības vadības direktīvas tiek sniegtas, izmantojot speciāli šim nolūkam izveidotu Informācijas drošības komiteju. Komitejas pienākumos ietilpst informācijas drošības politikas pārbaude un apstiprināšana un vispārīgā atbildība par tās definēšanu un ieviešanu. Papildus tam komiteja pārskata drošības incidentus, par kuriem to informējis Informācijas drošības pārvaldnieks.

3.3. Informācijas drošības pārvaldnieks. Lai nodrošinātu konkrētu drošības pasākumu īstenošanu un koordināciju kopumā, Organizācijas vadītājs nozīmē Informācijas drošības pārvaldnieku, kurš ir tieši pakļauts augstākai vadībai. Informācijas drošības pārvaldnieks atbild par risku analīzes veikšanu, nepieciešamo IS drošības normatīvās bāzes uzturēšanu un īstenošanu, noteikto drošības prasību ievērošanas uzraudzību, IT drošības incidentu izmeklēšanu un darbinieku apmācību informācijas drošības jomā.

3.4. Informācijas lietotājs. Informācijas lietotājs ir atbildīgs par visām darbībām, kuras ir veikts ar viņa lietotāja vārdu un ir pienākums informēt Informācijas drošības pārvaldnieku par visiem IT drošības incidentiem un aizdomīgiem notikumiem.

3.5. IS audits. IS audita uzdevums ir novērtēt drošības prasību izpildi. Nepieciešamības gadījumā, bet ne retāk kā reizi gadā, auditam ir jāveic Organizācijas IS drošības audits. Drošības auditu var veikt piesaistot ārpakalpojuma sniedzēju.

4. Resursu piederība

4.1. Visi informācijas un tehnoloģiskie resursi pieder Organizācijai. Tomēr atbildības nodrošināšanas un uzskaitamības nolūkos visiem informācijas resursiem Organizācijā, vadība rakstiskā formā norīko informācijas un tehnoloģisko resursu turētājus.

4.2. Par resursa turētāju var noteikt Organizācijas nodaļas vadītāju vai augstāk stāvošu darbinieku, kurš ikdienā atbild par attiecīgo jomu.

4.3. Informācijas resursu turētāja pienākumi ir šādi:

4.3.1. klasificēt viņa turējumā esošos informācijas resursus;

4.3.2. sadarbojoties ar Informācijas drošības pārvaldnieku veikt viņa turējumā esošo informācijas resursu risku analīzi;

4.3.3. noteikt informācijas resursu lietošanas kārtību un apstiprināt lietotāju pieejas tiesības;

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

4.3.4. noteikt informācijas resursa drošības prasības, t.sk noteikt auditācijas pierakstu veidošanas un glabāšanas kārtību, prasības informācijas resursu atjaunošanai;

4.3.5. sadarboties ar tehnoloģisko resursu turētāju IS funkcionalitātes un drošības jautājumos.

4.4. Tehnoloģisko resursu turētāja pienākumi ir šādi:

4.4.1. nodrošināt tehnoloģisko resursu fiziskās un loģiskās aizsardzības pasākumus;

4.4.2. sadarboties ar informācijas resursu turētāju, lai īstenotu viņa prasības par informācijas resursu aizsardzību un piekļūšanu tiem;

4.4.3. piedalīties risku analīzē, noteikt ar tehnoloģiskajiem resursiem saistītus informācijas sistēmas apdraudējumus un novērtēt šo apdraudējumu īstenošanās varbūtību;

4.4.4. nodrošināt IS atjaunošanas procedūras, ja tehnoloģiskie resursi ir bojāti un IS funkcionēšana traucēta vai neiespējama;

4.4.5. sadarboties ar IS informācijas resursu turētāju IS funkcionalitātes un drošības jautājumos.

5. Informācijas klasifikācija

5.1. Informācijas klasifikācijas mērķis ir apzināt visas Organizācijas rīcībā esošās informācijas nozīmību un nodrošināt katras informācijas grupas aizsardzību atbilstoši tās klasifikācijas līmenim.

5.2. Informācijas resursu turētāji veic informācijas resursu klasificēšanu pēc to vērtības, konfidencialitātes un pieejamības. Informācijas klasificēšanu veic saskaņā ar informācijas resursu turētāja prasībām, ja tas tādas ir noteicis, piemēram, saskaņā ar Informācijas atklātības likumu, citos gadījumos – atbilstoši Organizācijas normatīvo aktu prasībām.

5.3. Informācijas klasifikācija attiecas uz visu informāciju neatkarīgi no informācijas nesēja (papīrs, mikrofilmas, videokasetes, magnētiskās lentes, kasetes, kompaktdiski, datoru cietie diski, disketes vai citi informācijas nesēji).

5.4. Informāciju klasificē pēc konfidencialitātes pakāpes, kad tiek vērtēti draudi tās nesakcionētai noplūdei, sekojoši:

5.4.1. vispārpieejamā informācija;

5.4.2. ierobežotas pieejamības informācija.

5.5. Informāciju klasificē pēc vērtības līmeņa, kad tiek vērtēti draudi informācijas integritātei, sekojoši:

5.5.1. augsti vērtīga informācija;

5.5.2. vidēji vērtīga informācija.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

5.6. Informāciju pēc pieejamības līmeņa, kad tiek vērtēti draudi tās pieejamībai. Klasificējot nosaka arī pieļaujamo laiku, kurā informācijas resursi var nebūt pieejami. Klasificē sekojoši:

5.6.1. informācija ir pieejama nepārtraukti;

5.6.2. informācija pieejama tikai darba laikā.

5.7. Informācija, kura nav klasificēta atbilstoši konfidencialitātes principiem automātiski tiek uzskatīta par ierobežotas pieejamības informāciju.

5.8. Ja informācijas nesējā glabājas dažādu līmeņu klasificētā informācija, kā kopīgo informācijas nesēja klasifikācijas līmeni norāda augstāko šajā nesējā esošās informācijas līmeni.

5.9. Visiem "ierobežotas pieejamības" informācijas nesējiem jābūt attiecīgai atzīmei par informācijas klasifikāciju.

6. Risku analīze un risku pārvaldības plāns

6.1. Ņemot vērā informācijas resursu klasifikāciju, tiek veikta risku pārvaldīšana. Lai plānotu risku pārvaldīšanas pasākumus, drošības pārvaldnieks sadarbojoties ar informācijas resursu turētājiem, kā arī ar tehnoloģisko resursu turētāju un veic IS risku analīzi.

6.2. Risku analīzes mērķis ir novērtēt:

6.2.1. IS apdraudējuma īstenošanās varbūtību, kur IS apdraudējums ir ar nodomu vai aiz neuzmanības izdarīta darbība vai bezdarbība, vai iespējams notikums, kas var izraisīt informācijas dzēšanu, noklusēšanu, informācijas resursu vai tehnoloģisko resursu maiņu, bojāšanu vai informācijas nonākšanu tādu personu rīcībā, kas nav tam pilnvarotas;

6.2.2. iespējamo kaitējumu informācijas resursu turētājam vai Organizācijai, ja nav nodrošināta informācijas sistēmas drošība.

6.3. Risku analīzi periodiski veic visām IS, kā arī katram jaunam ar IS saistītam projektam un IS, kurām veiktas izmaiņas, kas var ietekmēt IS drošību. Analizējot riskus, ņem vērā aktuālāko situāciju attiecībā uz IS aizsardzības pasākumiem.

6.4. Risku analīzi veic, lietojot Organizācijas noteikto risku analīzes metodoloģiju.

6.5. Informācijas resursu turētāji izvērtē atlikušo risku līmeni, veicot atkārtotu IS risku analīzi un ņemot vērā risku pārvaldīšanas pasākumu plānā iekļautos risinājumus. Ja atlikušais risku līmenis ir pieņemams, tad īsteno risku pārvaldīšanas pasākumus. Ja atlikušais risku līmenis nav pieņemams, tad veic atkārtotu IS risku pārvaldīšanas pasākumu plānošanu, līdz atlikušais risks ir pieņemams.

6.6. Saskaņā ar risku analīzes rezultātiem tiek sagatavots risku pārvaldības plāns par drošības līdzekļu ieviešanu.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

6.7. Informācijas sistēmu drošības riska pārvaldības plānā ir jāietver informācijas sistēmu drošības risku uzskaitījumu un riska izvērtējumu, kā arī drošības riska pasākumu aprakstu, to izpildes termiņus, finansējumu un par izpildi atbildīgi personu sarakstu.

7. Kopējā risku pārvaldība

7.1. Vispārējie drošības jautājumi:

7.1.1. Tehnoloģisko resursu turētājs seko informācijai par aparatūras un programmatūras jauninājumiem, lai novērstu citur atklātos attiecīgo IS drošības trūkumus, par kuriem ir publicēta informācija. Tehnoloģisko resursu turētājs apkopo informāciju par IS kļūdām, lietotāju jautājumiem un citām problēmām;

7.1.2. vispārējais datu uzglabāšanas režīms, kas tiek nodrošināts Organizācijas datortīklā, atbilst vidējas vērtības, iekšējas lietošanas informācijas statusam ar pieejamību darba laikā.

7.1.3. Darbiniekiem, kas veic IS uzturēšanu un uzraudzību, nosaka pienākumus, atbildību un nodrošina savstarpējo aizvietojamību.

8. Fiziskā aizsardzība

8.1. Risku pārvaldīšanas ietvaros realizē IS fiziskās aizsardzības pasākumus, kas aizsargā no nevēlamiem apkārtējās vides (ugunsgrēks, plūdi, temperatūras svārstības u.c.), tehniskajiem (neatbilstoša elektroenerģijas padeve u.c.) un cilvēkfaktoriem (tīši vai netīši bojājumi, zādzība u.c.).

8.2. IS fiziskās aizsardzības pasākumi detalizēti tiek aprakstīti informācijas sistēmu iekšējos drošības noteikumos. Atbildīgas par sistēmu iekšējo drošības noteikumu izstrādi ir Informācijas drošības pārvaldnieks.

9. Loģiskā aizsardzība

9.1. Risku pārvaldīšanas ietvaros realizē IS loģiskās aizsardzības pasākumus.

9.2. IS loģiskās aizsardzības pasākumi detalizēti tiek aprakstīti informācijas sistēmu iekšējos drošības noteikumos. Atbildīgas par sistēmu iekšējo drošības noteikumu izstrādi ir Informācijas drošības pārvaldnieks.

10. IS darbības nepārtrauktības un avārijas atjaunošanas plānošana un pārvaldība

10.1. Lai nodrošinātu informācijas sistēmu darbības nepārtrauktību un avārijas atjaunošanu, Organizācijā tiek izstrādāts informācijas sistēmu darbības nepārtrauktības un atjaunošanas plāns.

10.2. Atbildīgais par informācijas sistēmu darbības nepārtrauktības un atjaunošanas plāna izstrādi un uzturēšanu ir tehnoloģisko resursu turētājs.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

10.3. Informācijas sistēmu darbības nepārtrauktības un atjaunošanas plānā ir jāietver pasākumu apraksts, kuri nodrošina sistēmu nepārtrauktu darbību un to atjaunošanu avārijas gadījumā.

10.4. IS darbības nepārtrauktības pārvaldīšanas ietvaros tehnoloģisko resursu turētāji veic šādus pasākumus:

10.4.1. identificē visas būtiskās IS darbības funkcijas, kuras nodrošina IS;

10.4.2. nosaka prioritātes līmeņus atjaunojamajām funkcijām atkarībā no to svarīguma Organizācijas darbības veikšanai un zaudējumu samazināšanai;

10.4.3. sadarbībā ar informācijas turētājiem nosaka katras IS nepārtrauktības prasības.

10.5. Prasību izveidošanā jāizmanto IS klasifikācijā iegūtā informācija:

10.5.1. identificē apdraudējumus, kas var pārtraukt vai bojāt IS darbību;

10.5.2. nosaka darbības atjaunošanas vai aizstāšanas prasības katrai funkcijai un IS, kura šo funkciju nodrošina.

10.6. Tehnoloģisko resursu turētājs veic IS darbības atjaunošanas plāna izstrādi, uzturēšanu, testēšanu un realizēšanu vai nosaka rakstiski, kurš darbinieks to veic.

10.7. Tehnoloģisko resursu turētājs organizē regulāru (ne retāk kā reizi gadā) IS darbības atjaunošanas procesos iesaistīto personu apmācību un plāna testēšanu, lai pārliecinātos, ka plāns darbojas.

Pielikums Nr.2
Informācijas klasificēšanas noteikumu paraugs

Informācijas klasificēšanas noteikumi

1. Vispārīgie noteikumi

1.1. Noteikumos raksturoti informācijas klasificēšanas un klasificētas informācijas lietošanas pamatprincipi organizācijā un noteiktas IR un TR turētāju tiesības, pienākumi un atbildība par viņu pārziņā esošo IR klasificēšanu un atbilstošu izmantošanu.

1.2. Klasificēšanas mērķis ir apzināt organizācijas rīcībā esošās informācijas nozīmību, iedalīt to klasifikācijas grupās, lai nodrošinātu katras informācijas grupas aizsardzību atbilstoši klasifikācijas līmenim paredzētajām prasībām.

1.3. IR turētājs ir atbildīgs par visas viņa pārraudzībā esošās informācijas klasificēšanu, kā arī par regulāru klasifikācijas aktualizēšanu.

1.4. Informācijas klasifikācija attiecas uz visu organizācijas rīcībā esošo informāciju neatkarīgi no informācijas nesēja veida (papīrs, diskete, cietais disks, magnētoptiskais disks, magnētiskā lente vai citi).

1.5. Noteikumos minētās prasības ir obligātas un saistošas visiem organizācijas darbiniekiem un citām personām (piegādātāji, konsultanti, ārpakalpojumu kompāniju darbinieki utt.), kurām saistībā ar viņu pienākumu izpildi ir vai var būt pieeja organizācijas klasificētās informācijas resursiem.

1.6. Šie noteikumi ir izstrādāti saskaņā ar organizācijas "IS drošības politiku" un citiem organizācijas darbību reglamentējošiem dokumentiem.

2. Informācijas klasifikācijas kategorijas

2.1. Klasificējot informāciju pēc tās **konfidencialitātes** līmeņa, tiek lietotas 2 kategorijas:

2.1.1. K1 –ierobežotas pieejamības informācija;

2.1.2. K2 –vispārpieejamā informācija.

2.2. Konfidencialitātes līmeni nosaka atkarībā no tā, kādi zaudējumi organizācijai var rasties informācijas nesankcionētas izmantošanas gadījumā.

2.3. Klasificējot Informāciju pēc tās **pieejamības** līmeņa, tiek lietotas 3 kategorijas:

2.3.1. P1 – Informācija ir pieejama organizācijas darba laikā, ne vēlāk kā 1 stundas laikā;

2.3.2. P2 – Informācija ir pieejama organizācijas darba laikā, ne vēlāk kā 1 dienas laikā;

2.3.3. P3 – Informācija ir pieejama organizācijas darba laikā, ne vēlāk kā 2-3 dienu laikā.

2.4. Klasificējot Informāciju pēc tās **vērtības** līmeņa, tiek lietotas 3 kategorijas:

2.4.1. V1 – Augsta riska informācija;

2.4.2. V2– Vidēja riska informācija;

2.4.3. V3– Zema riska informācija.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

2.5. Vērtības līmeni nosaka atkarībā no tā, kādi zaudējumi organizācijas var rasties, ja tās darbiniekiem nav pieejama pilnīga, precīza un atbilstoša informācija noteiktā vietā un laikā.

3. Informācijas klasificēšanas process

3.1. Informācijas klasifikāciju veic izmantojot "Informācijas resursu klasifikācijas anketa" (Pielikums Nr.1)

3.2. IS turētājs ir atbildīgs par zaudējumiem, kas radušies, ja klasificējamā informācija nav klasificēta.

3.3. Veicot IR klasificēšanu vai mainot IR klasifikācijas līmeni IS drošības pārvaldnieks izvērtē un apstiprina IR turētāju noteikto informācijas atbilstību noteiktajiem klasifikācijas līmeņiem.

3.4. Organizācijas vadībai ir tiesības piešķirt vai mainīt klasifikācijas līmeni jebkuram organizācijas rīcībā esošam IR, informējot par to attiecīgā IR turētāju.

5. IR saraksts un tā uzturēšana

IS drošības pārvaldnieks apkopojot informācijas resursu klasifikācijas anketas izveido klasificēšanas sarakstu (Pielikums Nr. 2) par organizācijā esošajiem IR;

IR saraksts ir tabula, kurā uzskaitītas visas organizācijā esošās IS un to sastāvā esošie informācijas resursi.

Informācijas resursu klasifikācijas sarakstā ir jānorāda:
- informācijas sistēma, informācijas resursi un to turētāji;
- informācijas resursu konfidencialitātes, pieejamības, vērtības līmenis;

IR sarakstu veido un uztur IS drošības pārvaldnieks un nodrošina IS apraksta aktualitāti, kā arī uztur informāciju par IR turētājiem un aizbildņiem.

5. Klasificētas informācijas lietošana

[Šajā nodaļā tiek definēts, piemēram, prasības klasificētu informācijas izpaušanai ārpus organizācijas, kādi dati tiek izmantoti programmatūras izstrādē un testēšanā]

6. Klasificētas informācijas pārsūtīšana

[Šajā nodaļā tiek definēts, piemēram, kad informācija tiek šifrēta, kādas metodes tiek izmantotas, ja informācija tiek kopēta, kurš ir atbildīgais par drošības līmeni kāds tiek ievērots uz nokopētā datu nesēja]

7. Klasificētas informācijas fiziskā aizsardzība

[Šajā nodaļā tiek definēts, piemēram, kā informācija tiek uzglabāta, kādas ir prasības uzglabājot rezerves kopijas, kādas ir prasības attiecībā uz izdrukāto informāciju, klimata kontroli un nepārtrauktās barošanas iekārtām]

8. Klasificētas informācijas loģiskā aizsardzība

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

[Šajā nodaļā tiek definēts, piemēram, kā tiek ierobežota pieeja informācijai operētājsistēmas līmenī, kā tiek nodrošināta serveru dublēšana, kādas ir prasības lietotāju datoriem, kuri strādā ar klasificētu informāciju, vai tiek veidoti auditācijas pieraksti šādiem lietotāju datoriem]

9. Klasificētas informācijas nesēju iznīcināšana

[Šajā nodaļā tiek definēts, piemēram, kādas darbības tiek veiktas ar klasificētās informācijas nesējiem, izdrukām, elektronisko datu nesējiem, optiskiem diskiem]

1.Pielikums
Informācijas klasificēšanas noteikumiem

Informācijas resursu klasifikācijas anketa

1. Informācijas resurss

Informācijas resursa apraksts:	
Informācijas resursu turētājs:	
IS nosaukums, kuras sastāvdaļa ir klasificējamais informācijas resurss:	
Vispārējs IS nodrošināto pakalpojumu apraksts:	

2. Klasifikācijas metode

Informācijas resursu klasificēšanā tiek izmantoti jēdzieni: lieli zaudējumi, vidēji zaudējumi un niecīga ietekme uz organizāciju.

Organizācijai ir jānosaka kvantitatīvi kritēriji dažādiem atbilžu variantiem (zaudējumus var raksturot ar atbilstošiem naudas līdzekļiem):

	No	**Līdz**
Lieli zaudējumi		
Vidēji zaudējumi		
Niecīga ietekme		

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

2. Konfidencialitāte

Novērtējiet ietekmi uz organizāciju, kāda var rasties informācijas nesankcionētas atklāšanas gadījumā (sliktākais gadījums)		**Atbilžu varianti:** 1 - lieli zaudējumi 2 - vidēji zaudējumi 3 - niecīga ietekme	**Komentāri**
1	***REPUTĀCIJAS ZAUDĒŠANA*** Kādas sekas informācijas atklāšana atstātu uz organizācijas reputāciju?		
2	***JURIDISKAS SEKAS*** Vai informācijas atklāšana būtu juridisku (normatīvos aktos vai līgumos) noteiktu saistību pārkāpums?		
3	***DARBINIEKU NOSKAŅOJUMS*** Vai informācijas atklāšana negatīvi ietekmētu darbinieku noskaņojumu vai motivāciju?		
4	***KRĀPŠANA*** Vai informācijas atklāšana ļautu neatbilstoši izmantot materiālos resursus?		
5	***PAPILDU IZMAKSAS*** Vai informācijas atklāšanas gadījumā rastos papildu izmaksas?		
	KOPĒJAIS NOVĒRTĒJUMS Ņemot vērā iepriekš sniegto vērtējumu un citus nosacījumus, atzīmējiet lielāko negatīvo ietekmi uz darbību, kādu var radīt informācijas nesankcionēta atklāšana.		

Atbildot uz anketas "Konfidencialitāte" jautājumiem, jāatzīmē tas atbilžu variants, kas raksturo vislielāko iespējamo negatīvo ietekmi, kādu informācijas konfidencialitātes zudums var radīt organizācijai.

3. Integritāte vai vērtība

Novērtējiet ietekmi uz organizāciju, kāda var rasties kļūdainas vai apzināti sagrozītas (krāpšanas vai slēpšanas nolūkā) informācijas izmantošanas gadījumā (sliktākais gadījums)		**Atbilžu varianti:** 1 - lieli zaudējumi 2 - vidēji zaudējumi 3 - niecīga ietekme	**Komentāri**
1	***VADĪBAS LĒMUMI*** Vai vadība varētu pieņemt nepareizus lēmumus, pamatojoties uz kļūdainu vai sagrozītu informāciju?		
2	***KRĀPŠANA*** Vai informācija var tikt sagrozīta ar mērķi gūt materiālu labumu?		
3	***UZTICĪBAS ZAUDĒŠANA*** Kādas sekas varētu radīt kļūdaina vai sagrozīta informācija uz klientu uzticību?		

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

4	***JURIDISKAS SEKAS*** Vai kļūdaina vai sagrozīta informācija var radīt juridisku, normatīvos aktos vai līgumos noteiktu saistību pārkāpumu?		
5	***ORGANIZACIJAS DARBĪBAS TRAUCĒJUMI*** Vai kļūdainas vai sagrozītas informācijas rezultātā varētu rasties organizācijas darbības traucējumi?		
	KOPĒJAIS NOVĒRTĒJUMS Ņemot vērā iepriekš sniegto vērtējumu un citus nosacījumus, atzīmējiet lielāko negatīvo ietekmi uz darbību, kādu var radīt kļūdaina vai apzināti sagrozīta informācija.		

Atbildot uz anketas "Integritāte" jautājumiem, jāatzīmē tas atbilžu variants, kas raksturo vislielāko iespējamo negatīvo ietekmi, kādu informācijas integritātes zudums var radīt organizācijai.

4. Pieejamība

Novērtējiet ietekmi uz organizāciju, kāda var rasties IS darbības pārtraukuma rezultātā (sliktākais gadījums)		**Atbilžu varianti:** 1 - lieli zaudējumi 2 - vidēji zaudējumi 3 - niecīga ietekme			**Komentāri**
		IS darbības pārtraukuma ilgums			
		4 stundas	Viena diena	2-3 dienas	
1	***VADĪBAS LĒMUMI*** Vai IS darbības pārtraukums var negatīvi ietekmēt vadības lēmumu pieņemšanu?				
2	***UZTICĪBAS ZAUDĒŠANA*** Vai IS darbības pārtraukums var negatīvi ietekmēt klientu uzticību?				
3	***JURIDISKAS SEKAS*** Vai IS darbības pārtraukums būtu juridisku (normatīvā aktā vai līgumā noteiktu) saistību pārkāpums?				
4	***DATU ATJAUNOŠANA*** Kādas būtu IS darbības atjaunošanas izmaksas, ja tā uz laiku tiek apturēta?				

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

5	***KRĀPŠANA*** Vai IS darbības pārtraukumi var radīt naudas līdzekļu vai citu resursu piesavināšanos?				
6	***PAPILDU IZMAKSAS*** Kādas papildu izmaksas varētu rasties IS darbības pārtraukuma rezultātā?				
	KOPĒJAIS NOVĒRTĒJUMS Ņemot vērā iepriekš sniegto vērtējumu un citus nosacījumus, katram IS darbības pārtraukuma ilgumam atzīmējiet lielāko negatīvo ietekmi uz darbību, kādu tas var radīt.				

Atbildot uz anketas "Pieejamība" jautājumiem, katram norādītajam IS darbības pārtraukuma ilgumam jāieraksta tas atbilžu variants, kas raksturo vislielāko iespējamo negatīvo ietekmi, kādu IS darbības pārtraukums var radīt organizācijai.

Kopsavilkums

Konfidencialitātes līmenis:

☐ **Ierobežotas pieejamības informācija (K1)**	- nepilnvarotu personu piekļuve šai informācijai var radīt neatgriezenisku un būtisku kaitējumu informācijas devējam vai organizācijai. Piešķir, ja informācijas konfidencialitātes zudums tiek novērtēts ar "1".
☐ **Vispārpieejamā informācija (K2)**	- piekļuve šai informācija nerada kaitējumu informācijas devējam vai organizācijai. Piešķir, ja informācijas konfidencialitātes zudums tiek novērtēts ar "2".

Vērtības vai integritātes līmenis:

☐ **Augsta riska (V1)**	- kļūdaina vai sagrozīta informācija var apdraudēt organizācijas turpmāko darbību vai radīt nozīmīgus n ilgstošus zaudējumus. Piešķir, ja informācijas integritātes zudums tiek novērtēts ar "1".
☐ **Vidēja riska (V2)**	- kļūdaina vai sagrozīta informācija var radīt organizācijai jūtamus zaudējumus. Piešķir, ja informācijas integritātes zudums tiek novērtēts ar "2".
☐ **Zema riska (V3)**	- kļūdaina vai sagrozīta informācija var radīt organizācijai nebūtiskus zaudējumus. Piešķir, ja informācijas integritātes zudums tiek novērtēts ar "3".

Informācijas pieejamība (nepieciešamā, kas var nebūt arī esošā)**:**

- Darba dienās (no plkst. … līdz …): _____
- Brīvdienās un svētku dienās (no plkst. … līdz …): _____

Kopējais informācijas pieejamības zuduma novērtējums (A-C):

4 stundas	1 diena	2-3 dienas

1 - lieli zaudējumi (P1)
2 - vidēji zaudējumi(P2)
3 - niecīga ietekme (P3)

Klasifikāciju apstiprina IR turētājs: _____

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

2.Pielikums
Informācijas klasificēšanas noteikumiem

Organizācijas klasifikators

IS nosaukums	IR apraksts	Klasifikācijas datums	IR turētājs	Konfiden-cialitāte	Integritāte	1 dienas nepie-ejamības ietekme	2-3 dienu nepie-ejamības ietekme	Pieejamība (DD - darba dienas, BSD - brīvdienas un svētku dienas)

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

Pielikums Nr.3
Informācijas sistēmu riska analīzes noteikumu paraugs

Informācijas sistēmu riska analīzes noteikumi

1. Vispārīgi jautājumi

1.1. IS riska analīze ir process, kas ļauj izvērtēt informācijas sistēmu trūkumus, apdraudējumus un to īstenošanās iespējamās sekas, lai piemērotu atbilstošus drošības līdzekļus risku samazināšanai.

1.2. IS riska analīzes noteikumi izstrādāti saskaņā ar Latvijas Republikā spēkā esošo likumdošanu un citiem organizācijas darbību reglamentējošiem dokumentiem.

1.3. Noteikumos formulētās prasības ir obligātas un saistošas visiem organizācijas informācijas resursu turētājiem, tehnoloģisko resursu turētājiem, kā arī citām personām, kas piedalās riska analīzes procesā.

1.4. Noteikumi nosaka kārtību, kā organizācijā ir jāveic IS riska analīze, jāizvērtē iegūtie rezultāti un jāpiemēro atbilstošie drošības līdzekļi.

2. Riska analīzes nosacījumi

2.1. IS riska analīzi koordinē un veic IS drošības pārvaldnieks.

2.2. IS risku analīze tiek piemērota katrai informācijas sistēmai kopumā, nepieciešamības gadījumā to var pielietot arī atsevišķām IS komponentēm vai pakalpojumiem.

2.3. IS riska analīzes veikšana organizācijā notiek pēc IS riska analīzes metodoloģijas, kuru apstiprina organizācijas vadība.

2.4. IS riska analīze ir jāveic:

2.4.1. visām esošajām IS;

2.4.2. katrai jaunai IS, pirms tās ieviešanas.

2.5. Veicot riska analīzi nepieciešams:

2.5.1. izanalizēt kopš iepriekšējās riska analīzes notikušos drošības incidentus;

2.5.2. izanalizēt kopš iepriekšējās riska analīzes ieviesto drošības līdzekļu lietderību un efektivitāti;

2.5.3. noteikt iespējamos apdraudējumus informācijai un organizācijas darbības procesiem;

2.5.4. analizēt apdraudējumu īstenošanās iespējamību;

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

2.5.5. analizēt iespējamās apdraudējumu īstenošanās tiešās un netiešās sekas;

2.5.6. noteikt apdraudējumus, pret kuriem ir jāveic aizsardzība to novēršanai;

2.5.7. noteikt apdraudējumu novēršanas pasākumus;

2.5.8. novērtēt, vai atlikušais risks ir pieņemams informācijas sistēmas turētājiem;

2.5.9. veikt apdraudējumu novēršanas pasākumus;

2.5.10. pēc noteikta laika novērtēt veikto pasākumu lietderību. Ja atlikušais risks joprojām nav pieņemams, tad atkārtoti jālemj par apdraudējumu novēršanas pasākumiem.

2.6. Izvēloties drošības līdzekļus jāseko, lai to ieviešanas un uzturēšanas izmaksas nepārsniedz apdraudēto resursu vērtību.

2.7. Informatīvajai sistēmai ir jāveic atkārtota riska analīze, ja:

2.7.1. ievērojami mainās ar IS saistītie uzņēmējdarbības procesi;

2.7.2. ievērojami mainās IS funkcionalitāte un pielietojums;

2.7.3. IS tiek konstatēti jauni nopietni drošības apdraudējumi;

2.7.4. noticis nozīmīgs vai vairāki atkārtoti drošības incidenti;

2.7.5. ievērojami mainās ar informāciju vai IS saistīti faktori (likumdošana, līgumsaistības u.c.);

2.7.6. IS tiek likvidēta;

2.7.7. kopš iepriekšējās riska analīzes veikšanas ir pagājis 1 gads.

3. Darbības pēc riska analīzes

3.1. Riska analīzes veicējiem rezultāti jāapkopo un rakstiski jānoformē saskaņā ar izvēlēto IS riska analīzes metodoloģiju.

3.2. IR turētājam, sadarbībā ar TR turētāju un IS drošības pārvaldnieku, jānosaka apdraudējumu novēršanas pasākumu plāns, atbildīgie par to ieviešanu un ieviešanas termiņi.

3.3. IR turētājam ir jāapliecina, ka viņš piekrīt plānā iekļautajiem drošības līdzekļiem un uzņemas atbildību par atlikušo risku, pret kuru riska analīzes rezultātā nolemts nenodrošināties.

1. pielikums
Informācijas sistēmu riska
analīzes noteikumiem

Informācijas sistēmu risku analīzes metodika

1. Vispārīgie jautājumi

1.1 Informācijas sistēmu risku analīzes metodika ir uz biznesu orientēts risku novērtēšanas līdzeklis, kas paredzēts jaunu, ekspluatācijā esošu un likvidējamu informācijas sistēmu (IS) un ar tām saistīto procesu trūkumu un drošības apdraudējumu novērtēšanai, lai ieviestu atbilstošus riskus mazinošus drošības līdzekļus.

1.2 Metodika ir izstrādāta saskaņā ar organizācijas Informācijas drošības politiku un Informācijas sistēmu riska analīzes noteikumiem. Piedāvātā metodika ir paredzēta IS pamata risku novērtēšanai.

1.3 Saskaņā ar šo metodiku iegūtie rezultāti var kalpot par ieejas datiem detalizētākām risku analīzes metodēm vai tehniskām IS drošības pārbaudēm, kas nepieciešamības gadījumā var tikt pielietotas IS kritisko funkciju drošības risku novērtēšanai.

1.4 Ja kādam no IS elementiem ir nepieciešams veikt detalizētāku riska analīzi vai drošības pārbaudi, tad tas tiek fiksēts pamata IS risku analīzē kā viens no ieviešamiem drošības līdzekļiem.

2. Riska analīzes veikšana un riska novērtēšana

2.1. IS risku analīžu veikšanā tiek izmantota Apdraudējumu novērtējuma tabula (3. pielikums), kas ir neatņemama šīs metodikas sastāvdaļa.

2.2. Riska analīzes veikšanai nepieciešamo datu savākšana un apkopošana notiek analīzes un interviju veidā, ko koordinē IS drošības pārvaldnieks. Intervijās tiek piesaistīts IR turētājs. Intervijās var tikt piesaistīti:

2.2.1. TR turētājs;

2.2.2. citi darbinieki, kuru zināšanas un pieredze var palīdzēt risku identificēšanā.

2.3. Pēc interviju rezultātiem notiek datu apkopošana IS riska analīzes kopsavilkumā (2. pielikums) un apdraudējumu novērtējuma tabulā (3. pielikums):

2.3.1. ietekmes novērtēšanai tiek pielietota skala no 1 līdz 3;

2.3.2. riska iestāšanās varbūtības novērtēšanai tiek pielietota skala no 1 līdz 3;

2.4. Risku iegūst, sareizinot apdraudējuma ietekmi ar tā iestāšanās varbūtību.

2.5. Riski tiek klasificēti kā zemi, ja iegūst rezultātu diapazonā no 1 līdz 2.

2.6. Riski tiek klasificēti kā vidēji, ja iegūst rezultātu diapazonā no 3 līdz 4.

2.7. Riski tiek klasificēti kā augsti, ja iegūst rezultātu diapazonā no 6 līdz 9.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

2.8. Riska analīzes gaitā tiek veikta arī esošo IS drošības līdzekļu efektivitātes un atbilstības novērtēšana un konstatēto nopietnāko drošības incidentu analīze.

3. Drošības līdzekļu izvēle un ieviešana

3.1. Katra konstatētā riska mazināšanai/novēršanai ir jāpiedāvā ieviest gan tehniskos, gan administratīvos drošības līdzekļus, ja vien tas ir iespējams.

3.2. Veicot risku analīzi, galīgo slēdzienu par drošības līdzekļu ieviešanu pieņem pēc visu resursu risku analīzes veikšanas un visu risku identifikācijas.

3.3. Katram ieviešamajam drošības līdzeklim tiek noteikts atbildīgais par tā ieviešanu un ieviešanas termiņš. Tas tiek fiksēts IS riska analīzes kopsavilkumā.

3.4. IR turētājam ir jāapliecina ar parakstu, ka viņš piekrīt plānā iekļautajiem ieviešamajiem drošības līdzekļiem un uzņemas atbildību par atlikušo risku, kura samazināšanai/novēršanai riska analīzes rezultātā nolemts neieviest drošības līdzekļus.

4. Riska analīzes rezultātu noformēšana

4.1. Risku analīzes rezultāti tiek noformēti rakstiski, aizpildot IS riska analīzes kopsavilkumu, kas sastāv no šādām sadaļām:

4.1.1. vispārējie dati par IS riska analīzi (vispārējā informācija par konkrēto IS, tās turētāju, riska analīzes datumi un to veikšanas iemesli, kā arī īss nopietnāko incidentu uzskaitījums, kas notikuši kopš iepriekšējās riska analīzes);

4.1.2. IS informācijas resursu klasifikācija (dati no IS klasifikācijas anketas) un apdraudējuma ietekmes apmērs organizācijai atkarībā no IS dīkstāves laika;

4.1.3. īss IS funkcionalitātes un tehniskās uzbūves apraksts;

4.1.4. vidējo un augsto risku apraksts un drošības līdzekļu nepieciešamības pamatojums;

4.1.5. atceļamie drošības līdzekļi un atcelšanas iemesli (atceļamo drošības līdzekļu uzskaitījums un to atcelšanas iemesli gadījumā, ja šie līdzekļi ir zaudējuši aktualitāti);

4.1.6. ieviešamie drošības līdzekļi (obligāti ieviešamie drošības līdzekļi, norādot konkrēto apdraudējumu, kā arī par izpildi atbildīgās personas un izpildes termiņus);

4.1.7. ieteicamie drošības līdzekļi (ieteicamo drošības līdzekļu uzskaitījums un apraksts, kuru ieviešana nav obligāta, taču uzlabotu IS drošību).

4.2. IS riska analīzes kopsavilkumu paraksta IR turētājs, tādējādi apstiprinot atlikušos riskus un ieviešamo drošības līdzekļu termiņu plānu.

4.3. Risku analīzes rezultāti tiek iesniegti organizācijas vadībai apstiprināšanai.

2. pielikums
Informācijas sistēmu riska
analīzes noteikumiem

IS riska analīzes kopsavilkums

1. Vispārējie dati par IS riska analīzi

Informācijas sistēmas nosaukums _____

Informācijas resursu turētājs _____

Riska analīzes veikšanas datums _____

Iepriekšējās riska analīzes veikšanas datums _____

Riska analīzes veikšanas iemesls _____

2. **IS informācijas resursu klasifikācija** (dati no IS klasifikācijas anketas)

Informācijas resurss	**Klasifikācija**		
	Konfidencialitāte	**Integritāte**	**Pieejamība**

Kopējais informācijas pieejamības zuduma novērtējums (A-C):

4 stundas	1 diena	2-3 dienas

A - lieli zaudējumi
B - vidēji zaudējumi
C - niecīga ietekme

3. IS funkciju un tehniskās uzbūves apraksts

_____

_____

4. Konstatētie nopietnākie drošības incidenti

_____

_____

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

5. Risku apraksts un drošības līdzekļu nepieciešamības pamatojums

_____

_____

6. Ieviešamie drošības līdzekļi

Ieviešamais drošības līdzeklis	**Atbildīgais** (vārds, uzvārds, amats)

Informācijas resursu turētājs: _____

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

3. pielikums
Informācijas sistēmu riska
analīzes noteikumiem

Apdraudējumu novērtējuma tabula (1.variants)

IS nosaukums:
Risku analīzes veikšanas datums:

	Apdraudējums	Apraksts	K	I	P	Varbūtība	Ietekme	Risks
	Aparatūra							
1	Apkalpošanas kļūda	Kļūdas aparatūras ekspluatācijā un apkopē, piemēram, rezerves kopēšanas iekārta netiek regulāri tīrīta, kas izraisa rezerves kopēšanas ierakstu kļūdas		X	X	*2*	*3*	*6*
2	Aparatūras nepietiekama veiktspēja	Strauji pieaugot datu apjomam, tiek pārslogota aparatūra, kā rezultātā sistēma vairs nespēj savlaicīgi apkalpot pieprasījumus			X	1	2	2
3	Barošanas iekārtu (UPS) atteikums	Traucējumi sistēmā UPS nolietošanās rezultātā		X	X			0
4	Aparatūras atteice	Kļūda aparatūras darbībā, kas rodas iekšēja defekta vai fiziskā nolietojuma dēļ			X			0
	Datu nesēji							
6	Datu nesēju nolietošanās vai lasīšanas kļūdas	Datu nesēju kļūdas to nolietošanās vai iekšējo defektu dēļ		X	X			0
7	Neautorizētas darbības ar datu nesējiem	Datu nesēju tīša bojāšana, to neautorizēta kopēšana vai pārvietošana	X	X	X			0

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

9	Rezerves kopiju atjaunošanas problēmas	Avārijas gadījumā nav iespējama nepieciešamo datu atjaunošana, jo netiek veiktas regulāras datu rezerves kopēšanas un pārbaudes atjaunošanas procedūras		X	X			0
	Programmatūra							
11	Programmatūras kļūda	Neadekvāts programmatūras darbības rezultāts tās kļūdas dēļ	X	X	X			0
12	Nedokumentētas iespējas programmatūrā	Izmantojot programmatūras nedokumentētas iespējas, tiek veiktas neautorizētas darbības sistēmā	X	X				0
13	Ieviešanas kļūda	Kļūda programmatūras ieviešanas laikā		X	X			0
14	Uzturēšanas kļūda	Kļūda programmatūras uzturēšanas laikā, piemēram, rezerves kopiju veidošana laikā, kad lietotāji strādā ar sistēmu		X	X			0
15	Nelicencētas programmatūras lietošana	Lietotāji izmanto nelicencētu programmatūru			X			0
16	Destruktīva programmatūra (vīrusi…)	Sistēmas tiek inficētas ar programmatūru, kuras darbības var traucēt, bojāt vai paralizēt organizācijas datorus, datortīklu, sakaru kanālus (piemēram, datorvīrusi) vai arī atļaut pieeju resursiem vai tos publiskot	X	X	X			0
	Personāls							
18	Neautorizētas darbības ar programmatūru vai datiem	Lietotājs izmanto programmatūru savos darba pienākumos neparedzētu darbību veikšanai	X	X	X			0
19	Paroles izpaušana	Organizācijas darbinieki izpauž savu paroli citiem darbiniekiem vai trešajām personām	X	X				0
20	Svešas identitātes izmantošana	Organizācijas darbinieks vai trešā persona identificē sevi par citu personu	X	X				0

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

21	Paroļu neatbilstība prasībām	Lietotāji autentifikācijai lieto vienkāršas paroles, kas viegli uzminamas	X	X				0
22	Personāla trūkums	Darbinieku trūkums, kā dēļ netiek veikti vai tiek veikti nepilnīgi organizācijas funkcionēšanai nepieciešamie uzdevumi		X	X			0
23	Nekompetents personāls	Lietotāji nav apmācīti rīkoties ar ikdienas darbam nepieciešamo aparatūru, programmatūru, informāciju.	X	X				0
23	Nekompetenti lietotāji	Lietotāji nav iepazīstināti ar organizācijas politiku attiecībā uz darbu ar konfidenciālu informāciju, augsta riska sistēmām	X	X				0
24	Lietotāju kļūdas	Lietotājs pieļauj kļūdas savā darbā, piemēram, ievada kļūdainu informāciju		X				0
25	Informācijas izpaušana	Lietotāji izpauž viņu rīcībā esošo informāciju	X					0
	Sakari un komunikācijas							
27	Pieslēgšanās komunikāciju līnijām	Tieša pieslēgšanās komunikāciju līnijām	X					0
28	Noklausīšanās	Komunikācijas līniju vai telpu noklausīšanās	X					0
29	Komunikāciju līniju bojājumi	Fiziskās iedarbības rezultātā radusies nespēja nodrošināt komunikācijas starp pieslēguma punktiem, piemēram, kabeļa pārrāvums		X	X			0
30	Pārraides kļūda	Pārraides laikā ārējās vides, cilvēku ļaunprātīgas rīcības vai aparatūras bojājumu dēļ tiek noraidīti nepareizi dati		X				0

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

31	Kļūda ziņojumu adresācijā	Nepareiza ziņojuma adresācija, piemēram, nepareizi norādīta e-pasta adrese, nepareiza maršrutizētāja darbība	X		X			0
32	Datu plūsmas pārslodze	Neplānoti liela datu plūsma sakaru kanālos, kas izraisa sakaru kvalitātes pasliktināšanos		X	X			0
33	Atkarība no citām IS	Tādas IS atteikums, kuras izejas dati tiek izmantoti dotajā IS			X			0
34	Neautorizētu personu piekļūšana iekšējiem resursiem, izmantojot datortīklu	Cilvēku darbības vai nepareizas datortīkla konfigurācijas dēļ notiek neautorizēta iekšējo resursu izmantošana	X					0
	Apkārtējā vide							
36	Ugunsgrēks	Ugunsgrēka izcelšanās organizācijā vai tās apkārtnē, tādējādi radot draudus organizācijas resursiem, tai skaitā informācijas un tehniskajiem resursiem			X			0
37	Plūdi	Plūdu izcelšanās organizācijas apkārtnē, maģistrālā ūdensvada pārrāvums organizācijā vai tās tiešā tuvumā			X			0
38	Zibens	Zibens spēriens organizācijas ēkās, būvēs vai tehniskajos līdzekļos			X			0
39	Vētra	Vētra, kuras izraisītais vējš var izraisīt organizācijas resursu bojāšanos (piemēram, norauti ēku jumti, pārrauti elektrības vadi)			X			0
40	Zādzība	Neautorizēta organizācijas resursu pārvietošana vai kopēšana	X		X			0
41	Sprādziens	Sprādziens organizācijā vai tās tuvumā, kas var izraisīt resursu bojājumus vai iznīcināšanu			X			0
42	Tīšs bojājums	Tīšs informācijas, programmatūras vai tehnisko resursu bojājums		X	X			0

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

43	Putekļi	Putekļu, smilšu u.c. paaugstināta koncentrācija gaisā vai nokļūšana uz aparatūras, kas var izsaukt aparatūras bojājumus			X			0
44	Temperatūra	Paaugstināta vai pazemināta āra vai telpu temperatūra			X			0
45	Mitrums	Paaugstināts mitrums telpās vai ārpus tām, kas var izsaukt aparatūras un citu organizācijas resursu bojājumus			X			0
46	Strāvas padeves atteice	Strāvas padeves pārtraukumi, kā dēļ tiek traucēta sistēmas darbība		X	X			0
47	Sprieguma svārstības	Sprieguma svārstības, kā rezultātā sistēma darbojas nestabili vai arī tā tiek bojāta		X	X			0
	Citi							
48	Nekorekta datu apmaiņa ar saistītam sistēmām	Pārtraukumi vai kļūdas savstarpēja datu apmaiņā		X	X			0
49	Nepietiekama dokumentācija	Apgrūtināta sistēmas pārvalde un korekta lietošana			X			0
...	...	...						
Risku analīzi veica:								
Amats, vārds, uzvārds:								
Datums:								

Skaidrojums:
Lai noteiktu risku, jānovērtē katra tabulā minētā apdraudējuma varbūtība un tā iespējamā ietekme katrai ar "X" apzīmētajai drošības kategorijai.
Ailē "Ietekme" jāieraksta vislielākā no visām ietekmes vērtībām. Riska apmērs tiek iegūts, sareizinot aiļu "Varbūtība" un "Ietekmes" vērtības.
Apzīmējumi:
Varbūtība (apdraudējuma īstenošanās ticamība): 3 – iespējams; 2 – varbūtējs; 1 – mazticams.
Ietekmes apmēri: 3 – būtisks; 2 – jūtams; 1 – niecīgs.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

K – konfidencialitāte; I – integritāte; P – pieejamība.
X norāda apdraudējuma ietekmes esamību uz attiecīgo drošības kategoriju.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

3. pielikums
Informācijas sistēmu riska
analīzes noteikumiem

Apdraudējumu novērtējuma tabula (2.variants)

IS nosaukums:
Risku analīzes veikšanas datums:

Apdraudējumi	Sistēmai atbilst (jā/nē)	Iespējamība 1 = zema 2 = vidēja 3 = augsta	Ietekme 1 = zema 2 = vidēja 3 = augsta	Riska līmenis bez kontroles	Noteiktā kontrole / drošības līdzeklis	Jaunais riska līmenis
Dabas apdraudējumi						
Sniega vētra						
Vējš (29+m/s)						
Zibens						
Plūdi						
Epidēmija						
...						
Cilvēku radīti apdraudējumi (netīši)						
Ugunsgrēks (iekšējs, neliels)						
Ugunsgrēks (iekšējs, liels)						
Ugunsgrēks (ārējs)						
Darbinieku kļūda, nolaidība (IS uzturēšana)						
Darbinieku kļūda (lietotājs)						
Darbinieku kļūda, nolaidība (programmēšana)						
Darbinieku trūkums						
...						
Cilvēku radīti (netīši)						
Sabotāža/terorisms: ārējs-fizisks						
Sabotāža/terorisms: iekšējs-fizisks						
Viltošana, krāpšana						

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

Ļaunprātīga izmantošana (iekšēja)						
Ļaunprātīga izmantošana (ārēja)						
Darbinieku streiks						
Masu nekārtības						
...						
Vides apdraudējumi						
Strāvas traucējumi, impulsi						
Strāvas īslaicīgi pārrāvumi						
Strāvas ilgstoši pārrāvumi						
Appludināšana						
Telekomunikāciju traucējumi						
...						

Risku analīzi veica:
Amats, vārds, uzvārds:
Datums:

Pielikums Nr.4
Iekšējie informācijas sistēmu drošības noteikumu paraugs

Iekšējie informācijas sistēmu drošības noteikumi

1. Informācijas sistēmu fiziskā aizsardzība

1.1. Organizācija risku pārvaldīšanas ietvaros veic Informācijas sistēmu (IS) fiziskās aizsardzības pasākumus, kas aizsargā tās no nevēlamiem apkārtējās vides (ugunsgrēks, plūdi, temperatūras svārstības u.c.), tehniskajiem (neatbilstoša elektroenerģijas padeve u.c.) un cilvēkfaktoriem (tīši vai netīši bojājumi, zādzība u.c.).

1.2. Serveru fiziskā aizsardzība:

1.2.1. Organizācija nodrošina, ka visi IS tiek ekspluatēti ierobežotas pieejamības, slēdzamās telpās, kuru fiziskā aizsardzība nodrošina tikai pilnvarotu personu piekļuvi, vai arī nodrošina serveru fizisko aizsardzību, lai tos nevarētu izslēgt, pārvietot, bojāt un nesankcionēti mainīt to konfigurāciju. Serveru telpas izvieto ēkas vietās, kurās ir mazāka apdraudējumu īstenošanās iespējamība;

1.2.2. nepiederošas personas, t.sk. ārējie pakalpojumu sniedzēji serveru telpās drīkst uzturēties tikai pilnvarotu personu pavadībā;

1.2.3. atkarībā no iespējamo zaudējumu apmēra Organizācija nodrošina pietiekamu serveru un serveru telpu aizsardzību pret fiziskiem apdraudējumiem (t.sk. neatbilstošiem klimatiskajiem apstākļiem, ugunsgrēku, plūdiem, elektroenerģijas padeves pārtraukumiem, tīšiem bojājumiem), nepieciešamības gadījumā ierīkojot ugunsdzēsības signalizāciju, automātiskās ugunsdzēšanas sistēmu, uzstādot alternatīvās strāvas padeves iekārtas un gaisa dzesēšanas iekārtas.

1.3. Tīklu infrastruktūrai (t.sk. komunikāciju tīklu aparatūrai, kabeļu tīklam) Organizācija nodrošina pietiekamu fizisko aizsardzību, to izvietojot tādējādi, lai tai nevarētu nesankcionēti un iemānīti piekļūt, pieslēgties vai bojāt ar Organizāciju nesaistītas personas, kā arī, lai tai nevarētu nesankcionēti piekļūt, pieslēgties un bojāt, vai nejauši aiz neuzmanības bojāt Organizācijas darbinieki vai apmeklētāji.

1.4. Darbstaciju fiziskā aizsardzība:

1.4.1. tehnoloģisko resursu turētāja darba vietu nodala ierobežotas pieejamības telpās;

1.4.2. darbstacijas lieto atbilstoši ražotāja noteiktām prasībām un lieto elektroenerģijas nepārtrauktas padeves iekārtas, ja atklājas, ka elektroenerģijas padeves traucējumu risks ir nepieņemami liels.

1.5. Portatīvo iekārtu fiziskā aizsardzība:

1.5.1. portatīvos datorus lieto atbilstoši ražotāja noteiktajām prasībām;

1.5.2. Organizācija veic portatīvo iekārtu aprites reģistrēšanu, lai noteiktu, kura persona lieto attiecīgo iekārtu.

1.6. Datu nesēju fiziskā aizsardzība:

1.6.1. Organizācija veic nepieciešamos drošības pasākumus šīs kārtības 2.-5.punktā neiekļauto datu nesēju fiziskai aizsardzībai neatkarīgi no veida (t.sk.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

demontētas disku iekārtas, papīra izdrukas, faksa izdrukas, disketes, optiskie diski u.tml.);

1.6.2. datu nesējus, kas satur Informācijas sistēmas resursus lietot un pārvietot bez īpaša laika ierobežojuma drīkst tikai Organizācija pilnvaroti darbinieki, kuriem ir pieeja Informācijas sistēmas resursiem. Informācijas sistēmas resursi, kurus nav nepieciešams lietot vai pārvietot, tiek glabāti Organizācijas telpās, tam paredzētās vietās. Ja ir nepieciešams iznīcināt datu nesējus, to iznīcināšanu uzrauga vai nodrošina tehnoloģisko resursu turētājs;

1.6.3. datu nesēju aizsardzības ietvaros Organizācija veic datu ievada un izvada iekārtu fizisko aizsardzību, novēršot nesankcionētu lietošanu - printeru iekārtas neizvieto publiski pieejamās telpās, nepieļauj diskešu iekārtu darbību, ja tā nav nepieciešama darbinieku pienākumu veikšanai;

1.6.4. datu nesējus ar klasificētiem Informācijas resursiem aizliegts atstāt nedrošās (piemēram, publiski pieejamās) vietās;

1.6.5. ja datu nesēju, kas satur klasificētus Informācijas resursus, ir paredzēts iznīcināt, tad to izdara tādā veidā, lai nebūtu iespējams veikt uz tā esošo datu atjaunošanu.

1.7. Nepieciešamības gadījumā Organizācija veic papildu fiziskās aizsardzības pasākumus atkarībā no Informācijas sistēmas resursu klasifikācijas līmeņa. Informācijas sistēmas fiziskās aizsardzības pasākumus veic sistemātiski, nepieļaujot situāciju, ka Informācijas sistēmas resursi atrastos ārpus ierobežotas pieejamības telpām bez Organizācijas pilnvarotu Organizācijas darbinieku uzraudzības. Organizācija regulāri veic fiziskās aizsardzības pasākumu pārbaudi.

2. Piekļuves kontrole

2.1. Katram IR lietotājam tiek piešķirts IS lietotājvārds(i) (identifikators(i)) un parole, kā arī noteiktas piekļuves tiesības. IS lietotājs ir atbildīgs par piešķirtā lietotājvārda (identifikatora) un paroles lietošanu, saglabāšanu un neizpaušanu.

2.2. Piekļuves tiesības apstiprina attiecīgo IR turētājs. Balstoties uz IR turētāja pieprasījumu, TR turētājs izveido lietotājam piekļuvi visās apstiprinājumā norādītajās informācijas sistēmās.

2.3. IR turētājam ir jāinformē TR turētājs par tiem darbiniekiem, kuri pārtrauc darba attiecības ar Organizāciju. TR pēc šīs informācijas saņemšanas nekavējoties anulē visas attiecīgā darbinieka piekļuves tiesības Organizācijas informācijas sistēmas resursiem.

2.4. IS lietotājs ir atbildīgs par darbībām, kas tiek veiktas, izmantojot viņa lietotājvārdu (identifikatoru). IS lietotāja autentiskumu nosaka, lai pārliecinātos, ka lietotājvārda (identifikatora) izmantotājs ir sankcionētais tā turētājs. Autentiskuma noteikšanai tiek izmantotas paroles. Pēc lietotājvārda (identifikatora) un paroles ievadīšanas IS lietotājs var izmantot informācijas sistēmas resursu atbilstoši noteiktajām piekļuves tiesībām. Parole sastāv no burtu un zīmju kombinācijas un tās garums nedrīkst būt īsāks par astoņiem simboliem. Nedrīkst par paroli izmantot personu identificējošus datus (piemēram, personas

datus, automašīnas numuru, radu vārdus vai uzvārdus, vārdus, kas saistīti ar darbavietu vai kas bieži tiek tajā lietoti).

2.5. IS lietotājs paroli jāmaina vismaz reizi trijos mēnešos. TR turētājam ir jānodrošina:
2.5.1. automātisku paroles maiņas pieprasījumu, lietotājam pirmo reizi reģistrējoties tīklā;
2.5.2. automātisku paroles maiņas pieprasījumu ik pēc trim mēnešiem;
2.5.3. sistēmas bloķēšanu, ja lietotājs piecas reizes pēc kārtas ir ievadījis nepareizu paroli vai lietotājvārdu.

2.6. IS lietotājam parole ir jāiegaumē. Rakstiskā veidā paroles atļauts glabāt tikai aizslēgtā seifā.

2.7. Ja radušās aizdomas, ka paroli uzzinājusi cita persona, IS lietotājs to nekavējoties nomaina un par incidentu ziņo IR turētājam un TR turētājam .

2.8. Aizliegts mēģināt uzzināt citu lietotāju paroles, izņemot gadījumus, kad tas ir nepieciešams IS administratoram viņa tiešo pienākumu veikšanai. Pēc minēto darbu pabeigšanas IS lietotājs paroli nomaina.

2.9. Uz datora ir jābūt uzstādītam ekrāna saudzētājam ar aktivizācijas paroli. Tam ir automātiski jāaktivizējas, ja piecu minūšu laikā lietotājs nav veicis nekādas darbības.

2.10. TR turētājam ir tiesības veikt lietotāju darbības auditus. Šādi auditi var ietvert lietotāja darbību auditācijas veikšanu (tai skaitā apmeklētos interneta resursus), analizēšanu un papildus informācijas pieprasīšanu par veiktajām darbībām

3. Rezerves datu kopēšana

3.1. Organizācija regulāri veic svarīgāko informācijas resursu un programmatūru rezerves datu kopēšanu. Rezerves datu kopēšanu nodrošina TR turētājs un to biežums un apjoms tiek saskaņots ar IR turētāju.

3.2. Rezerves datu kopijas tiek uzglabātas ārpus datu centra, tā lai tās neietekmē vieni un tie paši draudi. Rezerves datu kopijām ir jābūt pieejamām jebkurā laikā.

3.3. Rezerves kopēšana tiek organizēta tā, lai būtu iespējams atjaunot datus, kas ir dienu, nedēļu, mēnesi, gadu vai vārākus gadus veci. Organizējot rezerves datu kopēšanu, tiek ņemtas vērā normatīvajos aktos noteiktās prasības.

3.4. Rezerves kopiju integritāte tiek pārbaudīta vismaz vienu reizi ceturksnī.

3.5. Ne retāk kā reizi gadā, TR turētājs sadarbībā ar IR turētāju, veic pārbaudes, lai pārliecinātos, ka rezerves datu kopijas tiek sagatavotas kvalitatīvi un no tām ir iespējams atjaunot IS darbību.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

4. Informācijas sistēmas resursu loģiskā aizsardzība

4.1. Organizācija risku pārvaldīšanas ietvaros veic informācijas sistēmu loģiskās aizsardzības pasākumus. Organizācija dokumentē un veic informācijas sistēmu lietotāju reģistrācijas, tiesību piešķiršanas un anulēšanas procedūras:

4.1.1. katram lietotājam, IR turētājam un TR turētājam piešķir unikālu lietotāja kodu. Jauna lietotāja reģistrāciju veic saskaņā ar IT drošības politiku un iekšējiem sistēmas drošības noteikumiem. Informācijas sistēmu lietotāju, IR turētāju un TR turētāja darba pienākumu maiņas vai darba attiecību izbeigšanas gadījumā tiek nekavējoties mainīti vai anulēti piešķirtie lietotāja kodi un pieejas tiesības informācijas sistēmām;

4.1.2. informācijas pārvaldnieku informācijas sistēmu pieejas kodus kopā ar parolēm glabā drošā ierobežotas pieejas vietā.

4.1.3. Lietotāju autentiskuma noteikšanas ietvaros:

4.1.4. TR turētājs pārliecinās, ka attiecīgās informācijas sistēmas lieto pilnvarotais lietotāja koda turētājs, izmantojot dažādus, pietiekamas drošības autentifikācijas līdzekļus, kas var tikt pilnveidoti, mainīti un attīstīti;

4.1.5. autentifikācijas līdzekļu lietošanas veidus un kārtību nosaka IT drošības pārvaldnieks, bet tehniski nodrošina TR turētājs;

4.1.6. kā paroli izvēlas pietiekami sarežģītu simbolu kombināciju. Ievadot paroli, tā nedrīkst būt salasāma uz datora ekrāna. Paroles elektroniskajos nesējos glabā un pārsūta šifrētas. Paroli nekavējoties nomaina, ja tā varētu būt vai ir kļuvusi zināma citai personai.

4.2. Informācijas sistēmu lietošanas pārraudzības ietvaros:

4.2.1. TR turētājs nodrošina, ka Auditācijas pieraksti tiek veidoti par Informācijas sistēmām, kas satur klasificētus Informācijas resursus, un darbībām datortīklā, kurā ir pieeja Informācijas sistēmām, kas satur klasificētus Informācijas resursus. Auditācijas pierakstos iekļauj visu veiksmīgas un neveiksmīgas pieslēgšanās gadījumu datumu un laiku, kā arī lietotāja (t.sk. Tehnoloģisko resursu turētāja) kodu vai citu autentifikācijas līdzekli;

4.2.2. TR turētājs nodrošina Auditācijas pierakstu integritāti un regulāri veido Auditācijas pierakstu datu rezerves kopijas saskaņā ar šīs kārtības 4.punkta noteikumiem;

4.2.3. TR turētājs regulāri pārrauga visu Informācijas sistēmu darbību, taču īpašu uzmanību pievērsto Informācijas sistēmas darbības pārraudzībai, kas satur klasificētus Informācijas resursus. Šim nolūkam TR turētājs pēc izvēles lieto speciālas pārraudzības programmas vai datoru iebrukumu noteikšanas sistēmas;

4.2.4. TR turētājs pārrauga vismaz šādus gadījumus:

4.2.4.1. atkārtota neveiksmīga pieslēgšanās Informācijas sistēmai;

4.2.4.2. mēģinājumi piekļūt Informācijas resursiem, kuriem lietotājs nav pilnvarots piekļūt;

4.2.4.3. Informācijas sistēmas lietošana neparastā laikā, piemēram, ārpus darba laika;

4.2.4.4. atkārtoti mēģinājumi lietot lietotāja kodus, kuri jau ir atcelti;

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

4.2.4.5. privileģēto lietotāja kodu piešķiršana un lietošana (piemēram, tehnisko resursu pārvaldnieka kodi);

4.2.4.6. nesankcionētas programmatūras konfigurācijas maiņas un neatjautas programmatūras uzstādīšana.

4.3. Vīrusu kontrole Informācijas sistēmas resursos:

4.3.1. TR turētājs nosaka kārtību un veic pasākumus datoru vīrusu darbības novēršanai informācijas sistēmās.

4.3.2. vīrusu darbības novēršanai lieto speciāli šim nolūkam paredzētu programmatūru. Vīrusu definīciju failus nekavējoties atjauno, tiklīdz izstrādātājs piedāvā atjaunojuma failus;

4.3.3. TR turētājs regulāri veic antivīrusu programmas pārraudzību, lai pārliecinātos par tās darbību un jaunāko vīrusu definīciju failu esamību.

4.4. Personālo un portatīvo datoru aizsardzība:

4.4.1. informācijas turētājs nosaka, kādu informāciju drīkst glabāt uz personālā un portatīvā datora (tālāk tekstā - personālie datori). Portatīvajos datoros, kuri tiek lietoti ārpus Organizācijas darba telpām, glabā tikai to informāciju, kas nepieciešami noteiktajā laikā noteiktajam datora lietotājam;

4.4.2. personālajā datorā uzstāda un lieto tikai to programmatūru un tādā konfigurācijā, ko ir noteicis TR turētājs. Personālā datora funkcionalitāti ierobežo līdz darba vajadzībām nepieciešamo funkciju līmenim;

4.4.3. personālo datoru, atstājot bez lietotāja uzraudzības, slēdz, lietojot ekrānsaudzētāju ar paroli, speciālu slēgšanas funkciju vai citu metodi, kas ļauj turpināt darbu ar personālo datoru vienīgi tad, ja ir veikta lietotāja autentifikācija;

4.4.4. informācijas resursu turētājs nosaka kārtību, kādā darba vajadzībām darbinieki lieto viņiem piederošus datorus un kādā lieto Organizācijas datorus ārpus darba telpām. Šī kārtība nedrīkst samazināt noteikto informācijas resursu aizsardzības līmeni.

4.5. Datortīklu aizsardzība:

4.5.1. TR turētājs izstrādā un uztur datortīkla shēmu, kurā parādīta datortīklā savienotā aparatūra un nodrošinātie pakalpojumi;

4.5.2. datu plūsmā starp lokālo datortīklu un ārējo datortīklu atjauj tikai tos pakalpojumus, kas ir nepieciešami Organizācijas funkciju izpildei, šim nolūkam lieto ugunsmūra sistēmu;

4.5.3. TR turētājs regulāri pārbauda visu ārējo savienojumu eksistenci un pārliecinās, ka pastāv tikai tie savienojumi, kuri atbilst Organizācijas darbības vajadzībām un ka darbojas rezerves savienojumi;

4.5.4. pieslēgšanos Organizācijas informācijas sistēmām no loģiski attālas vietas aizsargā, lietojot kriptogrāfijas līdzekļus kopā ar lietotāja paroli tā, lai droši noteiktu lietotāja autentiskumu.

4.6. Organizācija pēc nepieciešamības veic papildu loģiskās aizsardzības pasākumus atkarībā no Informācijas sistēmas resursu klasifikācijas līmeņa.

4.7. Organizācija veic līdzvērtīgus loģiskās aizsardzības pasākumus klasificētiem Informācijas resursiem neatkarīgi no datu glabāšanas veida (t.sk. disketes, papīra dokumenti, audio kasetes u.tml.).

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

4.8. Organizācija sadarbībā ar ārējiem informācijas tehnoloģiju pakalpojumu sniedzējiem:
4.8.1. nosaka prasības iesaistīto personu atbildībai, pagaidu lietotāju kontu piešķiršanai, pārmaiņu pārvaldīšanai un citas Informācijas sistēmas drošības prasības;
4.8.2. saskaņojot ar informācijas turētājiem, piešķir pieejas tiesības Informācijas sistēmas resursiem ārējiem informācijas tehnoloģiju pakalpojumu sniedzējiem tikai to pienākumu veikšanai nepieciešamajā apjomā;
4.8.3. nosaka informācijas izpaušanas ierobežojumus.

4.9. Ja Organizācija izvēlas Informācijas sistēmas uzturēšanu uzticēt ārējam pakalpojumu sniedzējam, tam jānodrošina Informācijas sistēmas drošības līmenis, kas nav zemāks par šajā kārtībā noteikto. Organizācija iepazīstina ārējo pakalpojumu sniedzēju ar šajā kārtībā noteiktajām Informācijas sistēmas drošības prasībām.

5. Informācijas sistēmas izstrāde, iegāde un pārmaiņu pārvaldīšana

5.1. Veicot Informācijas sistēmas izstrādes, iegādes, ieviešanas un pārmaiņu pārvaldīšanas procesu, Organizācija ievēro un atbild par Informācijas sistēmas drošības prasību ievērošanu neatkarīgi no tā, vai šos procesus veic pats Organizācijas vai ārējais izstrādātājs un piegādātājs. Tas pats jāievēro, arī veicot būtiskas izmaiņas datortīkla ārējo pieslēgumu konfigurācijā.

5.2. Organizācija nosaka Informācijas sistēmas izstrādes, iegādes, ieviešanas un pārmaiņu pārvaldīšanas procesus iekšējos normatīvos aktos un dokumentē to gaitu.

5.3. Informācijas sistēmas izstrādes uzsākšana:
5.3.1. Organizācija nosaka par Informācijas sistēmas projektu atbildīgās personas, t.sk. arī saskaņā ar šiem noteikumiem nosaka izstrādājamās Informācijas sistēmas informācijas resursu turētāju un TR turētāju;
5.3.2. atbildīgās personas veic Informācijas sistēmas projekta un to Informācijas sistēmu, kuru darbību var ietekmēt jaunā Informācijas sistēma, risku analīzi, kā ari nosaka Informācijas sistēmas drošības prasības un risku ierobežošanas pasākumus;
5.3.3. izstrādājamās Informācijas sistēmas informācijas resursu turētājs un TR turētājs veic drošības prasību noteikšanu šai Informācijas sistēmai.

5.4. Informācijas sistēmas izstrāde:
5.4.1. informācijas sistēmas izstrādes videi ir jāatbilst drošības prasībām, un to nodala no lietošanas vides;
5.4.2. pieejas tiesības Informācijas sistēmas izstrādes videi nosaka atbilstoši projektā iesaistīto personu pienākumiem;
5.4.3. katrai Informācijas sistēmai ir jābūt dokumentētai. Dokumentāciju glabā un lieto atbilstoši šīs dokumentācijas klasifikācijas līmenim.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

Dokumentācijai nodrošina rezerves kopijas, kuras glabā pēc līdzīgiem nosacījumiem kā citu datu rezerves kopijas;

5.4.4. dokumentācijā iekļauj nepieciešamo informācijas apjomu, lai varētu kvalitatīvi veikt Informācijas sistēmas lietošanu, uzturēšanu un pārmaiņu pārvaldīšanu.

5.5. Informācijas sistēmas testēšana:

5.5.1. pirms Informācijas sistēmas ieviešanas Organizācija veic Informācijas sistēmas darbības funkcionalitātes un drošības atbilstības noteiktajām prasībām pārbaudi;

5.5.2. Organizācija nodala Informācijas sistēmas testa vidi no izstrādes un lietošanas vides;

5.5.3. testos piedalās personas, kas ir noteikušas funkcionalitātes un drošības prasības, informācijas resursu turētāji un lietotāji;

5.5.4. pamatojoties uz testu rezultātiem, Organizācija nodrošina Informācijas sistēmas koriģēšanu vai uzsāk tās ieviešanu.

5.6. Informācijas sistēmas ieviešana:

5.6.1. pirms Informācijas sistēmas ieviešanas ir jāsaņem to informācijas resursu turētāju atļauja, kuru Informācijas sistēmas tiks ietekmēti, lietojot jauno Informācijas sistēmu;

5.6.2. pirms Informācijas sistēmas nodošanas lietošanai Organizācija veic darbinieku apmācību un citus pasākumus, lai nodrošinātu darbinieku izpratni par Informācijas sistēmas lietošanu, aizsardzības pasākumiem un to nozīmīgumu;

5.6.3. ieviešot Informācijas sistēmu, tajā nedrīkst būt testētāju lietotāja kodi un testēšanas datu faili;

5.6.4. Organizācija nodrošina, lai tiktu saglabāti tam pieejamie ieviestās Informācijas sistēmas pirmkodi.

5.7. Informācijas sistēmas pārmaiņu pārvaldīšana:

5.7.1. Informācijas sistēmas pārmaiņas tiek veiktas tikai ar visu saistīto informācijas resursu turētāju atļauju;

5.7.2. Informācijas sistēmas pārmaiņas izdara, ievērojot šīs kārtības 2.-5. punkta prasības;

5.7.3. Organizācija identificē visus informācijas resursus un tehnoloģiskos resursus, kurus ietekmē pārmaiņas;

5.7.4. Organizācija analizē, kā pārmaiņas ietekmēs esošos informācijas sistēmas drošības pasākumus un vai pārmaiņu rezultātā nesamazināsies informācijas sistēmas drošības līmenis;

5.7.5. Organizācija veic informācijas sistēmas dokumentācijas papildināšanu;

5.7.6. Organizācija uztur visu pārmaiņu reģistrācijas žurnālu;

5.7.7. Organizācija veido un uztur informācijas sistēmas versiju bibliotēku, lai būtu iespēja uzstādīt programmas iepriekšējo versiju, ja jaunā, mainītā versija nav apmierinoša;

5.7.8. pirms pārmaiņu ieviešanas veido rezerves kopijas tām informācijas sistēmām, kuras var ietekmēt pārmaiņas;

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

5.7.9. pēc pārmaiņu ieviešanas Organizācija pārliecinās, vai informācijas sistēmas pārmaiņu rezultātā ir saglabāta datu integritāte un informācijas sistēmas drošības līmenis;

5.7.10. Organizācija izstrādā noteikumus par darbībām ārkārtas (neplānotu) pārmaiņu apstākļos un nosaka, kas ir tiesīgs pieņemt lēmumu par ārkārtas pārmaiņām. Jāveic pasākumi, lai samazinātu nepieciešamību veikt ārkārtas pārmaiņas. ārkārtas pārmaiņām veido auditācijas pierakstus.

5.8. Informācijas sistēmas lietošanas izbeigšana:

5.8.1. likvidējot informācijas sistēmu, nododot to citai personai, t.sk. gadījumos, kad Organizācija pārtrauc kādu darbības veidu, kuru nodrošina šī Informācijas sistēma, Organizācija veic nepieciešamos drošības pasākumus;

5.8.2. likvidējot informācijas sistēmu, Organizācija veic risku analīzi, kurā izvērtē iespējamo apdraudējumu citām Informācijas sistēmām un Organizācijai kopumā;

5.8.3. Organizācijai ir nepieciešams pieņemt lēmumu par informācijas sistēmas lietošanas izbeigšanu, nosakot turpmākās darbības ar informācijas sistēmu - pilnīga likvidēšana vai glabāšana arhīvā;

5.8.4. ja informācijas sistēmu pilnībā likvidē, Organizācija nodrošina informācijas sistēmā ietilpstošo informācijas resursu likvidēšanu saskaņā ar šīs kārtības 5. punktu;

5.8.5. ja informācijas sistēmu ievieto arhīvā, Organizācija nodrošina noteikto informācijas sistēmas drošības līmeni un likvidē lietošanas tiesības, kuras var atjaunot vēsturisko datu caurskatīšanai ar atbildīgās amatpersonas lēmumu.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

Pielikums Nr.5
IS lietošanas noteikumu paraugs

IS lietošanas noteikumi

1. Vispārīgie jautājumi

1.1. Noteikumi nosaka Organizācijas informācijas sistēmas (turpmāk – IS) drošības organizatoriskās un tehniskās prasības, kārtību, kādā ierēdņi un darbinieki (turpmāk – IS lietotāji) lieto IS resursus, un IS administratora tiesības un pienākumus.

1.2. Noteikumi attiecas uz tehnoloģiskajiem resursiem, informācijas sistēmu vai lietojumu programmatūru un informāciju, tajā skaitā saistībā ar personas datiem, kas tiek saņemta, sūtīta, pārsūtīta, kopēta, uzglabāta, apstrādāta un izdrukāta izmantojot Organizācija informācijas sistēmu.

1.3. IS lietotāji pēc iepazīšanās ar šiem noteikumiem paraksta apliecinājumu (pielikums) par šo noteikumu prasību ievērošanu.

1.4. Personālvadības nodaļa nodrošina, lai Organizācijas ierēdņi un darbinieki parakstītu apliecinājumu. Apliecinājums par šo noteikumu prasību ievērošanu atrodas katra Organizācijas ierēdņa un darbinieka personīgajā lietā.

1.5. IS lietotāja darba vieta tiek aprīkota ar informācijas sistēmas resursiem saskaņā ar struktūrvienības vadītāja pieprasījumu. Katram IS lietotājam tiek piešķirts lietotājvārds (identifikators) un parole, kā arī noteiktas piekļuves tiesības. IS lietotājs ir atbildīgs par piešķirtā lietotājvārda (identifikatora) un paroles lietošanu, saglabāšanu un neizpaušanu.

1.6. Darba pienākumu pildīšanai Organizācijas IS lietotājiem ir pieejams internets un e-pasts.

1.7. Aizliegts piekļūt tiem IS resursiem, kuriem nav piešķirtas piekļuves tiesības.

2. Datu glabāšana un aizsardzība

2.1. Katrai struktūrvienībai darba informācijas glabāšanai tiek piešķirts noteikta apjoma katalogs uz failu servera. Par šī kataloga saturu ir atbildīga attiecīgā struktūrvienība.

2.2. Veidojot faila vai kataloga nosaukumus, IS lietotājs var izmantot:

2.2.1. latīņu alfabēta burtus bez garumzīmēm un mīkstinājuma zīmēm;

2.2.2. ciparus.

2.3. Veidojot faila vai kataloga nosaukumus, IS lietotājs nedrīkst izmantot perifērijas ierīču un portu apzīmējumus (PRN; LPT1; LPT2 utt.; COM1; COM2 utt.; CON; NUL; AUX).

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

2.4. Katram IS lietotājam darba informācijas apmaiņai vai īslaicīgai datu uzglabāšanai failu serverī ir pieejams koplietošanas katalogs. Datnes, kas gada laikā nav izmantotas, var tikt izdzēstas.

2.5. Visiem Organizācija informatīvajiem resursiem IS administrators regulāri veido rezerves kopijas:

2.5.1. e-pastam - vienu reizi mēnesī un uzglabā 6 mēnešus;

2.5.2. failu servera katalogos uzkrātajai informācijai - vienu reizi mēnesī un uzglabā 6 mēnešus;

2.5.3. grāmatvedības uzskaites sistēmai - vienu reizi nedēļā un uzglabā 3 mēnešus, kā arī katra mēneša pirmās nedēļas kopiju uzglabā 18 mēnešus.

2.6. Pēc rezerves kopijas izgatavošanas IS administrators to nodod Administratīvajam departamentam glabāšanā.

2.7. IS lietotāju datoru (turpmāk - darba staciju) diskos uzkrātajai informācijai rezerves kopijas netiek veidotas. IS lietotājs, ja nepieciešams, veido datņu rezerves kopijas savas struktūrvienības katalogā.

2.8. Darba stacijas un serveri tiek aizsargāti ar pretvīrusu programmām. Darba staciju vīrusu aprakstu datu bāzes tiek atjaunotas reizi dienā.

3. E-pasta lietošana

3.1. Viena e-pasta sūtījuma apjoms nedrīkst pārsniegt 2 MB. Aizliegts atkārtoti sūtīt e-pasta vēstuli, ja ir saņemts paziņojums, ka adresāts nevar saņemt sūtījumu e-pasta servera limita pārsniegšanas dēļ.

3.2. Aizliegts atvērt neskaidras izcelsmes e-pasta sūtījumus (piemēram, īpatnēji temati laukā "Subject", pievienota nezināma formāta datne vai izpildāmā datne, interneta saites vēstules saturā), it īpaši, ja par bīstamo datņu veidiem saņemts brīdinājums no IS administratora. Par šādiem e-pasta sūtījumiem nekavējoties jāziņo IS administratoram.

3.3. Aizliegts e-pasta ziņojumam pievienot izpildāmās datnes (piemēram, *.exe, *.com, *.shs, *.vbs).

3.4. E-pasta lietotājs, regulāri nodzēšot nevajadzīgo informāciju, kontrolē, lai viņa pastkastes kopapjoms serverī nepārsniegtu 200 MB. IS administrators drīkst bloķēt lietotāja e-pasta kontu, ja pastkastes kopapjoms pārsniedz minēto apjomu.

4. IS lietotāja identifikācija un autentiskums

4.1. IS lietotājs ir atbildīgs par darbībām, kas tiek veiktas, izmantojot viņa lietotājvārdu (identifikatoru). IS lietotāja autentiskumu nosaka, lai pārliecinātos, ka lietotājvārda (identifikatora) izmantotājs ir sankcionētais tā turētājs. Autentiskuma noteikšanai tiek izmantotas paroles. Pēc lietotājvārda

(identifikatora) un paroles ievadīšanas IS lietotājs var izmantot informācijas sistēmas resursu atbilstoši noteiktajām piekļuves tiesībām.

4.2. Parole sastāv no burtu un zīmju kombinācijas un tās garums nedrīkst būt īsāks par astoņiem simboliem. Nav ieteicams par paroli izmantot personu identificējošus datus (piemēram, personas datus, automašīnas numuru, radu vārdus vai uzvārdus, vārdus, kas saistīti ar darbavietu vai kas bieži tiek tajā lietoti).

4.3. IS lietotājs paroli maina vismaz reizi trijos mēnešos. Izveidojot jaunu paroli, aizliegts lietot iepriekšējās trīs izmantotās paroles.

4.4. IS lietotājam parole ir jāiegaumē. Rakstiskā veidā paroles atļauts glabāt tikai aizslēgtā seifā.

4.5. IS administrators nodrošina:

4.5.1. automātisku paroles maiņas pieprasījumu, lietotājam pirmo reizi reģistrējoties tīklā;

4.5.2. automātisku paroles maiņas pieprasījumu ik pēc trim mēnešiem;

4.5.3. trīs iepriekšējo paroļu atkārtotas izmantošanas bloķēšanu.

4.6. Pieļaujamais pēc kārtas nepareizi ievadīto paroļu skaits ir pieci. Pēc piecām nepareizi ievadītām parolēm pieeja sistēmai tiek bloķēta, un to atjauno tikai IS administrators.

4.7. Ja radušās aizdomas, ka paroli uzzinājusi cita persona, IS lietotājs to nekavējoties nomaina un par incidentu ziņo IS administratoram.

4.8. Aizliegts mēģināt uzzināt citu lietotāju paroles, izņemot gadījumus, kad tas ir nepieciešams IS administratoram viņa tiešo pienākumu veikšanai. Pēc minēto darbu pabeigšanas IS lietotājs paroli nomaina.

4.9. IS lietotājam izbeidzot darba attiecības ar Organizāciju, visas piekļuves tiesības Organizācija informācijas sistēmas resursiem IS administrators anulē.

5. IS lietotāju atbildība un pienākumi

5.1. IS lietotāji drīkst izmantot piešķirtos informācijas sistēmas resursus tikai darba pienākumu veikšanai.

5.2. Izmantojot informācijas sistēmas resursus, IS lietotāju pienākums ir:

5.2.1. nekavējoties ziņot IS administratoram (darba laikā pa tālruni 7123456, ārpus darba laika ziņojumus nosūtīt pa e-pastu admin@organizacija..lv) šādos gadījumos:

5.2.1.1. ja radušās aizdomas, ka lietotāja paroli uzzinājusi cita persona;

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

5.2.1.2. saņemot neskaidras izcelsmes e-pasta sūtījumus (piemēram, nepazīstami korespondenti, īpatnēji norādīti vēstuļu temati);

5.2.1.3. ja radušās aizdomas, ka dators inficēts ar vīrusu, kā arī izslēgt datoru;

5.2.1.4. ja radušās aizdomas par datortehnikas bojājumu, kā arī nekavējoties izslēgt bojāto tehniku;

5.2.1.5. pamanot novirzes datora vai informācijas sistēmas darbībā;

5.2.1.6. ja nepieciešams mainīt datortehnikas izvietojumu;

5.2.1.7. izlasīt IS administratora sūtītos ziņojumus un laikus izpildīt norādītās darbības;

5.2.1.8. iepazīties ar koplietošanas katalogā ievietotajām instrukcijām un ieteikumiem;

5.2.1.9. regulāri izdzēst darbam nevajadzīgos e-pasta sūtījumus;

5.2.1.10. nepārtraukt pretvīrusu programmas atjaunināšanas procesu;

5.2.1.11. sekot, lai uz datora obligāti būtu aktivizēts ekrāna saudzētājs ar paroles aizsardzību. Ekrāna saudzētājam automātiski jāaktivizējas, ja piecu minūšu laikā lietotājs nav veicis nekādas darbības.

5.3. IS lietotājiem aizliegts:

5.3.1. izmantot IS resursus, lai izplatītu vai uzglabātu ar darbu nesaistītu informāciju (piemēram, komerciāla vai personīga rakstura sludinājumus, uzsaukumus, reklāmas, destruktīvas programmas, spēles);

5.3.2. veikt darbības, kas nevajadzīgi noslogo informācijas sistēmas resursus, neņemot vērā citu informācijas sistēmas lietotāju vajadzības (piemēram, pārmērīgi izmantot internetu, drukāt nevajadzīgi daudz dokumentu kopiju, atstāt atvērtas uz failu servera esošās datnes, kuras nav nepieciešamas darbam);

5.3.3. veikt internetā pieejamo programmu lejupielādi;

5.3.4. patstāvīgi instalēt datoros programmatūru;

5.3.5. nesankcionēti nodot programmatūras un darba datu kopijas trešajai personai;

5.3.6. bez saskaņošanas ar Organizācija vadītāju veidot sev vai piešķirt citiem lietotājiem attālinātu pieeju savas darba stacijas, portatīvā datora vai servera resursiem;

5.3.7. patstāvīgi mainīt datora konfigurāciju, pārvietot stacionāro biroja tehniku un novērst jebkurus datortehnikas bojājumus;

5.3.8. datoru nepārtrauktās energoapgādes sistēmai pieslēgt jebkuras elektroierīces, izņemot datorus, monitorus un drukas ierīces.

5.4. IS lietotājs ir atbildīgs par zaudējumiem, kas radušies šajos noteikumos noteikto prasību neievērošanas dēļ.

5.5. Administratīvais departaments nodrošina jauno IS lietotāju iepazīstināšanu pirms darbu uzsākšanas:

5.5.1. ar darba aizsardzības instrukciju darbam ar datortehniku (pret parakstu darba aizsardzības instruktāžas žurnālā);

5.5.2. ar viņam piešķirto datortehniku un biroja tehniku.

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

6. IS administratora atbildība un pienākumi

6.1. IS administrators:

6.1.1. pēc Administratīvā departamenta rakstiskas informācijas izveido, modificē un likvidē IS lietotāju identifikatorus (kontus) un piešķir attiecīgās tiesības;

6.1.2. ja nepieciešams, ierobežo failu servera diska vai kāda tā kataloga apjomu, par to informējot visus šī diska vai kataloga lietotājus ar e-pastu;

6.1.3. kontrolē, lai informācijas sistēmas resursu lietotāji ievērotu šajos noteikumos noteiktos paroļu maiņas nosacījumus.

6.2. IS administrators ir tiesīgs:

6.2.1. brīvdienās un ārpus oficiālā darba laika (17.00–8.30) atslēgt informācijas sistēmas resursus, lai veiktu uzturēšanas darbus, 3 darba dienas iepriekš par to brīdinot IS lietotājus;

6.2.2. atslēgt informācijas sistēmas resursus un apturēt sistēmu darbu arī darba laikā, ja notikusi avārija (ja iespējams, iepriekš par to brīdinot lietotājus pa telefonu un e-pastu).

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

Pielikums Nr.6
Sistēmu darbības nepārtrauktības un atjaunošanas plāna paraugs

Sistēmu darbības nepārtrauktības un atjaunošanas plāns

1. Informācijas sistēmu darbības nepārtrauktības un atjaunošanas vadības process

1.1. Informācijas sistēmu darbības nepārtrauktības un atjaunošanas vadības process satur pasākumu kopumu problēmu novēršanai vai preventīvas darbības, kuras samazina iespējamos riskus.
1.2. Informācijas sistēmu darbības nepārtrauktības un atjaunošanas plāna izstrādi, uzturēšanu un atjaunošanu veic tehnoloģisko resursu turētājs.
1.3. Tehnoloģisko resursu turētājs ir atbildīgs par problēmu pieteikšanas procedūras izstrādi, uzturēšanu un atjaunošanu.
1.4. Informācijas sistēmu darbības nepārtrauktības un atjaunošanas plānā tiek noteikts:
   1.4.1. avāriju novēršanas procedūru turētāji;
   1.4.2. avāriju novēršanas kārtība un kontrollaiks.

2. Organizācijas tehnoloģisko resursu apraksts

2.1. Lokālais datortīkls un komutācijas iekārtas

2.1.1. Organizācijas datortīkla komutāciju nodrošina sekojošas iekārtas:

Nosaukums	Atrašanās vieta

Ja kāda no tīkla komutācijas iekārtām ir izgājusi no ierindas, datortīkla darbība ir jāatjauno [stundu skaits] stundu laikā.

2.1.2. Organizācijas tīklam ir pieslēgti vairāki tīkla printeri:

Nosaukums	Atrašanās vieta

Ja kāds no tīkla printeriem ir izgājis no ierindas, darbiniekam ir jāspēj turpināt darbu [stundu skaits] stundu laikā.

2.2. Interneta pieslēgums

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

[Šajā sadaļā tiek nodefinēts un aprakstīts Organizācijas Interneta pieslēgumi, ugunsmūru raksturojums]

Ja Interneta pieslēgums nav pieejams, tā darbība ir jāatjauno [stundu skaits] stundu laikā.

2.3.Darba stacijas

[Šajā sadaļā tiek nodefinēts un aprakstīts kādas darba stacijas ir Organizācijas pārziņa – specifikācija, programmatūra]

Ja darbinieka dators ir izgājis no ierindas, darbiniekam ir jāspēj turpināt darbu [stundu skaits] stundu laikā.

2.4.Lokālo serveru infrastruktūra

N.p.k.	Servera nosaukums	Ražo-tājs	Modelis	S/N un „Type" (IBM) vai „PartNumber" (HP)	Garantijas saistības no ražotāja puses	IP adrese	Procesors (CPU)	Atmiņa (RAM)	Cietais disks (HDD) un RAID	Operētāj-sistēma
1										
2										
3										

2.5.Lietojumprogrammas un informācijas sistēmas

[Šajā nodaļā ir aprakstītas lietojumprogrammas un informācijas sistēmas, kā arī to atjaunošanas laiki]

N. p.k	Servera nosaukums	Operētājsistēma	Informācijas sistēmas					Nepieciešamais atjaušanas laiks.
1								

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

2								
3								

2.6.Datu rezerves kopēšana

[Šajā nodaļā tiek aprakstīts, kā un cik bieži tiek veiktas datu rezerves kopijas]

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

3. Organizācija tehnoloģisko resursu darbības atjaunošana

[Šajā sadaļā ir aprakstītas uzņēmuma infrastruktūras atjaunošanas soļi, kā rīkoties, ja iestājās kāds no uzskaitītajiem negadījumiem, piemēram:
a) iekārta pilnībā iziet no ierindas;
b) informācijas sistēmas dati ir izdzēsti.
c) U.c. negadījums]

3.1.Lokālais datortīkls un komutāciju iekārtas

Nosaukums	Atrašanās vieta	Atjaunošanas soļi	Atbildīgais

3.2.Interneta pieslēgums

Nosaukums	Atrašanās vieta	Atjaunošanas soļi	Atbildīgais

3.3.Darba stacijas

Nosaukums	Atrašanās vieta	Atjaunošanas soļi	Atbildīgais

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

3.4.Lokālo serveru infrastruktūra

N. p.k	Nosaukums un atrašanās vieta	Informācijas sistēmas					Atjaunošanas soļi	Atbildīgais
1								
2								

3.5.Ārpakalpojumu sniedzēja datu centrā izvietotās iekārtas

N. p.k	Nosaukums un atrašanās vieta	Informācijas sistēmas		Atjaunošanas soļi	Atbildīgais

3.6.Lietojumprogrammas un informācijas sistēmas

Atjaunošanas soļi aprakstīti iepriekšējās divās nodaļās (3.4. Lokālo serveru infrastruktūra un 3.5.Ārpakalpojumu sniedzēja datu centrā izvietotās iekārtas).

3.7.Datu rezerves atjaunošana

[Šajā nodaļā tiek aprakstīts datu atjaunošanas process, kādus datus un IS kādā veidā atjauno, cik senus datus var atjaunot, atbildīgos]

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"

4. Valsts informācijas sistēmas [VIS nosaukums] infrastruktūra

[Šajā nodaļā tiek atsevišķi aprakstīta katras Valsts informācijas sistēmas darbības nepārtrauktības un IS atjaunošanas plānošana]

4.1.[VIS nosaukums] tehnoloģisko resursu izmitināšana un uzturēšana

Vārds, uzvārds	amats	uzņēmums	tālrunis	e-pasts

4.2.[VIS nosaukums] pieejamības prasības

4.3.[VIS nosaukums] sistēmas darbības nepārtrauktības un atjaunošanas plāns

Īpašu uzdevumu ministre
elektroniskās pārvaldes lietās I.Gudele

Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāta vadītājs	Juridiskās nodaļas vadītāja p.i.	Par kontroli atbildīgā amatpersona	Atbildīgā amatpersona
V.Krievāns	I.Burmistrovs	M.Plaude	J.Timermanis

04.04.2008. 8:30
19031
I.Elme
inga.elme@eps.gov.lv

Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas; Pielikums „Informācijas sistēmu drošības pārvaldības vadlīnijas" informatīvajam ziņojumam „Par informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijām labas prakses risinājumiem informācijas sistēmu drošības apdraudējumu gadījumā"