Pašvaldību un valsts iestāžu Informācijas tehnoloģiju drošības noteikumu vadlīnijas

1. **Vispārīgie jautājumi**
   1.1. Pašvaldību un valsts iestāžu Informācijas tehnoloģiju (IT) drošības noteikumi (turpmāk – noteikumi) izstrādāti saskaņā ar Informācijas tehnoloģiju drošības likumu.
   1.2. Noteikumi domāti valsts un pašvaldību institūcijām.
   1.3. Noteikumi nosaka kārtību kādā valsts un pašvaldības institūcijas (turpmāk – iestādes) nodrošina tai piederošo informācijas un tehnisko resursu (turpmāk – resursu) aizsardzību.
   1.4. Noteikumi ietver minimālās prasības, iestāde var lietot stingrākus drošības pasākumus.
   1.5. Noteikumu mērķis ir
      1.5.1. apliecināt iestādes vadības apņemšanos nodrošināt iestādē resursu drošību, lai nodrošinātu to integritāti, pieejamību un konfidencialitāti,
      1.5.2. nodrošināt iestādē vienādu un sistemātisku pieeju informācijas tehnoloģiju drošības jautājumu risināšanā,
      1.5.3. panākt iestādes darbinieku izpratni par nepieciešamajiem informācijas tehnoloģiju drošības jautājumiem,
      1.5.4. būt par pamatu nepieciešamo procedūru, instrukciju un citu nepieciešamo drošības dokumentu izstrādē un ieviešanā.
   1.6. Noteikumu ievērošana ir obligāta visiem iestādes darbiniekiem.

2. **Noteikumos lietotie termini**
   2.1. Informācijas resursi – sistēmprogrammas, lietojumprogrammas, sistēmu un datu faili un cita informācija, ko izmanto informācijas apstrādei, pārraidei, glabāšanai un citu funkciju veikšanai.
   2.2. Tehniskie resursi – datori, tīkla aparatūra, komunikāciju līnijas un citi tehniskie līdzekļi ko izmanto informācijas apstrādei, pārraidei un glabāšanai.
   2.3. Informācijas sistēma (IS) – informācijas un tehnisko resursu kopums.
   2.4. Resursu turētājs – iestādes vadītājs, vai ar vadītāja rīkojumu iecelts **iestādes** darbinieks, kurš atbild par IT drošības pārvaldību.
   2.5. IT drošības pārzinis – resursu turētājs vai ārpakalpojuma sniedzējs, kurš nodrošina IT drošības pārvaldību. *(likuma izpratnē atbildīgā persona)*
   2.6. Resursu aizbildnis – resursu turētāja vai ārpakalpojuma sniedzēja norīkota persona, kura atbild par resursu funkcionēšanu un/vai saturu.
   2.7. Resursu lietotājs – iestādes darbinieks, kurš izpilda noteiktus pienākumus, kuriem atbilstoši tiek piešķirtas tiesības lietot noteiktus resursus.
   2.8. Informācijas integritāte – raksturo, cik lielā mērā informācija ir pilnīga, patiesa, precīza un aktuāla.
   2.9. Informācijas pieejamība – raksturo to, vai lietotāji var piekļūt nepieciešamajai informācijai ne vēlāk, kā noteiktā laikā pēc informācijas pieprasīšanas brīža.
   2.10. Informācijas konfidencialitāte – raksturo to, cik lielā mērā informācija ir pieejama tikai šīs informācijas saņemšanai paredzētajiem lietotājiem.
   2.11. Informācijas vērtība – informācijas nozīmīgums iestādes funkciju veikšanai.
   2.12. Drošības incidents – ir kaitīgs notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas resursu integritāte, pieejamība vai konfidencialitāte.

2.13. Auditācijas pieraksti - analīzei pieejams resursu veikto darbību (piekļūšana, datu ievade, mainīšana, dzēšana, izvade) atspoguļojums elektroniskas informācijas veidā.
2.14. Drošības dokumenti – dokumentu kopums, kas apraksta iestādes resursu lietošanas kārtību.
2.15. Risku pārvaldīšana – Informācijas sistēmu risku identificēšana, novērtēšana, samazināšana un kontrolēšana, kuras ietvaros tiek veikta informācijas sistēmu risku ierobežošana līdz iestādei pieņemamam līmenim.
2.16. Ārpakalpojuma sniedzējs - trešā persona, kas uz līguma pamata nodrošina iestādes IT drošības pārvaldību vai citas funkcijas.

3. Ārpakalpojuma pārvaldība

3.1. Iestādes IT drošības pārvaldību, attīstību vai drošību var nodrošināt ārpakalpojuma sniedzējs.
3.2. Iestāde veic ārpakalpojumu uzraudzību. Ārpakalpojuma saņemšana uzliek atbildību par ārpakalpojuma sniedzēja veikumu tādā pašā mērā kā par savu.
3.3. Ārpakalpojuma līgumā jāiekļauj IT drošības likumā noteiktie pienākumi.

4. Resursu pārvaldība

4.1. Resursu turētājs norīko **IT drošības pārzini**, kura pienākums ir:
4.1.1. organizēt iestādes IT drošības noteikumu izstrādi,
4.1.2. nodrošināt izmaiņu pārvaldību,
4.1.3. uzturēt (apstiprināt) aktuālas izmaiņas drošības dokumentos.
4.2. IT drošības pārzinis norīko visiem resursiem vienu vai pēc nepieciešamības atsevišķiem **resursiem aizbildni**, kura pienākums ir:
4.2.1. nodrošināt resursu normālu (pareizu) darbību,
4.2.2. nodrošināt resursu lietotāju pārvaldību,
4.2.3. pildīt citus iestādes IT drošības noteikumos uzliktos pienākumus,
4.2.4. veikt kopā ar resursu turētāju risku aktualizāciju.
4.3. **Resursu lietotāja** pienākumi
4.3.1. Ievērot iestādē apstiprinātos IT drošības noteikumus.

5. Informācijas resursu klasifikācija

5.1. Iestāde veic visu informācijas resursu klasifikāciju ar mērķi novērtēt resursa saturošās informācijas nozīmību pēc konfidencialitātes, vērtības un pieejamības. Informācija var būt **publiska** un **ierobežotas** pieejamības.
5.1.1. **Informācijas konfidencialitātes** līmeni nosaka izejot no kaitējuma, kas varētu tikt nodarīts iestādei ja informācijai piekļūst personas, kas nav pilnvarotas.
5.1.1.1. **Publiska informācija (P)** – nav svarīga konfidencialitātes aspektā, tā ir brīvi pieejama iestādes darbiniekiem, jebkurai personai vai organizācijai, kas to ir pieprasījusi. Šīs informācijas izplatīšana neietekmē iestādi negatīvā veidā.
5.1.1.2.**Ierobežotas pieejamības informācija (I)** – ir svarīga konfidencialitātes aspektā, tās pazīmes noteiktas Informācijas atklātības likuma 5., 6., un 7. pantā. Šī informācija ir pieejama tikai iestādes darbiniekiem, kuriem ir piešķirtas šādas tiesības.

5.1.2. **Informācijas vērtības** līmeni nosaka atkarībā no kaitējuma, kas varētu būt nodarīts iestādei, ja netiktu nodrošināta informācijas resursu integritāte, pēc šādas skalas:

5.1.2.1.V1 - augstas vērtības informācija,

5.1.2.2. V2 - vidēja vērtības informācija,

5.1.2.3. V3 - zema vērtības informācija.

5.1.3. **Informācijas pieejamības** līmeņus nosaka atkarībā no iestādes darbības jomas, ņemot vērā kaitējumu kas varētu tikt nodarīts iestādei vai tās klientiem, ja netiktu nodrošināta resursu pieejamība. Informācijas pieejamības līmeni nosaka pēc šādas skalas:

5.1.3.1. P1- informācija pieejama 24 stundas diennaktī, 7 dienas nedēļā,

5.1.3.2. P2 - informācija pieejama iestādes darba laikā.

5.2. Resursi, kuriem nav piešķirts neviens no konfidencialitātes, vērtības vai pieejamības līmeņiem tiek uzskatīti par **neklasificētiem**. *(tiem nav jāveic riska analīze)*

5.3. Informācijas klasifikācijas tabula (V- informācijas vērtība, K – informācijas konfidencialitāte, P- informācijas pieejamība)

Nr.	Resurss	Informācijas sistēma	Informācijas vērtība (V)	Informācijas konfidencialitāte (K)	Informācijas pieejamība (P)
1	2	3	4	5	6

6. Riska analīze

6.1. Risku analīzi veic ar mērķi izvērtēt resursu apdraudējumus un iespējamās sekas apdraudējuma iestāšanās gadījumā.

6.2. Risku pārvaldīšanu veic ņemot vērā informācijas klasifikāciju un risku pārvaldīšanas pasākumus nosaka samērojot drošības pasākumu izmaksas ar iespējamiem zaudējumiem.

6.3. Atbildīgais par risku analīzes veikšanu ir resursu turētājs, kurš organizē risku analīzi, piesaistot struktūrvienību vadītājus.

6.4. Struktūrvienību vadītāju pienākums ir nodrošināt pēc iespējas pilnīgu un precīzu risku identificēšanu un novērtēšanu.

6.5. Risku analīzi veic ne retāk kā vienu reizi gadā.

6.6. Resursu apdraudējuma varbūtību nosaka izmantojot skalu:

6.6.1. A1 – maza apdraudējuma varbūtība – vērtība 1,

6.6.2. A2 – vidēja apdraudējuma varbūtība – vērtība 2,

6.6.3. A3 – liela apdraudējuma varbūtība – vērtība 3.

6.7. Resursiem radīto kaitējumu no katra apdraudējuma nosaka izmantojot skalu:

6.7.1. RK1 – mazs kaitējums – vērtība 1,

6.7.2. RK2 – vidējs kaitējums – vērtība 2,
6.7.3. RK3 – liels kaitējums – vērtība 3.
6.8. Risku aprēķināšanu veic - risks= (apdraudējuma varbūtība x resursa apdraudējuma kaitējums). R=AVxRK .
6.9. Tabulā apkopo iespējamos resursu apdraudējumus, atzīmējot ietekmi uz (K- konfidencialitāti, P – pieejamību, I – integritāti, AV - apdraudējuma varbūtību, RK - resursiem radīto kaitējumu , R - aprēķināto risku).

Nr.	Apdraudējums	Apraksts	K	P	I	AV	RK	R
1	2	3	4	5	6	7	8	9 (7x8)

7. Riska novērtējuma skala
7.1. 1 – zems risks, ieteicams sekot līdz izmaiņām,
7.2. 2,3,4 –vidējs risks, ieteicams veikt drošības pasākumus,
7.3. 6 – augsts risks, drošības pasākumus ieteicams veikt pēc iespējas ātrāk.
7.4. 9 – ļoti augsts risks, drošības pasākumi jāveic nekavējoši

8. Risku mazināšanas pasākumu tabula. (izvēlamies kam drošības risks ir 6 vai vairāk no risku novērtējuma tabulas)

Nr	Drauds	Papildus drošības pasākums	Ieviešanas termiņš	Izmaksas	Izpildītājs
1	2	3	4	5	6

9. Izmaiņu pārvaldība
9.1. IT drošības pārzinis:
9.1.1. ne retāk, kā reizi gadā veic un dokumentē,
9.1.1.1. informācijas resursu klasifikāciju,
9.1.1.2. resursu risku analīzi,
9.1.1.3. organizē atklāto trūkumu novēršanu.
9.1.2. pēc nepieciešamības organizē iestādes darbinieku apmācību,
9.1.3. apstiprina un atceļ lietotājiem pieejas tiesības resursiem, ko fiksē resursu pieejas tiesību žurnālā,
9.1.4. nodrošina datu rezerves kopiju veidošanu,
9.1.5. nodrošina resursu konfigurāciju pārvaldību,
9.1.6. nodrošina atsevišķu iestādei būtisku resursu pārvaldību,
9.1.7. nodrošina auditācijas pierakstu veikšanu.
9.2. veic drošības incidentu pārvaldību.

10. Drošības incidentu pārvaldība
10.1. Incidentu pārvaldību veic ar mērķi samazināt drošības incidenta ietekmi uz iestādes normālu darbību.
10.2. IT drošības pārzinis identificē drošības incidentu pēc šādiem kritērijiem:
10.2.1. notiek uzbrukums resursiem no ārpuses,

10.2.2. notiek svarīgu resursu atteice,
10.2.3. apgrūtināta iestādes normāla darbība,
10.2.4. apgrūtināta būtisku pakalpojumu sniegšana.

10.3. Drošības incidenta gadījumā IT drošības pārzinis:
10.3.1. informē Informācijas tehnoloģiju drošības incidentu novēršanas institūciju CERT.LV,
10.3.2. saglabā pierādījumus,
10.3.3. atjauno informācijas sistēmas darbību,
10.3.4. reģistrē drošības incidentu žurnālā.

11. Pielikumi

11.1. Ieteicamās prasības izmaiņu pārvaldībai.