CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Dokumentācijas sakārtošana un prasību ievērošana

Rīga, 2016.gada 18.februāris

Termini

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Sistēmas auditācijas pieraksti
- Informācijas integritāte
- Informācijas konfidencialitāte
- Informācijas pieejamība
- Drošības apdraudējums
- Drošības incidents
- Drošības nepilnība
- Lietotājs
- Sistēmas informācijas resursi
- Sistēmas tehniskie resursi
- Autentifikācija
- Autorizācija

Iesaistītās personas

- Informācijas sistēmas pārzinis
- Informācijas sistēmas turētājs
- Atbildīgās persona par informācijas tehnoloģiju drošības pārvaldību
- Informācijas resursu valdītājs
- Tehnisko resursu valdītājs

Esošā dokumentācija

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Esošās dokumentācijas inventarizācija
- Spēkā, ciktāl nav pretrunā ar MK noteikumiem
- Var paredzēt stingrākas drošības prasības
- Iespējams iekļaut jaunajā regulējumā

Dokumentu hierarhija

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Nosaukums	Piemēri
ES regulas un direktīvas	Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti
Likumi	Elektronisko dokumentu likums Informācijas tehnoloģiju drošības likums Apgrūtināto teritoriju informācijas sistēmas likums
Ministru kabineta noteikumi	Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām Kriminālprocesa informācijas sistēmas noteikumi
Standarti	ISO 27001 «Informācijas tehnoloģija. Drošības paņēmieni. Informācijas drošības pārvaldības sistēmas. Prasības»
Iekšējie normatīvie akti	Drošības politika Lietošanas noteikumi Drošības noteikumi
Procedūras/ darbību apraksts/ shēmas	Lietotāju pārvaldības procedūra Darbību apraksts rezerves kopiju testēšanai Resursu klasifikācija

Ieteikumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Vienoti termini
- Atsauces uz iekšējām procedūrām
- Maksimāli ievērot MK noteikumu tekstu
- Izmantot veselo saprātu
- Prasības ievērot pēc būtības

Prasības

Konti

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Atsevišķi administratoru konti
- Lietotāja konts piesaistīts fiziskai personai
- Konta bloķēšana pēc 5 neveiksmīgiem pieteikšanās mēģinājumiem
- Administrators izmanto daudzfaktoru autentifikāciju, pieslēdzoties ārpus iestādes

Paroles

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Parole katram lietotājam
- Minimālās sarežģītības prasības
- Šifrēšana
- Neattēlo lietotājam
- Sistēma nepiedāvā atcerēties
- Neizmanto noklusētās
- Minimālās maiņas prasības
- Atšķiras no 5 iepriekšējām

Auditācijas pieraksti

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Glabā 6 mēnešus
- Darbība un lietotāja konts vai IP adrese
- Glabā 18 mēnešus
- Glabā atsevišķi no sistēmas
- Sinhronizēts pulksteņa laiks
- Plānveida analīze

Pārējā sistēmas funkcionalitāte

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Pretvīrusu funkcionalitāte gala lietotāju iekārtām
- Sistēma darbojas ar minimāli iespējamām tiesībām
- Kļūdu paziņojumi lietotājam satur tikai minimāli nepieciešamo informāciju

Datortīkls un fiziskā drošība

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Tiek kontrolēta fiziskā piekļuve iekārtām
- Ugunsmūris katra sistēmai
- Atslēgti nevajadzīgie *Network services*

Pārējās prasības

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Visi nepieciešamie programmatūras atjauninājumi
- Testēšana neapdraudot sistēmā glabājamo informāciju
- Informācija uzglabājas tikai ES vai EEZ

Nepieciešamie dokumenti

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

	Pamata drošības sistēmai	Paaugstinātas drošības sistēmai
Sistēmas drošības politika		
Sistēmas drošības iekšējie noteikumi		
Sistēmas lietošanas noteikumi		
Sistēmas drošības riska pārvaldības plāns		
Sistēmas darbības atjaunošanas plāns		

Drošības politika

Vispārējie jautājumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Politika pamata drošības sistēmai
- Politika paaugstinātas drošības sistēmai
- Jānodrošina, ka sistēmas lietotājiem ir pieejami:
  - Drošības principi
  - Drošības risku pieņemamais līmenis
  - Drošības kritēriji

Sistēmas drošības politikas mērķi un pamatnostādnes

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

13. Sistēmas drošības politika ietver:

13.1. sistēmas drošības politikas mērķus un pamatnostādnes;

- Vadības atbalsts politikas īstenošanai
- Iestādes mērķi
- Piemēri:
  - Aizsardzība pret apdraudējumiem
  - Atbilstība normatīvo aktu prasībām

Sistēmas raksturojums un analīze drošības jomā

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

13. Sistēmas drošības politika ietver:
...
13.2. sistēmas raksturojumu un analīzi drošības jomā;

- Augsta līmeņa sistēmas apraksts
- Kādām iestādes funkcijām tā paredzēta
- Lietotāju raksturojums

Sistēmas drošības politikas uzdevumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

5. Sistēmas drošībai īsteno pasākumu kopumu, lai:
5.1. nodrošinātu informācijas pieejamību (piekļuvi informācijai noteiktā laikposmā pēc informācijas pieprasīšanas);
5.2. nodrošinātu informācijas integritāti (pilnīgas un nemainītas informācijas saglabāšanu);
5.3. nodrošinātu informācijas konfidencialitāti (informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot);
5.4. aizsargātu sistēmas informācijas resursus (datnes, arī tās, kuras satur sistēmā glabājamo, apstrādājamo un sistēmas lietotājiem pieejamo informāciju, un sistēmas dokumentāciju);
5.5. aizsargātu sistēmas tehniskos resursus (datorus, programmatūru, datu nesējus, datortīkla iekārtas un citas tehniskās iekārtas, kuras nodrošina sistēmas darbību);
5.6. noteiktu sistēmas drošības apdraudējumu (ar nodomu (tīši) vai aiz neuzmanības izdarītu darbību vai notikumu, kas var izraisīt sistēmas informācijas vai tehnisko resursu izmaiņas, bojājumu, iznīcināšanu vai nonākšanu tādu personu rīcībā, kuras nav tam pilnvarotas, vai kura dēļ piekļūšana sistēmas informācijas resursiem var būt traucēta vai neiespējama);
5.7. novērtētu sistēmas drošības risku;
5.8. atklātu sistēmas drošības incidentu;
5.9. atjaunotu sistēmas darbību pēc sistēmas drošības incidenta.

- Izmantot MK noteikumos minēto
- Pielāgot iestādes vajadzībām
- Papildus uzdevumi attiecīgai sistēmai

Sistēmas drošības pārvaldības organizācijas principi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

13. Sistēmas drošības politika ietver:
..
13.3. sistēmas drošības pārvaldības organizācijas principus;

- Sistēmas drošības pārvaldības apraksts
- Pienākumu un atbildības sadalījums
- Atbildība par politikas prasību neievērošanu

Sistēmas drošības atbilstība normatīvajiem aktiem un standartiem

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

13. Sistēmas drošības politika ietver:
...
13.4. sistēmas drošības atbilstību normatīvajiem aktiem un standartiem;

- Latvijas normatīvie akti
- Eiropas Savienības normatīvie akti
- Standarti, kas ir piemērojami Sistēmas drošībai
- Standarti, kas piemērojami Sistēmas darbībai

Sistēmas drošības principi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

13. Sistēmas drošības politika ietver:
..
13.5. sistēmas drošības principus ..

- MK noteikumu tehniskās prasības
- Lietotāju konti
- Izsekojamība
- Atjauninājumi
- Fiziskā aizsardzība
- Loģiskā aizsardzība

Sistēmas drošības risku pieņemamais līmenis

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

13. Sistēmas drošības politika ietver:
..
13.5. ...sistēmas drošības risku (pieejamības, integritātes un konfidencialitātes risku) pieņemamo līmeni atbilstoši šo noteikumu 7. punktā minētajai metodikai;

- Iestādes pieeja drošības risku pārvaldīšanai
- Risku pieņemamais līmenis
- Risku ierobežošanas pasākumi
- Risku ierobežošanas izmaksu novērtējums

Sistēmas drošības kritēriji

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

13. Sistēmas drošības politika ietver:

..

13.5. ...un citus sistēmas drošības kritērijus (piemēram, sistēmas nepārtrauktās darbības laiks, sistēmas darbības atjaunošanas laiks, nosacījumi, pie kuriem ikdienas procedūras aizstājamas ar krīzes pārvaldības procedūrām).;

- Nepārtrauktās darbības laiks
- Sistēmas atjaunošanas laiks
- Krīzes pārvaldība

Sistēmas drošības iekšējie noteikumi

Vispārējie jautājumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Sistēmas informācijas resursi
- Sistēmas tehniskie resursi

Informācijas sistēmas dzīves cikls

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

25. Iekšējie sistēmas drošības noteikumi nosaka:
25.1. sistēmas informācijas resursu izveidošanas, papildināšanas, mainīšanas, apstrādes, pārraidīšanas, glabāšanas, atjaunošanas un iznīcināšanas kārtību;

- Sistēmas izstrādes, iegādes, ieviešanas un izmaiņu pārvaldīšanas procesi
- Izstrādes, testa un produkcijas vides
- Sistēmas dokumentācijas uzturēšana
- Sistēmas lietošanas izbeigšana

Piekļuves kontrole

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

25. Iekšējie sistēmas drošības noteikumi nosaka:
...
25.2. sistēmas informācijas un tehnisko resursu lietošanas un tās kontroles kārtību;
25.3. kārtību, kādā tiek nodrošināta piekļūšana sistēmas informācijas un tehniskajiem resursiem;

- Lietotāju pārvaldības process
- Paroles
- Informācijas un Tehnisko resursu valdītāju tiesības un pienākumi
- Auditācijas pieraksti

Informācijas resursu rezerves kopijas

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

25. Iekšējie sistēmas drošības noteikumi nosaka:
..
25.4. 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;

- Rezerves kopiju pārvaldības process
- Kopiju veidošana
- Kopiju uzglabāšana
- Kopiju pārbaude

Datu nesēji

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

25. Iekšējie sistēmas drošības noteikumi nosaka:
...
25.5. datu nesēju lietošanas, pārvietošanas, glabāšanas un iznīcināšanas kārtību;

- Datu nesēju marķēšana
- Datu nesēju uzglabāšana
- Datu nesēju pārvietošana

Piekļuves dati un sistēmas informācija

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

25. Iekšējie sistēmas drošības noteikumi nosaka:
...
25.6. kārtību, kādā lieto un glabā informāciju vai datus, kas nepieciešami, lai piekļūtu sistēmas informācijas un tehniskajiem resursiem;

- Informācijas klasifikācija
- Informācijas aizsardzība
- Informācijas glabāšana

Loģiskā aizsardzība

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

25. Iekšējie sistēmas drošības noteikumi nosaka:
...
25.7. 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);

- Informācijas un Tehnisko resursu valdītāju tiesības un pienākumi
- Aizsardzības pasākumi

Fiziskā aizsardzība

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

25. Iekšējie sistēmas drošības noteikumi nosaka:
...
25.8. 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);

- Piekļuve tehniskajiem resursiem
- Apmeklētāju piekļuve
- Aizsardzības līdzekļi

Apdraudējumu un incidentu pārvaldība

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

25. Iekšējie sistēmas drošības noteikumi nosaka:
...
25.9. kārtību, kādā novēro sistēmas drošības apdraudējuma tuvošanās pazīmes;
25.10. kārtību, kādā atklāj un pārvalda sistēmas drošības incidentus;

- Informācijas aprite
- Tehniskie līdzekļi
- Incidentu analīze
- Pasākumi incidentu novēršanai

Sistēmas darbība, ja resursi pieejami nepilnā apjomā

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

25. Iekšējie sistēmas drošības noteikumi nosaka:
...
25.11. kārtību, kādā sistēma darbojas, ja sistēmas informācijas vai tehniskie resursi nav pieejami pilnā apjomā;

- Alternatīvas sistēmas darbībai
- Darbības atjaunošanas pasākumi

Tehnisko resursu izmaiņu pārvaldība

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

25. Iekšējie sistēmas drošības noteikumi nosaka:
...
25.12. kārtību, kādā maina sistēmas tehniskos resursus;

- Tehnisko resursu valdītāju tiesības un pienākumi
- Izmaiņu uzskaite un izsekojamība

Darbinieku apmācības

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

25. Iekšējie sistēmas drošības noteikumi nosaka:
...
25.13. institūcijas darbinieku apmācības un zināšanu pārbaudes kārtību sistēmas drošības jomā.

- Apmācību veidi
- Atbildīgais par apmācību veikšanu
- Apmācību uzskaite

Sistēmas lietošanas noteikumi

Vispārējie jautājumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Iestādes atbildība
- Saistības lietotājiem

Sistēmas lietotāju tiesības, pienākumi, ierobežojumi un atbildība

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

26. Sistēmas lietošanas noteikumi ietver:
26.1. sistēmas lietotāju tiesības, pienākumus, ierobežojumus un atbildību;

- Lietotāju tiesības, pienākumi, ierobežojumi un atbildība
- Atbildīgās personas kontaktinformācija
- Iestādes specifiskiem nosacījumiem

Sistēmas lietotāju reģistrācija un tās atcelšanas kārtība

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

26. Sistēmas lietošanas noteikumi ietver:
..
26.2. sistēmas lietotāju reģistrācijas un tās atcelšanas kārtību;

- Lietotāju «dzīves cikla» apraksts iestādē

Sistēmas lietošanas kārtība

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

26. Sistēmas lietošanas noteikumi ietver:
..
26.3. sistēmas lietošanas kārtību;

- Ierobežojumi sistēmas lietošanai
- Lietotāju uzraudzības kārtība

Sistēmas lietotāju atbalsta kārtība

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

26. Sistēmas lietošanas noteikumi ietver:
...
26.4. sistēmas lietotāju atbalsta kārtību.

- Pamata nosacījumi lietotāju atbalstam
- Informēšanas kārtība
- Atbalsta kontaktinformācija

Drošības riska pārvaldības plāns

Vispārējie jautājumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Kārtība, kādā veicama risku analīze
- Periodisks dokuments aktuālo risku novērtēšanai un ierobežošanai

Risku analīzes metodoloģija

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

27. Sistēmas drošības riska pārvaldības plāns ietver:
27.1. veicamās risku analīzes metodoloģijas aprakstu;

- Analīzes mērķi
- Veikšanas regularitāte
- Iesaistītās personas

Sistēmas drošības risku analīzes apraksts

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

27. Sistēmas drošības riska pārvaldības plāns ietver:
..
27.2. sistēmas drošības risku analīzi;

- Apdraudējuma novērtējums
- Kaitējuma novērtējums
- Riska aprēķins un novērtēšana

Sistēmas drošības apdraudējumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

30. Sistēmas drošības risku analīze ietver:
30.1. sistēmas drošības apdraudējumu uzskaitījumu, to īstenošanās varbūtības novērtējumu un tuvošanās pazīmju uzskaitījumu;

- Ar aparatūru saistītie apdraudējumi
- Ar programmatūru saistītie apdraudējumi
- Ar lestādes personālu saistītie apdraudējumi
- Ar komunikācijām saistītie apdraudējumi
- Apkārtējās vides apdraudējumi

Sistēmas drošības riska novērtējums

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

30. Sistēmas drošības risku analīze ietver:
..
30.3. sistēmas drošības riska novērtējumu;

- Identificēto risku apraksts
- Novērtējums

Sistēmas drošības riska mazināšanas pasākumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

30. Sistēmas drošības risku analīze ietver:
..
30.4. sistēmas drošības riska mazināšanas pasākumu un tajos izmantojamo līdzekļu uzskaitījumu;

- Identificēt riska mazināšanas pasākumus
- Ieviešanas termiņš
- Nepieciešamie līdzekļi
- Atbildīgais par īstenošanu

Sistēmas drošības riska mazināšanai veikto pasākumu lietderības novērtējums

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

30. Sistēmas drošības risku analīze ietver:
...
30.5. sistēmas drošības riska mazināšanai veikto pasākumu lietderības novērtējumu.

- Kā tiek izvērtēts pasākumu lietderīgums
- Kā tiek noteikti citi mazināšanas pasākumi

Sistēmas darbības atjaunošanas plāns

Vadības apliecinājums

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Plāns ir pilnīgs
- Informācija atbilstoša
- Plānotā sistēmas atjaunošana atbilst iestādes vajadzībām
- Apliecinājums regulārai plāna pārbaudei

Sistēmas atjaunošanas raksturlielumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Maksimāli pieļaujamā dīkstāve
- Maksimāli pieļaujamais datu zudums
- Sistēmas funkcijas

Sistēmas informācijas un tehnisko resursu atjaunošanas pasākumi, kas veicami pēc sistēmas drošības incidenta

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

33. Sistēmas darbības atjaunošanas plāns ietver:
33.1. sistēmas informācijas un tehnisko resursu atjaunošanas pasākumus, kas veicami pēc sistēmas drošības incidenta;

- Atjaunošanas pasākumi
- Incidenta analīze
- Nepieciešamo uzlabojumu novērtējums

Sistēmas darbības atjaunošanas pasākumu apraksts

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

33. Sistēmas darbības atjaunošanas plāns ietver:
..
33.2. sistēmas darbības atjaunošanas pasākumu procedūru aprakstu;

- Atjaunošanas vietas noteikšana
- Nepieciešamo resursu identificēšana
- Rezerves kopiju un sistēmas instalēšanas datu iegūšana
- Tehnisko resursu atjaunošana
- Tehnisko resursu darbības pārbaude
- Sistēmas informācijas resursu atjaunošana
- Sistēmas informācijas resursu integritātes pārbaude

Atbildīgo personu apziņošanas kārtība un darbības instrukcijas

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

33. Sistēmas darbības atjaunošanas plāns ietver:
..
33.3. sistēmas darbības atjaunošanas pasākumos iesaistīto atbildīgo personu apziņošanas kārtību un darbības instrukcijas;

- Atbildīgo kontaktinformācija
- Apziņošanas kārtība

Atbildīgo personu apmācības, nodarbību un sagatavotības pārbaužu plānu

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

33. Sistēmas darbības atjaunošanas plāns ietver:
..
33.4. atbildīgo personu apmācības, nodarbību un sagatavotības pārbaužu plānu.

- Darbinieku iepazīstināšana ar plānu
- Apmācību norise
- Pārbaužu norise un regularitāte

Kārtība saziņai ar sadarbības partneriem un sabiedrību

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Vai nepieciešams apziņot:
  - Sadarbības partnerus
  - Sabiedrību
- Saziņas kārtība

Noslēgums

Procedūras, darbību apraksti

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Sistēmas izstrādes process
- Sistēmas izmaiņu pārvaldības procedūra
- Sistēmas likvidēšanas kārtība
- Sistēmas lietotāju pārvaldības procedūra
- Sistēmas rezerves kopiju izgatavošanas un sistēmas atjaunošanas kārtība
- Informācijas klasifikācijas kārtība
- Sistēmas dokumentācija
- Pieejas tiesību saraksts
- Incidentu pārvaldības pasākumi
- Tehnisko resursu pārvaldības procedūra
- Apmācību kārtība
- Apmācību reģistrs
- ...

Noslēguma jautājumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

10. .. Institūcija visus šo noteikumu 8. punktā minētos dokumentus pārskata vismaz reizi gadā, kā arī šādos gadījumos:

10.1. ja izmaiņas sistēmā var ietekmēt sistēmas drošību;

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

10.3. ja pēkšņi pieaug sistēmas drošības incidentu skaits vai ir noticis nozīmīgs sistēmas drošības incidents;

10.4. ja izmaiņas institūcijas organizatoriskajā struktūrā skar sistēmas drošības vadības organizāciju;

10.5. ja izdarīti grozījumi normatīvajos aktos, kas regulē sistēmas darbību.

10. Noslēguma jautājumi

10.1. Dokumentu pārskata vismaz reizi gada, kā arī šādos gadījumos:
10.1.1. ja izmaiņas sistēmā var ietekmēt sistēmas drošību;
10.1.2. ja mainījušies vai ir atklāti jauni sistēmas drošības apdraudējumi;
10.1.3. ja pieaug sistēmas drošības incidentu skaits vai noticis nozīmīgs sistēmas drošības incidents;
10.1.4. ja izmaiņas institūcijas organizatoriskajā struktūrā skar sistēmas drošības vadības organizāciju;
10.1.5. ja izdarīti grozījumi normatīvajos aktos, kas regulē sistēmas darbību.
10.2. Ja, pārskatot dokumentu, konstatēta atbilstoša nepieciešamība, to aktualizē.

Kopsavilkums

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Drošības prasības iepirkumos
- Prasības ārpakalpojumu sniedzējiem
- Atrast atbildīgo
- Nodrošināt vadības izpratni un atbalstu
- Saprast, kādi dokumenti ir
- Izstrādāt jaunos dokumentus līdz 01.01.2017.
- Nodrošināt prasību izpildi sistēmām
- Izbeigt neatbilstošo sistēmu darbību

Paldies!