*Nacionālais kiberdrošības centrs, 29.07.2025.*

**[NKDL Subjekta indentificējoša informācija]**

**Kiberdrošības pārvaldības poltika**

*Dokuments, kas nosaka organizācijas pieeju kiberdrošībai, mērķus, principus un atbildību sadalījumu.*

|  |  |  |
| --- | --- | --- |
| Nr. | Apakšnodaļa nosaukums | Statuss |
| 1.1 | Organizācijas konteksts | ✔️ Obligāta |
| 1.2 | Ieinteresēto pušu identificēšana | ✔️ Obligāta |
| 1.3 | Atbilstība nacionālajiem normatīvajiem aktiem | ✔️ Obligāta |
| 1.4 | Jomai specifiskās prasības | ✔️ Obligāta  |
| 2.1 | Pārvaldības apņemšanās | ✔️ Obligāta |
| 2.2 | Informācijas drošības politika | ✔️ Obligāta |
| 2.3 | Lomas, pienākumi un atbildība | ✔️ Obligāta |
| 2.4 | Pārbaudes un auditi | ✔️ Obligāta |
| 2.5 | Kiberdrošības kultūra un izpratne | ☑ Rekomendējama |
| 2.6 | Atbildības | ✔️ Obligāta |
| 2.7 | Atbalsts | ☑ Rekomendējama |
| 2.8 | Kompetence | ☑ Rekomendējama |
| 2.9 | Informētība | ✔️ Obligāta |
| 2.10 | Komunikācija | ☑ Rekomendējama |
| 3.1 | Riska novērtēšana | ✔️ Obligāta |
| 3.2 | Riska apstrāde | ✔️ Obligāta |
| 3.3 | Informācijas drošības mērķi | ✔️ Obligāta |
| 3.4 | Aizsardzība pret riskiem un apdraudējumiem | ✔️ Obligāta |
| 3.5 | Nepārtrauktības un incidentu reaģēšanas plāni | ✔️ Obligāta |
| 4.1 | Politikas, apmācības un pieejamības plāni | ✔️ Obligāta |
| 4.2 | Fiziskā drošība | ✔️ Obligāta |
| 4.3 | Personāla drošība un IAM | ✔️ Obligāta |
| 4.4 | Apmācība un informētība | ✔️ Obligāta |
| 4.5 | Tīkla un darba staciju drošība | ✔️ Obligāta |
| 4.6 | Piekļuves kontrole, šifrēšana, atjauninājumi | ✔️ Obligāta |
| 4.7 | Aplikāciju drošība | ☑ Rekomendējama |
| 4.8 | Konfigurāciju pārvaldība un privilēģētā piekļuve | ☑ Rekomendējama |
| 4.9 | Kaitīgā programmatūra | ✔️ Obligāta |
| 4.10 | Ārpakalpojumu pārvaldība | ✔️ Obligāta |
| 4.11 | Uzraudzība un auditi | ✔️ Obligāta |
| 4.12 | Datu rezerves kopēšana un atjaunošana | ✔️ Obligāta |
| 4.13 | Iznīcināšana | ✔️ Obligāta |
| 4.14 | Uzlabošana un korektīvās darbības | ☑ Rekomendējama |
| 5.1–5.8 | Incidentu pārvaldība (visi punkti) | ✔️ Obligāti |
| 6.1–6.2 | Atbilstības pārbaude  | ✔️ Obligāta |
| 7.1–7.7 | Plānošana, audits, izvērtēšana un pašvērtējums | ✔️ Obligāta |

SATURS

[1. VISPĀRĪGĀ INFORMĀCIJA 4](#_Toc204681867)

[1.1. Organizācijas konteksts 4](#_Toc204681868)

[1.2. Ieinteresēto pušu identificēšana 4](#_Toc204681869)

[1.3. Atbilstība nacionālajiem normatīvajiem aktiem 4](#_Toc204681870)

[1.4. Jomai specifiskās prasības 4](#_Toc204681871)

[2. INFORMĀCIJAS SISTĒMAS PĀRVALDĪBA 5](#_Toc204681872)

[2.1. Pārvaldības apņemšanās 5](#_Toc204681873)

[2.2. Organizācijas drošības politika 5](#_Toc204681874)

[2.3. Lomas, pienākumi un atbildība 5](#_Toc204681875)

[2.4. Pārbaudes un auditi 5](#_Toc204681876)

[2.5. Kiberdrošības kultūra un izpratne 5](#_Toc204681877)

[2.6. Atbildības sadalījums 6](#_Toc204681878)

[2.7. Atbalsts 6](#_Toc204681879)

[2.8. Kompetence 6](#_Toc204681880)

[2.9. Informētība 6](#_Toc204681881)

[2.10. Komunikācija 6](#_Toc204681882)

[3. RISKU PĀRVALDĪBA 7](#_Toc204681883)

[3.1. Riska novērtēšana 7](#_Toc204681884)

[3.2. Riska apstrāde 7](#_Toc204681885)

[3.3. Informācijas drošības mērķi 7](#_Toc204681886)

[3.4. Aizsardzība pret riskiem un apdraudējumiem 7](#_Toc204681887)

[3.5. Nepārtrauktības un incidentu reaģēšanas plāni 8](#_Toc204681888)

[4. KONTROLES 8](#_Toc204681889)

[4.1. Politika 8](#_Toc204681890)

[4.2. Fiziskā drošība 8](#_Toc204681891)

[4.3. Personāla drošība un identitātes pārvaldība (IAM) 8](#_Toc204681892)

[4.4. Apmācība un informētība 8](#_Toc204681893)

[4.5. Tīkla un darba staciju drošība 9](#_Toc204681894)

[4.6. Piekļuves kontrole, šifrēšana un atjauninājumi 9](#_Toc204681895)

[4.7. Programmatūras izstrādes drošība 9](#_Toc204681896)

[4.8. Konfigurāciju pārvaldība un privileģētā piekļuve 9](#_Toc204681897)

[4.9. Kaitīgā programmatūra (*Malware*) un aizsardzība 9](#_Toc204681898)

[4.10. Ārpakalpojumu pārvaldība 9](#_Toc204681899)

[4.11. Uzraudzība, žurnālfaili un auditi 9](#_Toc204681900)

[4.12. Datu rezerves kopēšana un atjaunošana 9](#_Toc204681901)

[4.13. Iznīcināšana 9](#_Toc204681902)

[4.14. Uzlabošana un korektīvās darbības 9](#_Toc204681903)

[5. INCIDENTU PĀRVALDĪBA 10](#_Toc204681904)

[5.1. ATBILDĪBAS SADALĪJUMS 10](#_Toc204681905)

[5.2. Sadarbība ar iekšējām un ārējām pusēm 10](#_Toc204681906)

[5.3. Darbības pēc incidenta 10](#_Toc204681907)

[5.4. Uzraudzība un nepārtraukta uzlabošana 11](#_Toc204681908)

[6. ATBILSTĪBAS PĀRBAUDE 11](#_Toc204681909)

[6.1. Atbilstība normatīvajiem aktiem 11](#_Toc204681910)

[6.2. Atbilstība drošības prasībām 11](#_Toc204681911)

[7. PLĀNOŠANA UN PĀRSKATĪŠANAS PASĀKUMI 11](#_Toc204681912)

[7.1. Informācijas drošības integrācija organizācijas procesos 11](#_Toc204681913)

[7.2. Riska apstrādes pasākumu īstenošana 12](#_Toc204681914)

[7.3. Izmaiņu un konfigurācijas vadība 12](#_Toc204681915)

[7.4. Kontroļu monitorings un izvērtēšana 12](#_Toc204681916)

[7.5. Iekšējais audits un pašvērtējums 12](#_Toc204681917)

[7.6. Pārvaldības pārskatīšana 12](#_Toc204681918)

[7.7. Politikas, procedūras un kontroles veidi 12](#_Toc204681919)

# VISPĀRĪGĀ INFORMĀCIJA

**Mērķis:** šī politika definē organizācijas vispārējo pieeju kiberdrošības pārvaldībai un kalpo kā pamats iekšējai drošības kontrolei, riska pārvaldībai un atbilstības nodrošināšanai. Tā palīdz strukturēti veikt ikgadējo **pašvērtējumu**, kā arī sagatavoties **iekšējiem vai ārējiem auditiem**.

Politika ietver:

* organizācijas kiberdrošības mērķus un pamatprincipus;
* lomu un atbildību sadalījumu kiberdrošības pārvaldībā;
* apņemšanos ievērot drošības prasības, kas izriet no normatīvajiem aktiem, tostarp Nacionālā kiberdrošības likuma un uz tā pamata izdotajiem Ministru kabineta noteikumiem;
* piemērošanas jomu, norādot, uz kuriem procesiem, informācijas sistēmām un resursiem tā attiecas.

##  Organizācijas konteksts

Organizācija regulāri identificē un izvērtē iekšējos un ārējos faktorus, kas ietekmē kiberdrošības mērķu sasniegšanu, tostarp:

* tehnoloģiju attīstību un mainīgās apdraudējuma vides;
* normatīvās prasības un izmaiņas regulējumā;
* piegādes ķēdes riskus un partneru ietekmi;
* organizatoriskās izmaiņas un struktūru.

##  Ieinteresēto pušu identificēšana

Organizācija identificē ieinteresētās puses, kuru vajadzības un prasības attiecas uz informācijas drošību (konfidencialitāti, integritāti, pieejamību). Tās var būt:

* klienti, darbinieki, partneri;
* valsts iestādes, auditori;
* ārpakalpojumu sniedzēji.
* …

##  Atbilstība nacionālajiem normatīvajiem aktiem

Tiek izvērtēts, vai organizācija atbilst Kiberdrošības likuma un MK noteikumu subjektu definīcijām, tai skaitā vai tā ir Nacionālajai drošībai svarīgs pakalpojumu sniedzējs. Pamatojums tiek dokumentēts un periodiski pārskatīts.

##  Jomai specifiskās prasības

Papildus vispārējām drošības prasībām organizācija ievēro nozares vai pakalpojuma specifiskās prasības (piemēram, veselības, finanšu, enerģētikas sektoriem). Šīs prasības tiek:

* dokumentētas un integrētas informācijas drošības vadībā;
* pārskatītas riska izvērtēšanas gaitā.

# 2. INFORMĀCIJAS SISTĒMAS PĀRVALDĪBA

##  Pārvaldības apņemšanās

Informācija par to kā organizācijas vadība apņemas nodrošināt informācijas drošību. Organizācijas vadība nodrošina informācijas drošības pārvaldību, integrējot drošības mērķus stratēģijā un piešķirot nepieciešamos resursus. Vadība iesaistās drošības plānošanā, uzraudzībā un izvērtēšanā.

##  Organizācijas drošības politika

Informācija par to kā organizācijā ir izstrādāta, ieviesta un tiek regulāri uzturēta visaptveroša informācijas drošības politika, kas nosaka:

* drošības mērķus un principus;
* attieksmi pret riskiem;
* atbilstību normatīvajiem aktiem;
* atbildības sadalījumu.

Politika tiek pārskatīta vismaz reizi gadā vai pēc būtiskām izmaiņām.

## Lomas, pienākumi un atbildība

Informācija par to kā informācijas drošības vadības struktūra ir skaidri definēta un dokumentēta. Katram darbiniekam, kura darbība var ietekmēt drošības līmeni, ir piešķirtas konkrētas lomas un atbildības, kas saistītas ar:

* politikas ievērošanu;
* risku identificēšanu un ziņošanu;
* incidentu pārvaldību;
* piekļuves pārvaldību.

Šī informācija tiek nodota darbiniekiem, izmantojot ievadinstruktāžas, apmācības un iekšējās komunikācijas kanālus.

##  Pārbaudes un auditi

Organizācijā regulāri tiek veikti informācijas drošības auditi un pārbaudes, lai:

* novērtētu iekšējās drošibas kotnroļu vidi un tās atbilstību politikām;
* identificētu šī brīza kiberdrošības stāvokli.
* plānotu uzlabojumus, balstoties uz konstatētajām neatbilstībām.

Tiek veikti gan iekšējie auditi, gan nepieciešamības gadījumā – ārējie novērtējumi. Rezultāti tiek dokumentēti un izmantoti vadības pārskatam.

##  Kiberdrošības kultūra un izpratne

Organizācija veido kiberdrošības kultūru, kas balstīta uz izpratni un līdzdalību, īstenojot:

* regulāras apmācības, testus un simulācijas (piemēram, pikšķerēšanas kampaņas);
* iekšējo komunikāciju un informētības materiālus;
* atbildības deleģēšanu visos organizācijas līmeņos;
* izpratnes rādītāju uzraudzību un analīzi.

## Atbildības sadalījums

|  |  |  |  |
| --- | --- | --- | --- |
| **Vārds un uzvārds** | **Amats un atbildība** | **E-pasts** | **Tālrunis** |
| [.…] | Vadītājs (IT nodaļas vadītājs) | darba: [e-pasts] | birojs / mobilais |
| [….] | Kiberdrošības pārvaldnieks (Arhitektūras un drošības vadītājs) | darba: [e-pasts] | birojs / mobilais |

## Atbalsts

Informācija par to kā organizācija nodrošina nepieciešamos resursus informācijas drošības uzturēšanai, tai skaitā:

* specializētus drošības risinājumus (piem., IDPS);
* tīkla uzraudzības un infrastruktūras jaudu;
* personālu incidentu analīzei un reaģēšanai;
* budžetu testēšanai, uzlabojumiem un ārējai ekspertīzei.

##  Kompetence

Piem. Darbiniekiem, kuri iesaistīti informācijas drošībā, tiek nodrošināta:

* regulāra profesionālā pilnveide un sertifikācijas iespējas (CISSP, CISM u.c.);
* praktiskas simulācijas un incidentu pārvaldības apmācības;
* kompetenču pārbaude (testi, simulācijas) atbilstoši apdraudējumu attīstībai.

##  Informētība

Informācija par to kā organizācija veido un uztur augstu darbinieku informētības līmeni par informācijas drošību, tostarp:

Organizācija veicina darbinieku informētību par drošību, nodrošinot:

* piekļuvi politikām un instrukcijām;
* apmācības, informatīvas kampaņas un ievadapmācības jaunajiem darbiniekiem;
* regulāras pārbaudes (sociālās inženierijas testi u.c.).

##  Komunikācija

Informācija par to kā tiek noteikta strukturēta komunikācijas kārtība drošības jautājumos:

* pienākumu sadalījums atbilstoši delaģētajai atbildībai;
* incidentu reaģēšanas un saziņas protokoli;
* saziņa ar ārējām pusēm (CERT.LV, piegādātāji, klienti);
* ziņošanas kanāli iekšējiem incidentiem (e-pasts, tālrunis, sistēmas).

# 3. RISKU PĀRVALDĪBA

##  Riska novērtēšana

Informācija par to, kā organizācijā tiek veikta regulāra informācijas drošības risku novērtēšana, lai identificētu potenciālos apdraudējumus, ievainojamības un to iespējamo ietekmi uz konfidencialitāti, integritāti un pieejamību. Riska novērtēšanas process ietver:

* informācijas aktīvu identificēšanu un klasificēšanu;
* draudu un ievainojamību analīzi;
* riska līmeņa aprēķinu (ietekme × iespējamība);
* prioritāšu noteikšanu un riska pieņemamības izvērtēšanu.

Novērtēšana tiek veikta sistēmas izstrādes vai ieviešanas posmā, kā arī regulāri pārskatīta – vismaz reizi gadā vai pēc būtiskām izmaiņām.

##  Riska apstrāde

Informācija par to, kā organizācija, pamatojoties uz risku novērtēšanas rezultātiem, izstrādā risku apstrādes plānus, nosakot kontroles pasākumus, lai:

* ierobežotu riskus līdz pieņemamam līmenim;
* izvairītos no nepieņemamiem riskiem;
* pārceltu riskus uz trešajām pusēm (piemēram, ar apdrošināšanu vai deleģēšanu);
* pieņemtu zema līmeņa, kontrolētus riskus.

Risku apstrādes plāni tiek dokumentēti, pārskatīti un piesaistīti konkrētām atbildīgajām personām un termiņiem.

##  Informācijas drošības mērķi

Informācija par to, kā organizācija nosaka konkrētus, izmērāmus un sasniedzamus informācijas drošības mērķus, kas atbilst tās stratēģijai un riska profilam. Mērķi tiek:

* definēti augstākajā vadības līmenī (piem., samazināt incidentu skaitu);
* sasaistīti ar klientu, normatīvajām un kvalitātes prasībām;
* regulāri pārskatīti un novērtēti ar noteiktiem drošības rādītājiem (KPI).

##  Aizsardzība pret riskiem un apdraudējumiem

Informācija par to, kā organizācija ievieš integrētus drošības pasākumus, lai pārvaldītu identificēto risku ietekmi. Tiek īstenotas:

**a) Administratīvās kontroles:**

* drošības politikas, procedūras un piekļuves tiesību pārvaldība;
* personāla apmācība un uzvedības standarti;
* riska pārvaldība un atbilstības kontrole.

**b) Tehniskās kontroles:**

* ugunsmūri, IDPS, antivīrusi, SIEM;
* datu šifrēšana, autentifikācija un tīkla segmentācija.

**c) Fiziskās kontroles:**

* ierobežota piekļuve telpām (kartes, biometriskie risinājumi);
* video novērošana, signalizācija un ārējās dublēšanas vietas.

##  Nepārtrauktības un incidentu reaģēšanas plāni

Informācija par to, kā organizācija samazina sistēmu dīkstāves un operacionālo ietekmi apdraudējumu gadījumā, izstrādājot un regulāri pārskatot un, nepieciešamības gadījumā testējot, šādus plānus:

**Incidentu reaģēšanas plāns**

* nodrošina ātru un strukturētu rīcību kiberincidentu gadījumā;
* ietver atbildīgos, saziņas kārtību un eskalācijas soļus;
* ir saskaņots ar ziņošanas prasībām (t. sk. atbilstoši Nacionālās kiberdrošības likuma prasībām).

**Ārkārtas reaģēšanas un darbības nepārtrauktības plāns (BCP)**

* apraksta darbības rīcībai fizisku draudu gadījumā (ugunsgrēks, plūdi u. c.);
* nosaka kritisko iekārtu aizsardzību un pārvietošanu;
* nodrošina pakalpojumu un sistēmu atjaunošanu krīzes laikā;
* definē prioritātes, atjaunošanas secību un atbildības;
* integrēts ar katastrofu atjaunošanās plānu (DRP), t.sk., rezerves kopēšanas un atjaunošanas procedūrām.

# KONTROLES

##  Politika

Informācija par to, kā organizācijā tiek izstrādātas, apstiprinātas un regulāri pārskatītas informācijas drošības politikas un procedūras, kas definē standartus un prasības visos drošības aspektos.

Informācija par pieejamības plāniem, kas nodrošina sistēmu un datu atjaunošanu pēc incidentiem, integrēti biznesa nepārtrauktības stratēģijā.

##  Fiziskā drošība

Piekļuves kontrole kritiskajām vietām (telpām, skapjiem) ar autentifikācijas līdzekļiem un videonovērošanu drošības notikumu uzraudzībai.

## Personāla drošība un identitātes pārvaldība (IAM)

Informācija par IAM politiku, tai skaitā loģiskās piekļuves kontroles, autentifikācijas un tiesību dzīves cikla pārvaldību.

##  Apmācība un informētība

Organizācija nodrošina darbiniekiem regulāras apmācības, kampaņas un ievadinstruktāžas par kiberdrošību, lai veicinātu izpratni un stiprinātu drošības kultūru.

* Lietotāju apmācību plāni kiberdrošības jomā.
* Ikgadēja zināšanu pārbaude vai kampaņas.

## Tīkla un darba staciju drošība

Tīkla aizsardzības pasākumi (ugunsmūri, IDS/IPS, segmentācija), datu šifrēšana, gala iekārtu kontrole un drošība, uzraudzība un incidentu noteikšana.

Informācija par to kā darbiniekiem piešķirtajiem resursiem tiek noteiktas pārbaudes, uzsākot darbu, tā laikā un to pabeidzot:

* vizuāla pārbaude (bojājumi, plombas, drošības uzlīmes);
* informācijas sistēmas darbības anomāliju novērošana;
* aizvēršana un bloķēšana darba pārtraukumā.

## Piekļuves kontrole, šifrēšana un atjauninājumi

RBAC, MFA, datu šifrēšana, drošības ielāpi un programmatūras komponentu regulāra atjaunināšana.

## Programmatūras izstrādes drošība

Secure SDLC: drošības prasību integrācija izstrādē, kodu pārskatīšana, SAST/DAST testēšana, ievainojamību pārvaldība, ja aktuāli.

##  Konfigurāciju pārvaldība un privileģētā piekļuve

Privileģēto kontu pārvaldība (RBAC, JIT, MFA), konfigurāciju kontrole, SIEM uzraudzība, regulāri auditi.

##  Kaitīgā programmatūra (*Malware*) un aizsardzība

Aizsardzība pret ļaunatūru: antivīrusi, protokolu ierobežošana, tikai atļautu darbību politika, “nulles uzticamības” princips (*zero trust*).

## Ārpakalpojumu pārvaldība

Līgumos iekļautas drošības prasības, riska novērtējums, uzraudzība, datu nodošana trešajām pusēm, rezerves plāni, t.sk., atbilstība normatīvo aktu prasībām

##  Uzraudzība, žurnālfaili un auditi

Iekšējie/ārējie auditi, SIEM, logu pārvaldība, konfigurācijas kontrole, incidentu analīze un uzlabošanas pasākumi.

## Datu rezerves kopēšana un atjaunošana

Regulāri dublējumi, dažādi rezerves kopiju veidi, dokumentēti atjaunošanas plāni ar testēšanu.

## Iznīcināšana

Politikas un procedūras sensitīvo datu un ierīču drošai un pārbaudāmai iznīcināšanai, personāla apmācības.

## Uzlabošana un korektīvās darbības

Neatbilstību identificēšana un korekcija, pastāvīga uzlabošana balstīta uz auditiem, incidentiem, tehnoloģiju izmaiņām un atsauksmēm.

#  INCIDENTU PĀRVALDĪBA

## ATBILDĪBAS SADALĪJUMS

Informācija par to kā tiek noteikts kurš izpilda, atbildīgs, iesaistīts vai informējams katrā incidentu pārvaldības posmā.

**R** – *Responsible* (Izpildītājs): persona vai personas, kas praktiski veic uzdevumu.

**A** – *Accountable* (Atbildīgais): persona, kas nes atbildību par uzdevuma veikšanu un pieņem gala lēmumu. Parasti ir tikai viens “*Accountable*”.

**C** – *Consulted* (Iesaistītais): cilvēki, ar kuriem jākonsultējas pirms rīcības, jo viņiem ir būtiskas zināšanas vai ietekme.

**I** – *Informed* (Informējamais): personas, kurām jāzina, kas notiek, bet kuras nav iesaistītas lēmumu pieņemšanā vai praktiskā darbā.

Atbildības sadalījuma piemērs:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Aktivitāte | Izpildītājs (R) | Atbildīgs (A) | Iesaistītais (C) | Informējamais (I) |
| Incidentu identificēšana | IT drošība | Vadība | IT personāls | Vadība |
| Incidentu ziņošana | IT drošība | Vadība | Lietotājs, pakalpojumu sniedzēji | Vadība, CERT.LV |
| Incidentu analīze | IT drošība | IT nodaļa | Juridiskā nodaļa | Valde, PR |
| Ierobežošana un novēršana | IT drošība | Vadība | ISP, ārpakalpojumi | CERT.LV |
| Atjaunošana | IT nodaļa | Vadība | Infrastruktūras atbalsts | Biznesa pārstāvji |
| Atskaite un mācīšanās | CIRT | Vadība | Atbilstības nodaļa | Auditoru pārstāvji |

##  Sadarbība ar iekšējām un ārējām pusēm

Informācija par to, kā tiek uzturēta sadarbība un komunikācija ar:

* IT drošības un incidentu vadības atbildīgajiem;
* organizācijas vadību (IT direktors, valde);
* klientiem;
* pakalpojumu sniedzējiem (ISP, datu centri, izstrādātāji);
* tiesībsargājošām iestādēm (Valsts policija, utt.), kiberincidentu novēršanas institūcijām (CERT.LV).

##  Darbības pēc incidenta

Pēc riska iestāšanās tiek veiktas šādas darbības:

* cēloņu analīze un risku izvērtēšana;
* politiku, procedūru un kontroles mehānismu pārskatīšana;
* darbinieku informēšana un apmācības, balstoties uz incidenta laikā gūtajām mācībām, lai novērstu līdzīgu gadījumu atkārtošanos nākotnē;
* līgumu (SLA/OLA) un sadarbības nosacījumu pārskatīšana.

##  Uzraudzība un nepārtraukta uzlabošana

Informācija par to, kā tiek uzturēta risku pārvaldības kvalitāte:

* regulāri auditi un testēšana;
* SIEM un DLP sistēmu izmantošana uzraudzībai;
* korektīvās un preventīvās darbības pēc incidentiem;
* politiku un plānu regulāra pārskatīšana un pilnveidošana.

# ATBILSTĪBAS PĀRBAUDE

##  Atbilstība normatīvajiem aktiem

Informācija par to kā nodrošināt, ka informācijas sistēma atbilst visām piemērojamām normatīvajām prasībām un speciālajam regulējumas, piemēram, VDAR attiecībā uz personu datu aizsardzībai ES, nozarspecifiskiem tiesību aktiem.

##  Atbilstība drošības prasībām

Organizācija ievēro **"nepieciešamības zināt"** principu, piešķirot piekļuvi tikai atbilstoši amata pienākumiem. Šis princips tiek ieviests ar:

* lomu balstītu piekļuves kontroli (RBAC);
* identitāšu un piekļuves pārvaldību (IAM);
* minimālās piekļuves tiesības principa izmantošana (*least privilege*);
* regulāru piekļuves pārskatīšanu;
* privātuma un konfidencialitātes aizsardzības līdzekļiem.

Organizācija pārvalda informācijas aktīvus visā to dzīves ciklā, nodrošinot:

* identificēšanu, klasifikāciju un īpašnieku noteikšanu;
* datu aizsardzību (tai skaitā personas datu);
* glabāšanas termiņu un drošas iznīcināšanas noteikšanu.

IT arhitektūra tiek plānota pēc drošības principiem (“*security by design*”), iekļaujot:

* ievainojamību novēršanu tīmekļa un lietojumprogrammas līmenī;
* drošu infrastruktūras un lietojumprogrammu izstrādi un ieviešanu, ja saistoši.

Tīkla drošība tiek nodrošināta ar:

* segmentāciju, VPN, *Zero Trust* principu;
* drošu pārsūtīšanu (TLS, IPsec);
* aizsardzību pret tīkla apdraudējumiem (DoS, MITM u.c.);
* uzraudzību ar IDPS, SIEM un SOC risinājumiem.

# PLĀNOŠANA UN PĀRSKATĪŠANAS PASĀKUMI

##  Informācijas drošības integrācija organizācijas procesos

Informācija par to, kā informācijas drošība tiek sistemātiski integrēta organizācijas stratēģijā, operatīvajos procesos un projektos. Plānošana balstīta uz riska novērtējumu, atbilstības prasībām un biznesa mērķiem.

##  Riska apstrādes pasākumu īstenošana

Informācija par to, kā identificētie riski tiek praktiski apstrādāti – ieviešot, uzraugot un dokumentējot kontroles pasākumus, ar mērķi samazināt ietekmi un nepieļaut atkārtošanos. Nodrošināta atgriezeniskā saite efektivitātes novērtēšanai.

##  Izmaiņu un konfigurācijas vadība

Informācija par to, kā organizācija īsteno izmaiņu pārvaldības procesu, kas ietver:

* izmaiņu dokumentēšanu un apstiprināšanu;
* informācijas drošības ietekmes novērtēšanu;
* konfigurācijas pārvaldības procedūras;
* atjaunošanas mehānismus būtisku incidentu gadījumā.

##  Kontroļu monitorings un izvērtēšana

Informācija par to, kā tiek mērīta drošības kontroles efektivitāte:

* KPI un citu drošības rādītāju analīze;
* drošības notikumu pārskati (žurnāli, SIEM);
* tendences un draudu attīstības analīze.

##  Iekšējais audits un pašvērtējums

Informācija par regulāru auditu veikšanu, tostarp:

* Kontroļu kopuma efektivitātes pārbaudi;
* neatbilstību identificēšanu;
* korektīvo pasākumu ieviešanu;
* īpašu uzmanību pievēršot IDPS sistēmu izvērtējumam.

##  Pārvaldības pārskatīšana

Informācija par to, kā vadība pārskata informācijas drošības efektivitāti:

* balstoties uz auditēšanas un incidentu datiem;
* analizējot risku profila un ārējo prasību izmaiņas;
* pielāgojot politikas un resursus stratēģiskajiem mērķiem.

##  Politikas, procedūras un kontroles veidi

Informācija par to, kā organizācijā tiek definētas, dokumentētas un regulāri uzturētas drošības politikas, procedūras un apmācības. Praktiskas kontroles tiek piemērotas atbilstoši apdraudējumu raksturam un riska līmenim.

**Piemēram, kontroles var būt:**

|  |  |
| --- | --- |
| **Kontroles veids** | **Funkcija** |
| Preventīvās | Novērst apdraudējumus pirms to iestāšanās |
| Korektīvās | Atjaunot sistēmu darbību pēc incidenta |
| Detektīvās (identificējošās) | Atklāt un identificēt drošības notikumus |
| Atturošās | Samazināt apdraudējuma iespējamību ar psiholoģisku vai vizuālu efektu |
| Administratīvās | Noteikt rīcību, atbildības, lēmumu pieņemšanas kārtību. |

|  |
| --- |
| **Administratīvās kontroles** |
| **Kontroles nosaukums** | **Kontroles veids** | **Mērķis** |
| Minimālās piekļuves tiesības (*Least Privilege*) | Preventīvā | Samazināt apdraudējuma iespēju no iekšējiem draudiem |
| Atkopšanas plāni (*Disaster Recovery)* | Korektīvā | Nodrošināt uzņēmējdarbības nepārtrauktību |
| Paroļu politika | Preventīvā | Ierobežot konta uzlaušanas risku |
| Piekļuves kontroles politika | Preventīvā | Definēt, kurš un kādos gadījumos var piekļūt datiem |
| Kontu pārvaldības politika | Preventīvā | Ierobežot risku no pamestiem vai noklusētiem kontiem |
| Darbu nodalīšana | Preventīvā | Ierobežot piekļuvi un novērst ļaunprātīgu rīcību risku |
| **Tehniskās kontroles** |
| **Kontroles nosaukums** | **Kontroles veids** | **Mērķis** |
| Ugunsmūris (*Firewall*) | Preventīvā | Filtrēt nevēlamu tīkla trafiku |
| IDS/IPS | Detektīvā | Atklāt un reaģēt uz anomāliju |
| Šifrēšana | Atturošā | Aizsargāt sensitīvu informāciju |
| Dublēšana (*Backups*) | Korektīvā | Atjaunot datus pēc incidenta |
| Paroļu pārvaldība | Preventīvā | Samazināt paroļu izmantošanas kļūdas |
| Antivirus programmatūra | Korektīvā | Atklāt un izolēt draudus |
| Manuāla sistēmu uzraudzība | Preventīvā | Novērst riskus, kas rodas no novecojušām sistēmām |
| **Fiziskās kontroles** |
| **Kontroles nosaukums** | **Kontroles veids** | **Mērķis** |
| Dokumentu seifs | Atturošā | Samazināt fizisku apdraudējumu iespēju |
| Apgaismojums telpās | Atturošā | Ierobežot slēptu piekļuvi un riskus |
| Video novērošana | Preventīvā / Detektīvā | Gan atturošs, gan notikumu analīzei |
| Slēdzami skapji tīkla iekārtām | Preventīvā | Ierobežot piekļuvi kritiskajai infrastruktūrai |
| Signalizācijas sistēmas marķējums | Atturošā | Atturēt no ielaušanās |
| Fiziskās slēdzenes | Atturošā / Preventīvā | Novērst nesankcionētu piekļuvi |
| Ugunsgrēka atklāšanas / dzēšanas sistēmas | Detektīvā / Preventīvā | Aizsargāt fiziskos resursus no bojājumiem |