Valsts administrācijas skola

Raiņa bulvāris 4, Rīga, LV-1050, tālr. 28750160, e-pasts pasts@vas.gov.lv, www.vas.gov.lv

Rīgā

Iekšējie noteikumi

28.05.2026 Nr.1-1/3/2026

KIBERDROŠĪBAS PĀRVALDĪBAS POLITIKA

Dokuments, kas nosaka Valsts administrācijas skolas pieeju kiberdrošībai, mērķus, principus un atbildību sadalījumu

Izdots saskaņā ar
Valsts pārvaldes iekārtas likuma
72. panta pirmās daļas 2. punktu

Dokumenta versija	[1.0]
Apstiprināšanas datums	28.05.2026
Spēkā stāšanās datums	28.05.2026
Nākamā pārskatīšana	Ne retāk kā reizi gadā
Atbildīgais par dokumentu	Kiberdrošības pārvaldnieks
Subjekta statuss	Svarīgs pakalpojumu sniedzējs (Nacionālās kiberdrošības likuma izpratnē)

1. VISPĀRĪGĀ INFORMĀCIJA

Mērķis: šī politika definē Valsts administrācijas skolas (turpmāk – VAS, Iestāde) 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:

- VAS kiberdrošības mērķus un pamatprincipus;
- lomu un atbildību sadalījumu kiberdrošības pārvaldībā;
- apņemšanos ievērot drošības prasības, kas izriet no normatīvajiem aktiem, tostarp Nacionālās kiberdrošības likuma un 25.06.2025. Ministru kabineta noteikumiem Nr. 397 „Minimālās kiberdrošības prasības";
- piemērošanas jomu, norādot, uz kuriem procesiem, informācijas sistēmām un resursiem tā attiecas.

Politika attiecas uz visiem VAS darbiniekiem, ārpakalpojumu sniedzējiem, partneriem un trešajām pusēm, kas izmanto vai pārvalda VAS informācijas un komunikācijas tehnoloģiju (IKT) resursus.

1.1. Organizācijas konteksts

VAS ir tiešās valsts pārvaldes iestāde, kuras pamatuzdevums ir valsts pārvaldes darbinieku mācīšana un profesionālās pilnveides nodrošināšana. VAS regulāri identificē un izvērtē iekšējos un ārējos faktorus, kas ietekmē kiberdrošības mērķu sasniegšanu, tostarp:

- tehnoloģiju attīstību un mainīgu apdraudējumu vidi;
- normatīvās prasības un izmaiņas regulējumā (Nacionālās kiberdrošības likums, MK noteikumi Nr. 397, VDAR);
- piegādes ķēdes riskus un partneru ietekmi – VAS gandrīz visas IKT sistēmas tiek nodrošinātas kā ārpakalpojumi (SaaS un valsts kopīgie pakalpojumi), tāpēc ārpakalpojumu sniedzēju drošības līmenis ir VAS kiberdrošības konteksta būtiska sastāvdaļa;
- organizatoriskās izmaiņas un struktūras attīstību.

1.2. Ieinteresēto pušu identificēšana

VAS identificē ieinteresētās puses, kuru vajadzības un prasības attiecas uz informācijas drošību (konfidencialitāti, integritāti, pieejamību):

- VAS darbinieki un vadība;
- Mācību dalībnieki (valsts pārvaldes darbinieki) un to iestādes;
- Valsts kanceleja kā augstākā iestāde un nozares uzraudzības iestādes;
- Kiberincidentu novēršanas institūcija CERT.LV;
- Datu valsts inspekcija (personas datu jautājumos);
- Ārpakalpojumu sniedzēji un IKT pakalpojumu uzturētāji: Tiesu namu aģentūra (TNA), Latvijas Valsts radio un televīzijas centrs (LVRTC), Valsts kase, Microsoft (TNA), Intea (Docebo platforma);
- Auditori (iekšējie un ārējie).

1.3. Atbilstība nacionālajiem normatīvajiem aktiem

VAS atbilst Nacionālās kiberdrošības likuma 2. panta otrās daļas izpratnē par svarīgu pakalpojumu sniedzēju (vai citu atbilstošu kategoriju, ko nosaka kompetentā uzraudzības institūcija). VAS apņemas ievērot:

- Nacionālās kiberdrošības likumu;

- 25.06.2025. MK noteikumus Nr. 397 „Minimālās kiberdrošības prasības";
- Vispārīgo datu aizsardzības regulu (VDAR) un Fizisko personu datu apstrādes likumu;
- Valsts informācijas sistēmu likumu (ciktāl tas ir piemērojams);
- Citus piemērojamos normatīvos aktus un standartus.

VAS pamatojums kā svarīgam pakalpojumu sniedzējam tiek dokumentēts un periodiski (vismaz reizi gadā) pārskatīts.

1.4. Jomai specifiskās prasības

Papildus vispārējām drošības prasībām VAS ievēro nozares un pakalpojuma specifiskās prasības, kas izriet no:

- valsts pārvaldes darbības regulējuma un Valsts pārvaldes iekārtas likuma;
- izglītības pakalpojumu sniegšanas specifikas (mācību dalībnieku personas datu apstrāde, sertifikātu izsniegšana);
- valsts kopīgo IKT pakalpojumu izmantošanas prasībām (Valsts kase, TNA, LVRTC infrastruktūras lietošanas noteikumi).

Šīs prasības tiek dokumentētas un integrētas informācijas drošības vadībā, kā arī pārskatītas riska izvērtēšanas gaitā.

2. INFORMĀCIJAS SISTĒMAS PĀRVALDĪBA

2.1. Pārvaldības apņemšanās

VAS direktors apņemas nodrošināt kiberdrošības pārvaldību VAS, integrējot drošības mērķus iestādes stratēģijā un piešķirot nepieciešamos resursus. Direktors:

- apstiprina kiberdrošības pārvaldības politiku un saistītos dokumentus;
- nodrošina finanšu un personāla resursus kiberdrošības pasākumu īstenošanai;
- iesaistās drošības plānošanā, uzraudzībā un izvērtēšanā;
- saņem ikgadējus pārskatus par kiberdrošības stāvokli iestādē un pieņem lēmumus par korekcijām.

2.2. Informācijas drošības politika

VAS ir izstrādāta, ieviesta un tiek regulāri uzturēta informācijas drošības dokumentu kopa, kas nosaka:

- drošības mērķus un principus;
- attieksmi pret riskiem un riska pieņemamības līmeņus;
- atbilstību normatīvajiem aktiem;
- atbildības sadalījumu.

Kiberdrošības dokumentu kopā ietilpst:

- Kiberdrošības pārvaldības politika (šis dokuments);
- Kiberdrošības procedūru politika;
- IKT resursu un informācijas sistēmu katalogs;
- Kiberrisku pārvaldības un IKT darbības nepārtrauktības plāns;
- Kiberincidentu pārvaldības kārtība un kiberincidentu žurnāls.

Politika tiek pārskatīta vismaz reizi gadā vai pēc būtiskām izmaiņām (organizatoriskām, tehnoloģiskām vai normatīvām).

2.3. Lomas, pienākumi un atbildība

VAS kiberdrošības pārvaldības struktūra ir skaidri definēta un dokumentēta. Lomas un atbildības:

Loma	Pienākumi un atbildība
VAS direktors	Apstiprina kiberdrošības politikas; nodrošina resursus; pieņem stratēģiskus lēmumus; atbild par iestādes kopējo kiberdrošības stāvokli; pieņem lēmumus par augsta līmeņa risku apstrādi.
Kiberdrošības pārvaldnieks	Izstrādā un uztur kiberdrošības dokumentāciju; veic risku novērtēšanu; saskaņo ārpakalpojumu līgumus to kiberdrošības aspektos; pārvalda kiberincidentus un to ziņošanu CERT.LV; uzrauga ārpakalpojumu sniedzēju izpildi; veic darbinieku informētības pasākumus; sagatavo pašvērtējumus.
Resursu īpašnieki (struktūrvienību vadītāji)	Nosaka informācijas un IKT resursu klasifikāciju savā atbildības jomā; piešķir un atsauc piekļuves tiesības; ziņo par incidentiem un riskiem; piedalās ārpakalpojumu līgumu izstrādē.
Ārpakalpojumu sniedzēji	TNA, LVRTC, Valsts kase, Intea u.c. – atbild par konkrēto IKT pakalpojumu tehnisko drošību saskaņā ar līgumu un SLA noteikumiem; ziņo VAS par incidentiem un izmaiņām; nodrošina rezerves kopēšanu un atjaunošanu.
Personas datu aizsardzības speciālists (DPO)	Konsultē par personas datu apstrādes drošības jautājumiem; sadarbojas ar kiberdrošības pārvaldnieku incidentu gadījumos, kas skar personas datus.
Visi darbinieki	Ievēro kiberdrošības politikas un procedūras; nekavējoties ziņo par drošības incidentiem un aizdomīgām aktivitātēm; piedalās apmācībās.

Informācija par lomām un atbildībām tiek nodota darbiniekiem ievadinstruktāžās, apmācībās un iekšējās komunikācijas kanālos.

2.3.1. Atbildīgo personu kontaktinformācija

Vārds, uzvārds	Amats un atbildība	E-pasts	Tālrunis
Agita Kalviņa	VAS direktore	agita.kalvina@vas.gov.lv	29255772
Ojārs Vintišs	Kiberdrošības pārvaldnieks	ojars.vintiss@vas.gov.lv	27007737
Jānis Kāršenieks	Personas datu aizsardzības speciālists	janis.karsenieks@inbox.lv	20043645

2.4. Pārbaudes un auditi

VAS regulāri tiek veiktas kiberdrošības pārbaudes un auditi, lai:

- novērtētu iekšējās drošības kontroļu vidi un tās atbilstību politikām;
- identificētu šī brīža kiberdrošības stāvokli;
- novērtētu ārpakalpojumu sniedzēju izpildi atbilstoši līgumiem un SLA;
- plānotu uzlabojumus, balstoties uz konstatētajām neatbilstībām.

Tiek veikti:

- ikgadējais kiberdrošības pašvērtējums atbilstoši MK noteikumiem Nr. 397;

- iekšējās kontroles pārbaudes – atbilstoši VAS iekšējās kontroles plānam;
- ārējie auditi – nepieciešamības gadījumā vai pēc uzraudzības institūciju pieprasījuma;
- ārpakalpojumu sniedzēju pārskatu un atbilstības apliecinājumu izvērtēšana.

Rezultāti tiek dokumentēti un izmantoti vadības pārskatam un risku reģistra aktualizācijai.

2.6. Atbildības

Katrs VAS darbinieks, ārpakalpojumu sniedzēja pārstāvis vai trešās puses pārstāvis, kas piekļūst VAS informācijas sistēmām vai datiem, ir personīgi atbildīgs par:

- kiberdrošības politiku un procedūru ievērošanu;
- piešķirto piekļuves tiesību izmantošanu tikai amata pienākumu izpildei;
- nekavējošu ziņošanu par konstatētiem vai aizdomīgiem drošības notikumiem;
- konfidencialitātes saglabāšanu attiecībā uz iegūto informāciju arī pēc darba tiesisko attiecību vai līguma izbeigšanas.

Politikas pārkāpumi var radīt disciplināratbildību darbiniekiem atbilstoši Darba likumam, kā arī līgumiskas sekas ārpakalpojumu sniedzējiem.

2.9. Informētība

VAS uztur darbinieku informētības līmeni par informācijas drošību, nodrošinot:

- piekļuvi spēkā esošajām politikām un instrukcijām VAS iekšējos resursos (SharePoint);
- ievadapmācību kiberdrošības jautājumos visiem jaunajiem darbiniekiem ne vēlāk kā mēneša laikā no darba uzsākšanas;
- ikgadējas atkārtotās apmācības visiem darbiniekiem;
- informatīvas kampaņas un brīdinājumus par aktuāliem apdraudējumiem (piem., aktuālām pikšķerēšanas tendencēm);
- regulāras pārbaudes (piem., simulētas pikšķerēšanas kampaņas).

Informētības pasākumu rezultāti (līdzdalības līmenis, testu rezultāti) tiek dokumentēti.

3. RISKU PĀRVALDĪBA

3.1. Riska novērtēšana

VAS tiek veikta regulāra kiberdrošības risku novērtēšana, lai identificētu potenciālos apdraudējumus, ievainojamības un to iespējamo ietekmi uz konfidencialitāti, integritāti un pieejamību. Riska novērtēšanas process ietver:

- informācijas aktīvu un IKT resursu identificēšanu un klasificēšanu (atbilstoši IKT resursu katalogam);
- draudu un ievainojamību analīzi, t.sk. ārpakalpojumu sniedzēju radīto risku izvērtēšanu;
- riska līmeņa aprēķinu (ietekme × iespējamība, skalā 1–5);
- prioritāšu noteikšanu un riska pieņemamības izvērtēšanu.

Novērtēšana tiek veikta:

- vismaz reizi gadā;
- pēc būtiskām izmaiņām IKT vidē (jauna sistēma, ārpakalpojuma maiņa, jauns pakalpojumu sniedzējs);
- pēc nozīmīga kiberincidenta;
- pēc būtiskām izmaiņām normatīvajā regulējumā vai apdraudējumu ainavā.

Detalizēta metodoloģija aprakstīta dokumentā „Kiberrisku pārvaldības un IKT darbības nepārtrauktības plāns”.

3.2. Riska apstrāde

Pamatojoties uz risku novērtēšanas rezultātiem, VAS izstrādā risku apstrādes plānus, izvēloties vienu no šādām stratēģijām:

- Riska samazināšana – ieviešot kontroles pasākumus, lai ierobežotu risku līdz pieņemamam līmenim;
- Riska izvairīšanās – atsakoties no darbības vai pakalpojuma, kas rada nepieņemamu risku;
- Riska pārnešana – uz trešajām pusēm, izmantojot līgumu noteikumus, apdrošināšanu vai ārpakalpojumu deleģēšanu;
- Riska pieņemšana – attiecībā uz zema līmeņa, kontrolētiem riskiem ar dokumentētu pamatojumu un atbildīgās personas apstiprinājumu.

Tā kā VAS IKT sistēmas pārsvarā tiek nodrošinātas ārpakalpojumā, daudzi tehniskie riski tiek pārvaldīti caur līgumos iekļautām drošības prasībām un SLA. Riska apstrādes plāni tiek dokumentēti, pārskatīti un piesaistīti konkrētām atbildīgajām personām un termiņiem.

3.3. Informācijas drošības mērķi

VAS nosaka konkrētus, izmērāmus un sasniedzamus kiberdrošības mērķus, kas atbilst iestādes stratēģijai un riska profilam. Galvenie mērķi:

- Nodrošināt mācību pakalpojumu un atbalsta sistēmu pieejamību darba laikā ne zemāku par līgumos noteikto SLA līmeni;
- Aizsargāt mācību dalībnieku un darbinieku personas datus pret nesankcionētu piekļuvi vai izpaušanu;
- Nodrošināt 100% nozīmīgo kiberincidentu ziņošanu CERT.LV normatīvajos aktos noteiktajos termiņos;
- Sasniegt vismaz 95% darbinieku gada apmācību pabeigšanas rādītāju;
- Nodrošināt visu jauno ārpakalpojumu līgumu izvērtēšanu no kiberdrošības viedokļa pirms parakstīšanas.

Mērķi tiek pārskatīti reizi gadā un to izpilde tiek vērtēta ikgadējā pārskatā direktoram.

3.4. Aizsardzība pret riskiem un apdraudējumiem

VAS īsteno integrētus drošības pasākumus risku ietekmes pārvaldīšanai. Ņemot vērā, ka tehniskā infrastruktūra ir ārpakalpojumā, atbildības tiek dalītas:

a) Administratīvās kontroles (VAS atbildība):

- drošības politikas, procedūras un piekļuves tiesību pārvaldība;
- personāla apmācība un uzvedības standarti;
- risku pārvaldība un atbilstības kontrole;
- ārpakalpojumu līgumu izvērtēšana un uzraudzība.

b) Tehniskās kontroles (galvenokārt ārpakalpojumu sniedzēju atbildība):

- ugunsmūri, IDS/IPS – tīkla iekārtas (Palo Alto) – uztur TNA;
- antivīrusu un EDR risinājumi gala iekārtās;
- datu šifrēšana glabāšanā un pārraidē, autentifikācija un tīkla segmentācija;
- VPN piekļuve – uztur TNA;
- e-pasta un SharePoint drošība (Microsoft 365) – uztur TNA.

c) Fiziskās kontroles:

- VAS biroja telpu piekļuves kontrole (kartes/atslēgas);
- videonovērošana (ja piemērojama);

- datu centru fiziskās kontroles tiek nodrošinātas ārpakalpojumu sniedzēju pusē (LVRTC, Valsts kase, Microsoft datu centri).

3.5. Nepārtrauktības un incidentu reaģēšanas plāni

VAS samazina sistēmu dīkstāves un operacionālo ietekmi apdraudējumu gadījumā, izstrādājot un regulāri pārskatot un, nepieciešamības gadījumā, testējot:

Incidentu reaģēšanas plāns:

- nodrošina ātru un strukturētu rīcību kiberincidentu gadījumā;
- ietver atbildīgos, saziņas kārtību un eskalācijas soļus, tostarp komunikāciju ar ārpakalpojumu sniedzējiem;
- ir saskaņots ar ziņošanas prasībām atbilstoši Nacionālās kiberdrošības likumam un MK noteikumiem Nr. 397;
- detalizēti aprakstīts dokumentā „Kiberincidentu pārvaldības kārtība un kiberincidentu žurnāls".

Darbības nepārtrauktības plāns (BCP):

- apraksta rīcību fizisku draudu gadījumā (ugunsgrēks, plūdi u.c.) un IKT pakalpojumu pārtraukuma gadījumā;
- nosaka kritisko pakalpojumu RTO/RPO/MTD vērtības;
- definē atjaunošanas secību un atbildības, t.sk. komunikāciju ar ārpakalpojumu sniedzējiem;
- integrēts ar katastrofu atjaunošanas plānu (DRP) – rezerves kopēšanas un atjaunošanas procedūras tiek nodrošinātas ārpakalpojumu sniedzēju pusē saskaņā ar līgumiem;
- detalizēti aprakstīts dokumentā „Kiberrisku pārvaldības un IKT darbības nepārtrauktības plāns".

4. KONTROLES

4.1. Politikas, apmācības un pieejamības plāni

VAS izstrādā, apstiprina un regulāri pārskata kiberdrošības politikas un procedūras, kas definē standartus un prasības visos drošības aspektos. Politikas tiek pārskatītas vismaz reizi gadā vai pēc būtiskām izmaiņām.

Pieejamības plāni nodrošina sistēmu un datu atjaunošanu pēc incidentiem un ir integrēti darbības nepārtrauktības stratēģijā. Tā kā IKT sistēmas tiek nodrošinātas ārpakalpojumā, atjaunošanas darbības tiek koordinētas ar attiecīgajiem pakalpojumu sniedzējiem saskaņā ar SLA noteikumiem.

4.2. Fiziskā drošība

VAS biroja telpu fiziskā drošība:

- piekļuves kontrole VAS telpām un kritiskajām zonām ar autentifikācijas līdzekļiem (kartes/atslēgas);
- darba staciju un mobilo iekārtu fiziska aizsardzība darba vietā un ārpus tās;
- tukša galda principa ievērošana attiecībā uz dokumentiem ar ierobežotas pieejamības informāciju;
- ekrāna bloķēšana, darbinieku atstājot darba vietu.

Datu centru fiziskā drošība (serveri, tīkla iekārtas) tiek nodrošināta ārpakalpojumu sniedzēju pusē (LVRTC, Microsoft, Valsts kase, Dochebo datu centri Eiropā) atbilstoši attiecīgo organizāciju drošības standartiem un līgumos noteiktajām prasībām.

4.3. Personāla drošība un identitātes pārvaldība (IAM)

VAS īsteno identitātes un piekļuves pārvaldību (IAM) atbilstoši šādiem principiem:

- minimālo nepieciešamo piekļuves tiesību princips (least privilege);
- lomu balstīta piekļuves kontrole (RBAC);
- daudzfaktoru autentifikācija (MFA) attiecībā uz VPN, e-pastu un kritiskām sistēmām (nodrošina TNA un Microsoft 365);
- piekļuves tiesību dzīves cikla pārvaldība – piešķiršana darba uzsākšanas brīdī, izmaiņas pārcelšanas/lomas maiņas gadījumā, atsaukšana darba attiecību izbeigšanas brīdī;
- regulāra (vismaz reizi gadā) piekļuves tiesību pārskatīšana visās sistēmās;
- privileģēto kontu īpaša uzraudzība un dokumentēšana.

Personāla drošības prasības tiek iekļautas darba līgumos un amata aprakstos, nodrošinot konfidencialitātes prasību saglabāšanos arī pēc darba tiesisko attiecību izbeigšanas.

4.4. Apmācība un informētība

VAS nodrošina darbiniekiem:

- ievadapmācību kiberdrošības jautājumos visiem jaunajiem darbiniekiem;
- ikgadējas atkārtotās apmācības;
- specializētu apmācību darbiniekiem ar paaugstinātām atbildībām (vadība, darbinieki ar privileģētām piekļuvēm);
- informatīvas kampaņas par aktuāliem apdraudējumiem (pikšķerēšana, sociālā inženierija, ļaunatūra);
- zināšanu pārbaudi (testus, simulētas pikšķerēšanas kampaņas).

Apmācību plāns tiek izstrādāts katra gada sākumā un to izpilde tiek dokumentēta.

4.5. Tīkla un darba staciju drošība

Tīkla drošības pasākumus VAS infrastruktūrā nodrošina TNA kā ārpakalpojuma sniedzējs:

- ugunsmūris (Palo Alto) ar tīkla segmentācijas politikām;
- VPN risinājums attālinātajai piekļuvei ar MFA;
- WiFi pārvaldība ar autentifikāciju un šifrēšanu;
- tīkla satiksmes uzraudzība un anomāliju identificēšana.

Darba staciju drošība:

- darba staciju standartizēta konfigurācija;
- antivīrusu/EDR risinājumi;
- regulāri operētājsistēmas un programmatūras atjauninājumi (patch management);
- diska šifrēšana (BitLocker vai līdzvērtīgs);
- ekrāna automātiska bloķēšana pēc neaktivitātes perioda.

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.

4.6. Piekļuves kontrole, šifrēšana un atjauninājumi

VAS nodrošina:

- lomu balstītu piekļuves kontroli (RBAC) visās informācijas sistēmās;

- daudzfaktoru autentifikāciju (MFA) attālinātai piekļuvei un kritiskām sistēmām;
- datu šifrēšanu glabāšanā un pārraidē (TLS, šifrētas datu nesēju glabātuves);
- programmatūras drošības ielāpu (patch) regulāru piemērošanu – darba staciju līmenī koordinēti ar TNA, sistēmu līmenī koordinēti ar attiecīgajiem ārpakalpojumu sniedzējiem;
- novecojušas programmatūras nomaiņas plānošanu.

4.9. Kaitīgā programmatūra (Malware) un aizsardzība

VAS īsteno aizsardzību pret ļaunatūru:

- antivīrusu / EDR risinājumi visās darba stacijās un serveros;
- e-pasta filtrēšana un pielikumu skenēšana (nodrošina Microsoft 365 / TNA);
- tīmekļa satiksmes filtrēšana (TNA);
- protokolu ierobežošana un nevēlamu portu bloķēšana;
- lietotāju informētība par ļaunatūras izplatīšanas veidiem;
- principa „nulles uzticība" (zero trust) elementu pakāpeniska ieviešana.

4.10. Ārpakalpojumu pārvaldība

Tā kā VAS gandrīz visas IKT sistēmas tiek nodrošinātas kā ārpakalpojumi, ārpakalpojumu pārvaldībai ir kritiska nozīme. VAS izmanto šādus galvenos ārpakalpojumu sniedzējus:

Sistēma / pakalpojums	Sniedzējs	Apraksts
MAS (Docebo)	Intea (SaaS)	Mācīšanās un attīstības sistēma; serveri Eiropā; rezerves kopēšana sniedzēja pusē
MPS	TNA (LVRTC infrastruktūrā)	Iepriekšējā mācīšanās sistēma; funkcionāli vairs netiek uzturēta
E-pasts, SharePoint (M365)	TNA / Microsoft	Komunikācijas un sadarbības platforma
Horizon	Valsts kase (VPC)	Grāmatvedības sistēma
Namejs	[precizējams]	Dokumentu pārvaldības sistēma
Mājaslapa	VRAA (TVP projekts)	Iekļauta valsts pārvaldes vienotajā mājaslapu platformā
Tīkls, WiFi, ugunsmūris (Palo Alto)	TNA	VAS biroja tīkla infrastruktūra
VPN	TNA	Attālinātās piekļuves nodrošināšana

VAS ārpakalpojumu pārvaldības principi:

- līgumos tiek iekļautas drošības prasības un atbildības sadalījums;
- tiek veikts ārpakalpojuma sniedzēja sākotnējais kiberdrošības riska novērtējums pirms līguma slēgšanas;
- tiek uzraudzīta līguma izpilde – SLA rādītāji, atskaites, atbilstības apliecinājumi;
- tiek dokumentēta datu nodošana trešajām pusēm;
- ārpakalpojumi ir iekļauti VAS nepārtrauktības plānos;
- kiberdrošības pārvaldnieks saskaņo visus jaunos ārpakalpojumu līgumus pirms to parakstīšanas (atbilstoši MK noteikumiem Nr. 397);

- tiek pārbaudīta atbilstība normatīvo aktu prasībām, t.sk. VDAR (apstrādātāju līgumi).

4.11. Uzraudzība, žurnālfaili un auditi

VAS nodrošina:

- drošības notikumu žurnālu uzraudzību – tehniskā līmenī to nodrošina ārpakalpojumu sniedzēji (TNA, Microsoft, Intea u.c.);
- VAS kiberdrošības pārvaldnieks pieprasa un izvērtē ārpakalpojumu sniedzēju drošības pārskatus un atskaites;
- iekšējās un ārējās auditu rezultātu dokumentēšanu un seku darbības;
- incidentu analīzi un uzlabošanas pasākumu identificēšanu;
- konfigurācijas izmaiņu kontroli.

4.12. Datu rezerves kopēšana un atjaunošana

Datu rezerves kopēšanu un atjaunošanu galvenokārt nodrošina ārpakalpojumu sniedzēji saskaņā ar līgumos noteiktajām prasībām:

- MAS (Docebo) – rezerves kopēšanu nodrošina Intea atbilstoši SaaS pakalpojuma noteikumiem;
- E-pasts un SharePoint – atbilstoši Microsoft 365 standartiem (papildus konfigurējams caur TNA);
- Horizon – atbilstoši Valsts kases pakalpojuma noteikumiem;
- MPS, Namejs, mājaslapa – atbilstoši attiecīgā uzturētāja noteikumiem;
- Tīkla iekārtu konfigurāciju rezerves kopēšana – TNA atbildība.

VAS kiberdrošības pārvaldnieks reizi gadā pārbauda ārpakalpojumu sniedzēju rezerves kopēšanas un atjaunošanas procedūru piemērotību un, ja iespējams, līdzdarbojas atjaunošanas testos.

4.13. Iznīcināšana

VAS nodrošina drošu datu un datu nesēju iznīcināšanu:

- elektronisko datu nesēju (cietie diski, USB datu nesēji) droša iznīcināšana vai pārrakstīšana pirms nodošanas trešajām pusēm vai utilizācijas;
- papīra dokumentu ar ierobežotas pieejamības informāciju iznīcināšana ar smalcinātāju vai ar sertificēta pakalpojuma starpniecību;
- datu dzēšana ārpakalpojumu sniedzēju sistēmās līguma izbeigšanas gadījumā – atbilstoši līgumā noteiktajām procedūrām un VDAR prasībām;
- datu glabāšanas un dzēšanas termiņu ievērošana atbilstoši personas datu apstrādes mērķiem.

5. INCIDENTU PĀRVALDĪBA

5.1. Atbildības sadalījums

VAS incidentu pārvaldībā tiek piemērots RACI princips:

- R (Responsible) – persona, kas praktiski veic uzdevumu;
- A (Accountable) – persona, kas nes atbildību un pieņem gala lēmumu (parasti viena persona);
- C (Consulted) – konsultantu loma; iesaistāmie pirms rīcības;
- I (Informed) – personas, kuras tikai informējamas.

Aktivitāte	Izpildītājs (R)	Atbildīgs (A)	Iesaistītais (C)	Informējamais (I)
Incidenta identificēšana	Darbinieki, ārpakalpojumu sniedzēji	Kiberdrošības pārvaldnieks	Ārpakalpojumu sniedzēji	Direktors
Incidenta reģistrēšana žurnālā	Kiberdrošības pārvaldnieks	Kiberdrošības pārvaldnieks	Ārpakalpojumu sniedzēji	Direktors
Klasifikācija un analīze	Kiberdrošības pārvaldnieks	Kiberdrošības pārvaldnieks	Ārpakalpojumu sniedzēji, DPO	Direktors
Ierobežošana un novēršana	Ārpakalpojumu sniedzēji	Kiberdrošības pārvaldnieks	Resursu īpašnieki	Direktors, CERT.LV
Ziņošana CERT.LV	Kiberdrošības pārvaldnieks	Direktors	DPO (ja skarti dati)	VAS vadība
Atjaunošana	Ārpakalpojumu sniedzēji	Kiberdrošības pārvaldnieks	Resursu īpašnieki	Direktors, lietotāji
Pēc-incidenta analīze	Kiberdrošības pārvaldnieks	Direktors	Ārpakalpojumu sniedzēji	VAS vadība

5.2. Sadarbība ar iekšējām un ārējām pusēm

VAS uztur sadarbību un komunikāciju ar:

- iekšējām pusēm: VAS direktoru un vadību, struktūrvienību vadītājiem (resursu īpašniekiem), darbiniekiem, personas datu aizsardzības speciālistu;
- ārpakalpojumu sniedzējiem: TNA, LVRTC, Valsts kasi, Microsoft (caur TNA), Intea, kā arī mājaslapas un dokumentu pārvaldības sistēmas uzturētājiem;
- kiberincidentu novēršanas institūciju CERT.LV;
- Datu valsts inspekciju – ja incidents skar personas datus;
- Valsts policiju – ja konstatēta noziedzīga rīcība;
- Valsts kanceleju – attiecīgā informēšanas kārtībā.

5.3. Darbības pēc incidenta

Pēc katra nozīmīga vai augstas ietekmes incidenta tiek veiktas šādas darbības:

- cēloņu analīze (root cause analysis) un risku izvērtēšana;
- politiku, procedūru un kontroles mehānismu pārskatīšana;
- darbinieku informēšana un apmācības, balstoties uz incidenta laikā gūtajām mācībām;
- ārpakalpojumu līgumu (SLA/OLA) un sadarbības nosacījumu pārskatīšana, ja incidents notika ārpakalpojuma sniedzēja pusē;
- korektīvo darbību plāna izstrāde ar termiņiem un atbildīgajiem;
- ziņojums VAS direktoram.

5.4. Uzraudzība un nepārtraukta uzlabošana

VAS uztur incidentu pārvaldības kvalitāti, izmantojot:

- regulārus iekšējos auditus un kontroļu testēšanu;
- ārpakalpojumu sniedzēju drošības uzraudzības atskaišu izvērtēšanu;
- korektīvās un preventīvās darbības pēc incidentiem;

- incidentu pārvaldības kārtības regulāru pārskatīšanu (vismaz reizi gadā vai pēc augstas ietekmes incidenta).

6. ATBILSTĪBAS PĀRBAUDE

6.1. Atbilstība normatīvajiem aktiem

VAS nodrošina atbilstību visām piemērojamām normatīvajām prasībām, tostarp:

- Nacionālās kiberdrošības likumam;
- 25.06.2025. MK noteikumiem Nr. 397 „Minimālās kiberdrošības prasības";
- Vispārīgajai datu aizsardzības regulai (VDAR) un Fizisko personu datu apstrādes likumam;
- Valsts pārvaldes iekārtas likumam;
- citiem piemērojamiem normatīvajiem aktiem.

Atbilstība tiek izvērtēta ikgadējā pašvērtējumā un dokumentēta.

6.2. Atbilstība drošības prasībām

VAS 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);
- minimālo piekļuves tiesību principa (least privilege) izmantošanu;
- regulāru piekļuves tiesību pārskatīšanu (vismaz reizi gadā);
- privātuma un konfidencialitātes aizsardzības līdzekļiem.

VAS pārvalda informācijas aktīvus visā to dzīves ciklā, nodrošinot:

- identificēšanu, klasifikāciju un īpašnieku noteikšanu (IKT resursu katalogā);
- datu aizsardzību (tai skaitā personas datu);
- glabāšanas termiņu un drošas iznīcināšanas noteikšanu.

Tīkla drošība tiek nodrošināta ar ārpakalpojuma sniedzēja TNA palīdzību:

- tīkla segmentāciju, VPN, perimetra aizsardzību;
- drošu pārsūtīšanu (TLS, IPsec);
- aizsardzību pret tīkla apdraudējumiem;
- uzraudzību (IDPS un SIEM elementi).

7. PLĀNOŠANA UN PĀRSKATĪŠANAS PASĀKUMI

7.1. Informācijas drošības integrācija organizācijas procesos

Kiberdrošība tiek sistemātiski integrēta VAS stratēģijā, operatīvajos procesos un projektos. Plānošana balstīta uz riska novērtējumu, atbilstības prasībām un iestādes mērķiem. Kiberdrošības prasības tiek ietvertas:

- iepirkumu un ārpakalpojumu līgumu izstrādē (kiberdrošības pārvaldnieks obligāti saskaņo);
- personāla atlases un apmācības procesos;
- izmaiņu pārvaldības procedūrās;
- projektu vadībā.

7.2. Riska apstrādes pasākumu īstenošana

Identificētie riski tiek praktiski apstrādāti, ieviešot, uzraugot un dokumentējot kontroles pasākumus. Tiek nodrošināta atgriezeniskā saite efektivitātes novērtēšanai. Risku reģistrs tiek aktualizēts vismaz reizi gadā un pēc katras būtiskas izmaiņas.

7.3. Izmaiņu un konfigurācijas vadība

VAS izmaiņu pārvaldības process ietver:

- izmaiņu dokumentēšanu un apstiprināšanu;
- kiberdrošības ietekmes novērtēšanu pirms izmaiņas;
- saskaņošanu ar ārpakalpojumu sniedzējiem (TNA, Intea u.c.) attiecībā uz to pārvaldītajām sistēmām;
- konfigurācijas pārvaldības procedūras (tehniskā izpilde galvenokārt ārpakalpojumu sniedzēju pusē);
- atjaunošanas mehānismus būtisku incidentu gadījumā.

7.4. Kontroļu monitorings un izvērtēšana

Kontroļu efektivitāte tiek mērīta, izmantojot:

- KPI un citus drošības rādītājus (apmācību pabeigšana, incidentu skaits, ziņošanas termiņi, ārpakalpojumu SLA izpilde);
- ārpakalpojumu sniedzēju drošības notikumu pārskatus un atskaites;
- tendences un draudu attīstības analīzi;
- iekšējās kontroles ziņojumus.

7.5. Iekšējais audits un pašvērtējums

VAS veic:

- ikgadējo kiberdrošības pašvērtējumu atbilstoši MK noteikumiem Nr. 397;
- iekšējās kontroles pārbaudes atbilstoši iestādes plānam;
- neatbilstību identificēšanu un korektīvo pasākumu ieviešanu;
- ārpakalpojumu sniedzēju atbilstības apliecinājumu izvērtēšanu;
- ārējos auditus pēc uzraudzības institūciju pieprasījuma.

7.6. Pārvaldības pārskatīšana

VAS direktors reizi gadā pārskata kiberdrošības pārvaldības efektivitāti:

- balstoties uz auditu un incidentu datiem;
- analizējot riska profila un ārējo prasību izmaiņas;
- izvērtējot ārpakalpojumu sniedzēju izpildi;
- pielāgojot politikas un resursus stratēģiskajiem mērķiem.

7.7. Politikas, procedūras un kontroles veidi

VAS izstrādātās kontroles pēc to funkcijas iedalāmas:

Kontroles veids	Funkcija
Preventīvās	Novērst apdraudējumus pirms to iestāšanās
Detektīvās	Atklāt un identificēt drošības notikumus

Korektīvās	Atjaunot sistēmu darbību pēc incidenta
Atturošās	Samazināt apdraudējuma iespējamību ar psiholoģisku vai vizuālu efektu
Administratīvās	Noteikt rīcību, atbildības un lēmumu pieņemšanas kārtību

VAS specifikā galvenā atbildība un tiešās kontroles tiek nodrošinātas administratīvā līmenī (politikas, līgumi ar ārpakalpojumu sniedzējiem, apmācības, risku pārvaldība), savukārt tehniskās kontroles tiek nodrošinātas caur ārpakalpojumu sniedzēju izpildi un uzraudzību.

APSTIPRINĀŠANA UN PĀRSKATĪŠANA

Sagatavoja	**Apstiprināja**
Kiberdrošības pārvaldnieks Ojārs Vintišs*	VAS direktore Agita Kalviņa*

Šī politika tiek pārskatīta vismaz reizi gadā vai pēc būtiskām izmaiņām normatīvajā regulējumā, organizācijas struktūrā vai IKT vidē. Par pārskatīšanu atbildīgs VAS kiberdrošības pārvaldnieks.

**Dokuments ir parakstīts ar drošu elektronisko parakstu un satur laika zīmogu*