APSTIPRINĀTA
ar Sabiedrisko elektronisko plašsaziņas līdzekļu padomes
05.06.2025. lēmumu Nr.30/1-1

APSTIPRINĀTA
ar VSIA "Latvijas Sabiedriskais medijs"
27.05.2025. valdes lēmumu Nr. 57/2-2

KIBERDROŠĪBAS POLITIKA

1. Politikā lietotie termini

1.1. **Auditācijas pieraksti** - informācijas sistēmu ieraksti, kuros tiek reģistrēti būtiski LSM IKT darbības notikumi, tostarp piekļuve informācijai, tās ievade, izmaiņas, dzēšana vai izvade, atbilstoši konkrētās sistēmas specifikai.
1.2. **Autentifikācija** – process, ar kura palīdzību sistēma pārbauda lietotāja identitāti pirms piekļuves piešķiršanas informācijas sistēmām vai resursiem.
1.3. **Autentiskums** – informācijas vai lietotāja patiesuma un identitātes apliecināšana.
1.4. **Autorizācija** – process, kurā lietotājam pēc autentifikācijas tiek piešķirtas konkrētas tiesības veikt noteiktas darbības vai piekļūt konkrētiem resursiem.
1.5. **CERT.LV** – informācijas tehnoloģiju drošības incidentu novēršanas institūcija, kas ir Latvijas kompetentā iestāde un kas atbild par informācijas tehnoloģiju drošības incidentu novēršanu un koordinēšanu valsts mērogā.
1.6. **GDPR** (General Data Protection Regulation) – ES Vispārīgā datu aizsardzības regula, kas nosaka prasības personas datu aizsardzībai.
1.7. **Ievainojamība** – informācijas un komunikācijas tehnoloģiju (IKT) vai ar tām saistītu pakalpojumu vājums, nepilnība vai kļūda, kuru var izmantot kiberapdraudējums, lai iegūtu nesankcionētu piekļuvi, traucētu darbību vai apdraudētu datu drošību.
1.8. **IKT** – informācijas un komunikācijas tehnoloģijas.
1.9. **IKT resursi** – tīklu un informācijas sistēmu sastāvdaļa. IKT resursu kopums ietver tehniskos resursus un informācijas resursus, kā arī fizisko infrastruktūru, kurā uztur minētos resursus.
1.10. **Informācijas sistēmu resursu turētājs** - persona, kas atbild par konkrētas informācijas sistēmas satura un piekļuves pārvaldību, klasifikāciju un atbilstību drošības prasībām.
1.11. **Informācijas resurss** – strukturēta digitālo datu vienība (tai skaitā datne jeb fails), kas tiek elektroniski apstrādāta, izmantojot informācijas sistēmas un tehniskos resursus.
1.12. **Integritāte** – informācijas precizitātes un pilnīguma saglabāšana visā tās dzīves ciklā.
1.13. **IS** (informācijas sistēma) – organizēta sistēma, kas paredzēta informācijas resursu pārvaldībai un elektroniskajai apstrādei, izmantojot tehniskos resursus.
1.14. **Kiberapdraudējums** – jebkādi iespējami apstākļi, notikums vai darbība, kas varētu radīt bojājumus vai traucējumus, vai citādi negatīvi ietekmēt tīklu un informācijas sistēmas, to lietotājus un citas personas.
1.15. **Kiberdrošība** – pasākumu kopums, kas tiek veikts, lai aizsargātu informācijas un komunikāciju tehnoloģijas sistēmas, tīklus, ierīces un datus no nesankcionētas piekļuves, izmantošanas, izpaušanas, traucējumiem, modifikācijas vai iznīcināšanas.
1.16. **Kiberdrošības pārvaldības dokumentācija** – šī politika un citi LSM iekšējie normatīvie akti, kas izstrādāti, lai noteiktu LSM ievērojamos kiberdrošības principus LSM IKT infrastruktūras pārvaldībā, uzturēšanā un lietošanā.

1.17. **Kiberdrošības pārvaldnieks** – LSM noteikta atbildīgā persona, kura īsteno un pārrauga kiberdrošības pasākumu īstenošanu.
1.18. **Kiberhigiēna** – ikdienas prakse un uzvedības principi, kas samazina kiberincidentu risku (piemēram, drošu paroļu lietošana, programmatūras atjaunināšana).
1.19. **Kiberincidents** – notikums, kas apdraud apstrādātus datus vai tādu pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus piedāvā tīklu un informācijas sistēmas vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību.
1.20. **Kiberrisks** – iespējamība, ka kāds kiberapdraudējums radīs kaitējumu IKT sistēmām, datiem vai procesiem.
1.21. **KI** (Kritiskā infrastruktūra) - Latvijas Republikā izvietoti objekti, sistēmas vai to daļas un pakalpojumi, kuri ir būtiski svarīgu sabiedrības funkciju īstenošanai, cilvēku veselības aizsardzības, drošības, ekonomiskās vai sociālās labklājības nodrošināšanai, kā arī kuru iznīcināšana vai darbības traucējumi būtiski ietekmētu valsts un sabiedrības pamatfunkciju īstenošanu.
1.22. **Konfidencialitāte** – princips, kas nodrošina, ka informācija ir pieejama tikai pilnvarotām personām.
1.23. **Lietotājs** – LSM darbinieks, kontraktors, partneris vai praktikants, kam piešķirtas tiesības piekļūt LSM informācijas resursiem vai informācijas sistēmai/–ām.
1.24. **MFA** (daudzfaktoru autentifikācija) – autentifikācijas metode, kurā lietotāja identitāte tiek apstiprināta, izmantojot vismaz divus dažādus faktorus: zināšanas (parole), īpašumā esošs (ierīce) vai biometriskie dati.
1.25. **Nacionālais kiberdrošības centrs** (NKC) – Latvijas kompetentā iestāde kiberdrošības jomā, kas atbild par būtisko un svarīgo pakalpojumu sniedzēju uzraudzību, kā arī koordinē kiberdrošības politikas īstenošanu valstī.
1.26. **Pieejamība** – informācijas vai pakalpojumu nodrošināšana lietotājiem pēc nepieciešamības laikā un apjomā.
1.27. **RPO** (Recovery Point Objective) – maksimālais pieļaujamais datu apjoms, ko var zaudēt incidenta rezultātā, mērot no pēdējās datu rezerves kopijas veikšanas brīža.
1.28. **RTO** (Recovery Time Objective) – maksimālais pieļaujamais laiks, kurā pēc incidenta sistēmai jāatjauno darbība.
1.29. **SAB** (Satversmes aizsardzības birojs) – ir valsts drošības iestāde, kas atbild par valsts noslēpuma aizsardzību, valsts informācijas sistēmu drošību un informācijas tehnoloģiju kritiskās infrastruktūras uzraudzību.
1.30. **Tehniskais resurss** – aparatūra (hardware), tostarp tīkla darbību nodrošinošās iekārtas, darbstacijas, serveri, datu nesēji un citas saistītas iekārtas.
1.31. **Tehnoloģisko resursu turētājs** - persona, kas atbild par IKT infrastruktūras elementu (serveru, iekārtu u.c.) uzturēšanu, pieejamību un drošību.

2. Vispārīgie noteikumi

2.1. LSM Kiberdrošības politika (turpmāk – Politika) nosaka kiberdrošības pārvaldības struktūru, lomas un atbildības sadalījumu, principus un pamatprasības, kas jāievēro, lai nodrošinātu drošu un nepārtrauktu VSIA "Latvijas Sabiedriskais medijs" (turpmāk – LSM) informācijas un komunikācijas tehnoloģiju (turpmāk – IKT) sistēmu un informācijas resursu pārvaldību atbilstoši Latvijas Republikas normatīvajiem aktiem un starptautiskajai labajai praksei.
2.2. Politikas mērķis ir mazināt kiberincidentu iespējamību, nodrošinot LSM IKT resursu drošību, konfidencialitāti, integritāti, pieejamību un autentiskumu, kā arī veicināt darbinieku izpratni par kiberdrošību un atbildīgu IKT resursu lietošanu.
2.3. Kiberdrošības mērķi ietver četrus informācijas drošības pamatprincipus:
2.3.1. konfidencialitāte – nodrošināt, ka informācija ir pieejama tikai autorizētiem lietotājiem;

2.3.2. integritāte – nodrošināt informācijas precizitāti, pilnīgumu un aizsardzību pret neatļautām izmaiņām;
2.3.3. pieejamība – nodrošināt autorizētu lietotāju piekļuvi informācijai un IKT resursiem atbilstoši noteiktajām prasībām;
2.3.4. autentiskums – nodrošināt, ka informācijas avots un saņēmējs ir autentificēti, pārbaudāmi un uzticami.

3. Kiberdrošības politikas uzdevumi un piemērojamība

3.1. Politika nosaka kiberdrošības pārvaldības vispārējos principus, atbildības jomas un prasības LSM struktūrvienībām un darbiniekiem, kā arī paredz informēšanas un apmācību pasākumus kiberdrošības kultūras veidošanai.
3.2. Politikas uzdevumi:
3.2.1. lai sasniegtu Politikas mērķus un nodrošinātu LSM IKT sistēmu un informācijas resursu aizsardzību atbilstoši normatīvajiem aktiem un starptautiskajai praksei, šī politika nosaka šādus uzdevumus:
3.2.1.1. noteikt kiberdrošības pārvaldības struktūru un atbildības sadalījumu LSM,
3.2.1.2. nodrošināt atbilstību normatīvajiem aktiem un starptautiskajiem standartiem,
3.2.1.3. samazināt kiberincidentu risku, ieviešot drošības pasākumus,
3.2.1.4. ievērot informācijas drošības pamatprincipus - konfidencialitāti, integritāti, pieejamību un autentiskumu,
3.2.1.5. veicināt darbinieku izpratni un kiberhigiēnu,
3.2.1.6. noteikt struktūrvienību un lietotāju pienākumus kiberdrošībā,
3.2.1.7. pārvaldīt kiberriskus, nodrošinot to identificēšanu, novērtēšanu un mazināšanu.
3.3. Dokumenta tvērums un piemērojamība:
3.3.1. šī Politika ir saistoša visiem LSM darbiniekiem, līgumdarbiniekiem, praktikantiem, ārpakalpojumu sniedzējiem, sadarbības partneriem un citām personām, kurām piešķirtas tiesības piekļūt LSM informācijas sistēmām vai IKT resursiem;
3.3.2. Politikas prasības ir attiecināmas uz visu LSM rīcībā esošo informāciju, neatkarīgi no tās apstrādes, glabāšanas vai pārsūtīšanas veida un izmantotajiem tehnoloģiskajiem resursiem;
3.3.3. Politikas izpilde ir obligāta visās LSM struktūrvienībās un visos informācijas tehnoloģiju procesos, kas saistīti ar IKT resursu izmantošanu, attīstību un uzturēšanu.
3.4. Politika ir izstrādāta, ievērojot Latvijas Republikas un Eiropas Savienības normatīvos aktus, kā arī starptautiskos standartus kiberdrošības jomā, īpaši:
3.4.1. Nacionālo kiberdrošības likumu (turpmāk - NKDL);
3.4.2. Ministru kabineta noteikumus, kas izdoti uz NKDL pamata;
3.4.3. citiem normatīviem aktiem un standartiem, tostarp Eiropas Savienības normatīvajiem aktiem un starptautiskajiem standartiem, kas attiecas uz sabiedrisko elektronisko plašsaziņas līdzekļu darbību;
3.4.4. GDPR;
3.4.5. Starptautisko informācijas drošības pārvaldības standartu ISO/IEC 27001 un saistītos standartus.
3.5. Politikas aktualizācijas un pārskatīšanas kārtība:
3.5.1. Politiku regulāri pārskata un aktualizē vismaz reizi gadā vai biežāk, ja tiek konstatētas būtiskas izmaiņas normatīvajos aktos, LSM darbības specifikā, izmantotajās tehnoloģijās vai pēc nozīmīgu kiberincidentu iestāšanās;

3.5.2. par Politikas aktualizēšanu ir atbildīgs LSM kiberdrošības pārvaldnieks sadarbībā ar attiecīgajām struktūrvienībām, ievērojot izmaiņu apstiprināšanas kārtību, kuru nosaka LSM valde;
3.5.3. aktuālā Politikas versija tiek publicēta LSM iekšējā tīklā, un ar tās saturu tiek iepazīstināti visi LSM darbinieki, kuriem jāapliecina sava iepazīšanās ar Politikas saturu.

4. LSM vispārīgs raksturojums, darbības jomas un sniegtie pakalpojumi

4.1. LSM ir Latvijas sabiedriskais elektroniskais plašsaziņas līdzeklis, kas dibināts, apvienojot VSIA „Latvijas Televīzija" un VSIA „Latvijas Radio", ar mērķi nodrošināt mūsdienīgu, daudzplatformu mediju saturu un veicināt sabiedrības informētību, izglītošanu un izklaidi, stiprinot demokrātiskās vērtības, vārda brīvību un kultūras mantojuma saglabāšanu.
4.2. LSM galvenās darbības jomas ir:
4.2.1. televīzijas apraide – informācijas, analītisko raidījumu, kultūras, izklaides un sporta raidījumu veidošana un pārraidīšana;
4.2.2. radio apraide – sabiedriskā radio programmu veidošana un raidīšana, iekļaujot ziņas, diskusiju raidījumus, kultūras, izglītības un muzikālu saturu;
4.2.3. digitālie pakalpojumi – LSM.lv portāla un citu digitālo platformu pārvaldība, nodrošinot piekļuvi informācijai, multimediju saturam un digitālajiem pakalpojumiem jebkurā laikā un vietā.
4.3. LSM klasificējas kā kritiskās infrastruktūras un būtisko pakalpojumu sniedzējs atbilstoši NKDL prasībām, kas uzliek pienākumu ievērot īpašas kiberdrošības pārvaldības prasības un ziņošanas pienākumus par nozīmīgiem kiberincidentiem kompetentajām institūcijām.

5. Kiberdrošības pārvaldības struktūra

5.1. LSM kiberdrošības pārvaldības struktūra ir izveidota tā, lai skaidri noteiktu atbildības jomas, nodrošinātu efektīvu komunikāciju starp dažādām organizācijas struktūrvienībām un veicinātu sadarbību ar ārējām institūcijām kiberdrošības jautājumos.
5.2. Kiberdrošības pārvaldības struktūru veido šādas galvenās atbildīgās puses:
5.2.1. LSM valde;
5.2.2. Kiberdrošības pārvaldnieks;
5.2.3. Informācijas resursu un tehnoloģisko resursu turētāji;
5.2.4. struktūrvienību vadītāji;
5.2.5. LSM darbinieki un informācijas sistēmu lietotāji;
5.2.6. IT nodaļa un tehniskā atbalsta personāls.
5.3. LSM valdes loma un atbildība kiberdrošības pārvaldībā:
5.3.1. LSM valde ir atbildīga par kiberdrošības politikas apstiprināšanu un tās efektīvu īstenošanu visās LSM struktūrvienībās un darbības procesos;
5.3.2. valde nodrošina pietiekamu resursu piešķiršanu kiberdrošības funkciju realizēšanai, t.sk. nepieciešamo finanšu, cilvēkresursu un tehnoloģisko resursu nodrošināšanu;
5.3.3. valde regulāri pārskata kiberdrošības stāvokli organizācijā, analizē kiberdrošības pārvaldnieka sagatavotos ziņojumus par incidentiem, risku novērtējumiem un citiem būtiskiem jautājumiem, kā arī pieņem lēmumus par kiberdrošības pasākumu uzlabošanu.
5.4. Kiberdrošības pārvaldnieku ieceļ LSM valde, un tas ir atbildīgs par kiberdrošības pārvaldības procesa vadību un koordināciju.
5.5. Kiberdrošības pārvaldnieka galvenie pienākumi ietver:
5.5.1. nodrošināt LSM kiberdrošības politikas īstenošanu un aktualizēšanu atbilstoši normatīvo aktu prasībām;
5.5.2. izstrādāt, uzturēt un regulāri pārskatīt LSM kiberdrošības iekšējo dokumentāciju;

5.5.3. organizēt un koordinēt regulārus kiberdrošības risku novērtējumus un auditus;
5.5.4. vadīt un koordinēt kiberincidentu pārvaldību, tai skaitā incidentu identificēšanu, izmeklēšanu un seku novēršanu;
5.5.5. sagatavot regulārus ziņojumus LSM valdei par kiberdrošības situāciju, incidentiem un riskiem;
5.5.6. organizēt un koordinēt LSM darbinieku kiberdrošības apmācības un informēšanas pasākumus;
5.5.7. sadarboties ar ārējām kiberdrošības institūcijām (CERT.LV, Nacionālais kiberdrošības centrs).

5.6. Informācijas sistēmu resursu turētājs ir atbildīgs par:
5.6.1. Informācijas resursu klasifikāciju pēc konfidencialitātes, integritātes un pieejamības principiem;
5.6.2. Lietotāju piekļuves tiesību pieprasīšanas, piešķiršanas un regulāras pārskatīšanas organizēšanu;
5.6.3. sadarbību ar kiberdrošības pārvaldnieku kiberrisku novērtēšanā attiecībā uz informācijas saturu un tā apstrādes drošību;
5.6.4. regulāru sadarbību ar IT nodaļu un kiberdrošības pārvaldnieku attiecībā uz datu aizsardzības, glabāšanas un pieejamības jautājumiem.

5.7. Tehnoloģisko resursu turētājs ir atbildīgs par:
5.7.1. Tehnisko resursu konfigurāciju, atjauninājumu uzstādīšanu un darbspējas nodrošināšanu;
5.7.2. rezerves kopiju veidošanu, glabāšanu un datu atjaunošanas procesu organizēšanu;
5.7.3. drošības prasību ieviešanu un uzraudzību saistībā ar infrastruktūru, tīklu iekārtām, serveriem un lietojum vidēm;
5.7.4. sadarbību ar kiberdrošības pārvaldnieku tehnisko risku izvērtēšanā un drošības incidentu seku novēršanā.

5.8. LSM struktūrvienību vadītāji ir atbildīgi par to, ka viņu vadītajās struktūrvienībās tiek ievēroti kiberdrošības politikas principi un prasības.

5.9. Struktūrvienību vadītāju pienākumi kiberdrošībā:
5.9.1. nodrošināt, ka padotībā esošie darbinieki ir informēti par kiberdrošības prasībām un ievēro tās;
5.9.2. regulāri pārskatīt darbinieku piešķirtās piekļuves tiesības un ziņot IT nodaļai vai atbildīgo resursu turētājam par nepieciešamajām izmaiņām;
5.9.3. nekavējoties ziņot kiberdrošības pārvaldniekam par iespējamiem vai notikušiem kiberincidentiem, pārkāpumiem un drošības riskiem;
5.9.4. nodrošināt struktūrvienības darbinieku regulāru dalību kiberdrošības apmācībās un informēšanas pasākumos.

5.10. Katrs LSM darbinieks, līgumdarbinieks, praktikants vai sadarbības partneris, kam ir pieeja LSM informācijas sistēmām un resursiem, ir atbildīgs par drošas uzvedības normu ievērošanu.

5.11. Darbinieku galvenie pienākumi:
5.11.1. iepazīties ar kiberdrošības politiku un saistītajiem normatīvajiem dokumentiem un ievērot tos;
5.11.2. iIzmantot LSM informācijas sistēmas un resursus tikai darba pienākumu izpildei, ievērojot piešķirtās piekļuves tiesības un drošības prasības;
5.11.3. nekavējoties informēt kiberdrošības pārvaldnieku vai IT nodaļu par aizdomīgiem e-pastiem, incidentiem, neatļautām darbībām vai jebkuru citu drošības incidenta pazīmi;
5.11.4. regulāri piedalīties LSM organizētajās kiberdrošības apmācībās.

5.12. LSM regulāri sadarbojas ar ārējām kiberdrošības institūcijām, tostarp CERT.LV, SAB un Nacionālo kiberdrošības centru, lai saņemtu un sniegtu informāciju par iespējamiem

draudiem un incidentiem, kā arī dalītos pieredzē un iegūtu nepieciešamo atbalstu kiberdrošības incidentu pārvaldībā.

5.13. Kiberdrošības pārvaldnieks nodrošina operatīvu informācijas apmaiņu un incidentu ziņošanu CERT.LV un SAB atbilstoši spēkā esošajiem normatīvajiem aktiem un procedūrām.

5.14. Nepieciešamības gadījumā LSM var iesaistīt ārējos kiberdrošības ekspertus vai konsultantus, lai veiktu neatkarīgu auditu vai sniegtu atbalstu īpaši sarežģītu incidentu novēršanā un izmeklēšanā.

6. Nozīmīgākie kiberapdraudējumu veidi

6.1. Lai nodrošinātu efektīvu kiberdrošības pārvaldību un savlaicīgi novērstu kiberincidentu riskus, LSM regulāri identificē un novērtē nozīmīgākos kiberapdraudējumu veidus, kam var būt pakļauti LSM īpašumā un valdījumā esošie IKT resursi un informācijas sistēmas.

6.2. LSM kiberdrošības pārvaldnieks sadarbībā ar IT nodaļu un struktūrvienību vadītājiem regulāri aktualizē šo apdraudējumu sarakstu, izvērtējot incidentu statistiku, tehnoloģiju attīstību un ārējo institūciju sniegto informāciju par aktuāliem draudiem:

- 6.2.1. sociālās inženierijas uzbrukumi (Social Engineering);
- 6.2.2. pikšķerēšanas uzbrukumi (Phishing);
- 6.2.3. izspiedējvīrusi (Ransomware);
- 6.2.4. ļaunprogrammatūra (Malware);
- 6.2.5. pakalpojumu atteices uzbrukumi (DDoS – Distributed Denial of Service);
- 6.2.6. iekšējie draudi un neatļauta piekļuve;
- 6.2.7. sabotāža un mērķtiecīgi uzbrukumi;
- 6.2.8. citu apdraudējumu veidu izvērtējums.

6.3. Kiberdrošības pārvaldnieks nodrošina informācijas apriti un reaģēšanu uz potenciālajiem un aktuālajiem kiberapdraudējumiem, informējot darbiniekus par nepieciešamajiem drošības pasākumiem.

7. Informācijas sistēmu (IS) un IKT resursu pārvaldība

7.1. LSM uztur vienotu, aktualizētu un detalizētu katalogu, kurā tiek reģistrēti visi IS un informācijas un IKT resursi. Katalogs ietver resursu nosaukumus, atbildīgās personas (resursu turētājus), informācijas klasifikācijas līmeni, atrašanās vietu, kā arī citas būtiskas tehniskās un organizatoriskās īpašības.

7.2. Katalogu uztur IT nodaļa sadarbībā ar IS un IKT resursu turētājiem un kiberdrošības pārvaldnieku, aktualizējot informāciju vismaz reizi gadā vai pēc būtiskām izmaiņām.

7.3. LSM visi informācijas resursi tiek klasificēti pēc konfidencialitātes, integritātes un pieejamības līmeņiem, ievērojot risku novērtējumu un normatīvo aktu prasības.

7.4. Klasifikācija tiek veikta vismaz reizi gadā, un atbildība par klasifikāciju ir IS resursu turētājiem sadarbībā ar kiberdrošības pārvaldnieku.

7.5. Klasifikācijas rezultāti tiek izmantoti, lai noteiktu piemērotus drošības pasākumus un prioritātes incidentu pārvaldībā un resursu aizsardzībā.

7.6. Pieejas tiesības LSM informācijas resursiem un IS tiek piešķirtas pēc principa „tikai nepieciešamā piekļuve" – lietotājiem tiek piešķirtas tikai tās tiesības, kas ir nepieciešamas tiešo darba pienākumu izpildei.

7.7. Pieejas tiesību pieprasījumu, piešķiršanu, grozīšanu un anulēšanu administrē IT nodaļa pēc struktūrvienību vadītāju pieprasījuma.

7.8. Reizi gadā kiberdrošības pārvaldnieks sadarbībā ar IS resursu turētājiem veic lietotāju piekļuves tiesību pārskatīšanu un nepieciešamās korekcijas.

7.9. LSM izmanto daudzfaktoru autentifikāciju (MFA) vismaz kritisko IS un attālinātai piekļuvei LSM iekšējiem tīkliem, nodrošinot papildu drošības līmeni.

7.10. Autentifikācijas mehānismi ietver kombināciju no zināšanām (paroles), īpašumā esošām ierīcēm (mobilie autentifikatori, kodu kalkulatori u.c), ja tehniski iespējams un nepieciešams.
7.11. Autentifikācijas prasības regulāri pārskata kiberdrošības pārvaldnieks un IT nodaļa atbilstoši aktuālajiem kiberdrošības riskiem un tehnoloģiskajām iespējām.
7.12. LSM nodrošina atbilstošus fiziskās drošības pasākumus serveru telpām un kritiskajiem IKT resursiem, piemēram, piekļuves kontroli, videonovērošanu, klimata kontroli, nepārtrauktu elektroenerģijas padevi (UPS) un ugunsdrošības pasākumus.
7.13. Loģiskā drošība tiek nodrošināta ar efektīvu ugunsmūra risinājumu, regulārām drošības pārbaudēm, regulāriem programmatūras un sistēmu atjauninājumiem, kā arī sistēmu auditācijas pierakstu veidošanu un uzraudzību.
7.14. LSM nodrošina regulāru visu būtisko datu un informācijas sistēmu rezerves kopiju veidošanu, atbilstoši definētiem intervāliem un kritiskuma līmeņiem, lai nodrošinātu iespēju atjaunot datus un IS darbību incidentu vai datu zuduma gadījumā.
7.15. Rezerves kopijas tiek uzglabātas drošā un ģeogrāfiski atdalītā vietā, kā arī pārbaudītas regulārās datu atjaunošanas testēšanas procedūrās.
7.16. LSM izmanto tikai licencētu programmatūru, ievērojot licenču lietošanas noteikumus un nodrošinot nepieciešamo atbilstību autortiesībām un normatīvajiem aktiem.
7.17. IT nodaļa uztur centralizētu programmatūras uzskaiti un veic regulāru programmatūras atjauninājumu instalēšanu un drošības ielāpu uzstādīšanu, nodrošinot programmatūras drošības prasību ievērošanu.
7.18. Kiberdrošības pārvaldnieks sadarbībā ar IT nodaļu regulāri izvērtē programmatūras ievainojamības un veic nepieciešamos pasākumus, lai novērstu drošības riskus, kas saistīti ar novecojušu vai ievainojamu programmatūru.

8. Kiberdrošības risku pārvaldība

8.1. LSM kiberdrošības risku pārvaldība tiek īstenota, ievērojot starptautiski atzītu kiberrisku vadības metodoloģiju, kas balstīta uz ISO/IEC 27005 standartā aprakstītajiem principiem.
8.2. Kiberrisku pārvaldības procesā tiek identificēti, analizēti, novērtēti un uzraudzīti kiberdrošības riski, izvērtējot draudu avotus, sistēmu ievainojamības, iespējamo ietekmi un incidentu varbūtību.
8.3. Metodoloģiju apstiprina LSM valde, un tās ievērošanu koordinē kiberdrošības pārvaldnieks sadarbībā ar IT nodaļu, IS resursu turētājiem un LSM risku pārvaldības speciālistu.
8.4. Kiberrisku novērtēšana tiek veikta vismaz reizi gadā vai pēc būtiskām izmaiņām IS vai IKT resursu konfigurācijā, kā arī pēc nozīmīgu incidentu iestāšanās.
8.5. Novērtēšanas procesā tiek identificēti esošie un jaunie riski, noteikta to ietekme uz LSM darbību un resursiem, kā arī analizēta risku iespējamība un potenciālās sekas.
8.6. Kiberrisku uzraudzību veic kiberdrošības pārvaldnieks sadarbībā ar IS un IKT resursu turētājiem, regulāri atjauninot risku novērtējumu un nepieciešamos aizsardzības pasākumus, par ko tiek informēta LSM valde.
8.7. Pamatojoties uz kiberrisku novērtēšanas rezultātiem, tiek plānoti un ieviesti konkrēti kiberrisku mazināšanas pasākumi, kuru mērķis ir samazināt risku iestāšanās varbūtību vai negatīvās sekas.
8.8. Kiberdrošības pārvaldnieks nodrošina kiberrisku mazināšanas plāna izpildes kontroli un regulāri ziņo par plāna izpildes gaitu LSM valdei.
8.9. LSM uztur centralizētu kiberrisku reģistru, kurā tiek uzskaitīti visi identificētie kiberriski, to novērtējums, potenciālā ietekme, mazināšanas pasākumi, kā arī pasākumu izpildes statuss.
8.10. Kiberrisku reģistrs tiek aktualizēts vismaz reizi gadā vai pēc būtiskām izmaiņām LSM IS un IKT infrastruktūrā, kā arī pēc kiberincidentiem, kas var ietekmēt risku līmeni.

8.11. Kiberdrošības pārvaldnieks regulāri pārskata reģistru kopā ar IT nodaļu un IS resursu turētājiem, un nepieciešamības gadījumā veic izmaiņas, par ko tiek informējot LSM valdi.

9. IKT darbības nepārtrauktības nodrošināšana

9.1. LSM īsteno sistemātisku pieeju IKT darbības nepārtrauktības plānošanā, lai nodrošinātu kritisko pakalpojumu un funkciju atjaunošanu pēc iespējamiem incidentiem vai ārkārtas situācijām.
9.2. Nepārtrauktības plānošana tiek balstīta uz risku novērtējumu un IS resursu klasifikācijas rezultātiem, definējot pieļaujamos atjaunošanas laika mērķus (Recovery Time Objective - RTO) un pieļaujamo datu zaudējuma apjomu (Recovery Point Objective - RPO) katram kritiskajam resursam vai pakalpojumam.
9.3. Nepārtrauktības plānu izstrādā un regulāri aktualizē kiberdrošības pārvaldnieks sadarbībā ar šādām atbildīgajām pusēm:
  9.3.1. IT nodaļu;
  9.3.2. IS un IKT resursu turētājiem;
  9.3.3. struktūrvienību vadītājiem un to apstiprina LSM valde;
  9.3.4. LSM Tehnoloģisko procesu nodrošinājuma un attīstības vadītājs;
  9.3.5. Stratēģisko projektu vadītājs;
  9.3.6. Risku vadības speciālists.
9.4. Darbības nepārtrauktības plānu apstiprina LSM valde.
9.5. Nepārtrauktības plānā ietvertie pasākumi tiek savlaicīgi ieviesti, nosakot konkrētas atbildības, uzdevumus, termiņus un nepieciešamos resursus šo pasākumu īstenošanai.
9.6. Kiberdrošības pārvaldnieks regulāri (vismaz reizi gadā vai pēc būtiskām izmaiņām) pārskata un aktualizē nepārtrauktības plānu, nodrošinot tā atbilstību aktuālajiem draudiem, tehnoloģijām, kā arī izmaiņām LSM darbības procesos un infrastruktūrā.
9.7. LSM nodrošina rezerves tehnoloģiskos resursus un alternatīvus pieslēgumus (tīkla savienojumi, rezerves serveri, datu glabāšanas vietas), kas nepieciešami kritisko IS un pakalpojumu nepārtrauktas darbības nodrošināšanai incidentu vai ārkārtas situāciju gadījumā.
9.8. Rezerves resursu un pieslēgumu konfigurācija tiek regulāri pārbaudīta un testēta, lai pārliecinātos par to efektivitāti un gatavību nodrošināt nepārtrauktu IS darbību ārkārtas situācijās.
9.9. Nepārtrauktības plāna testēšana tiek veikta regulāri (vismaz reizi gadā), pārbaudot plānā ietverto pasākumu efektivitāti, spēju atjaunot sistēmu darbību un datu pieejamību plānotajos atjaunošanas laikos.
9.10. Testēšanas rezultāti tiek dokumentēti, analizēti, un nepieciešamie pilnveidošanas pasākumi tiek iekļauti atjauninātajā nepārtrauktības plānā, par ko tiek informēta LSM valde.
9.11. Kiberdrošības pārvaldnieks sadarbībā ar 9.3. punktā minētajām personām nodrošina nepārtrauktības plāna regulāru aktualizēšanu un pārskatīšanu, kā arī informē LSM darbiniekus un atbildīgās personas par nepārtrauktības pasākumiem un rīcību incidentu gadījumos.

10. Kiberhigiēnas un darbinieku izglītošanas pasākumi

10.1. Katram LSM jaunajam darbiniekam, līgumdarbiniekam vai praktikantam, kam tiek piešķirtas piekļuves tiesības LSM informācijas sistēmām un resursiem, tiek nodrošināta sākotnējā kiberdrošības instruktāža.
10.2. Sākotnējā instruktāža ietver iepazīstināšanu ar LSM Kiberdrošības politiku, IKT resursu lietošanas noteikumiem, pamata drošības prasībām un rīcību incidentu gadījumā.

10.3. Instruktāžu organizē un dokumentē kiberdrošības pārvaldnieks sadarbībā ar personāla daļu, nodrošinot instruktāžas veikšanu ne vēlāk kā viena mēneša laikā no darbinieka darba uzsākšanas brīža.
10.4. LSM nodrošina regulāras kiberdrošības apmācības visiem darbiniekiem, kuriem ir pieeja IS un IKT resursiem, lai veicinātu darbinieku izpratni par aktuālajiem kiberdrošības riskiem un labu praksi drošā darba veikšanai.
10.5. Kiberdrošības apmācības tiek organizētas vismaz reizi gadā vai biežāk, atkarībā no aktuālajiem riskiem, incidentiem vai izmaiņām normatīvajos aktos un tehnoloģiju vidē.
10.6. Apmācību saturu nodrošina kiberdrošības pārvaldnieks sadarbībā, iekļaujot praktiskus piemērus un reālas situācijas analīzes.
10.7. LSM regulāri īsteno informatīvas aktivitātes un kampaņas, lai stiprinātu darbinieku izpratni par kiberdrošību, veicinātu kiberdrošības kultūras attīstību un darbinieku aktīvu līdzdalību kiberrisku novēršanā.
10.8. Kiberdrošības kultūras veicināšanas pasākumos tiek izmantotas dažādas komunikācijas formas, piemēram, informatīvi ziņojumi iekšējā tīmekļa vietnē, e-pasta kampaņas, plakāti, interaktīvi semināri u.c.

11. Noslēguma jautājumi

11.1. Politika stājas spēkā pēc apstiprināšanas Sabiedrisko elektronisko plašsaziņas līdzekļu padomē.
11.2. Ja mainās procesu nosaukumi, LSM struktūrvienību nosaukumi, atbildīgie darbinieki, viņu amati, darba vietas adreses, telefonu numuri u.tml, ir mainījušies LSM iekšējie normatīvie akti, kā arī atsauces un saites uz citiem saistītajiem dokumentiem, tad tie netiek uzskatīti par dokumenta grozījumiem. Šādas izmaiņas dokumenta elektroniskajā versijā veic kiberdrošības pārvaldnieks, elektroniski apstiprina LSM valdes priekšsēdētājs un LSM valdes loceklis tehnoloģiju pārvaldības jautājumos.
11.3. Ja tiek izdarītas būtiskas izmaiņas dokumenta saturā un tajā aprakstītajās darbībās, grozījumus apstiprina LSM Sabiedrisko elektronisko plašsaziņas līdzekļu padome.