Informācijas drošības politika

SIA Paraugs

31.10.2026. · v1.0

Informācijas drošības politika

Dokumenta vadība

Lauks	Vērtība
Dokumenta īpašnieks	Valdes norīkota persona / IT pakalpojumu sniedzējs
Versija	v1.0
Sagatavots	31.10.2026
Valde apstiprinājusi	____
Nākamā pārskatīšana	31.10.2027
Klase	Konfidenciāls
Izplatīšana	Valde un par informācijas drošību atbildīgā persona

Versiju vēsture

Versija	Datums	Izmaiņas	Sagatavoja	Apstiprināja
v1.0	31.10.2026	Pirmā versija	____	____
____	____	____	____	____
____	____	____	____	____

Satura rādītājs

• 1. Mērķis un darbības joma
• 2. Atbildība
• 3. Riska pārvaldība
• 4. Piekļuve un paroles
• 5. Iekārtas un attālinātais darbs
• 6. Fiziskā drošība
• 7. Informācijas sistēmu droša lietošana
• 8. Kriptogrāfija un šifrēšana

• 9. Ievainojamības, atjauninājumi un žurnalēšana
• 10. Informācijas aktīvi un rezerves kopijas
• 11. Darbības nepārtrauktība un krīzes vadība
• 12. Piegādātāji un piegādes ķēde
• 13. Personāla drošība un apmācības
• 14. Incidenti
• 15. Personas datu aizsardzība
• 16. Informācijas klasifikācija
• 17. Efektivitātes novērtēšana un pārskatīšana
• 18. Atbilstības tabula
• 19. Noslēguma jautājumi

1. Mērķis un darbības joma

1.1. Šī politika nosaka kārtību, kādā SIA Paraugs aizsargā informācijas aktīvus, informācijas sistēmas un pakalpojumus. SIA Paraugs piemēro šo politiku visām darbībām, kurās tā apstrādā informāciju. Politiku nepiemēro informācijai, kas nav saistīta ar sabiedrības darbību.

1.2. Politika ir saistoša valdei, darbiniekiem un katrai personai, kurai SIA Paraugs ir piešķīrusi piekļuvi saviem informācijas aktīviem. Persona ievēro šo politiku no piekļuves piešķiršanas brīža līdz tās atcelšanai. Piekļuves izmantošana pretēji šai politikai nav pieļaujama.

1.3. SIA Paraugs reģistrācijas numurs ir 40000000000. Juridiskā adrese ir Rīga, Paraugu iela 1, LV-1001. Sabiedrība darbojas šādā valstī: Latvija. Šos datus norāda, lai noteiktu, kurai personai politika ir saistoša.

1.4. SIA Paraugs nodarbina 10–49 darbinieki. Sabiedrības nozare ir grāmatvedība un audits. Darbinieku skaitu un nozari ņem vērā, nosakot piekļuves tiesību apjomu un rezerves kopiju kārtību.

1.5. SIA Paraugs veic šādu darbību: Sniedz grāmatvedības un algu aprēķina pakalpojumus mazajiem uzņēmumiem un glabā klientu finanšu un darbinieku datus. Politiku piemēro šai darbībai un informācijai, kas rodas tās izpildē. Darbību, kas politikā nav aprakstīta, neuzskata par atļautu, kamēr valde to nav iekļāvusi politikā.

1.6. SIA Paraugs papildu precizējumus nav sniegusi. Politiku piemēro tikai darbības aprakstam. Faktus, kas aprakstā nav minēti, valde politikā nepievieno.

1.7. Politikas mērķa standarts ir ES NIS2 direktīva un Latvijas Nacionālais kiberdrošības likums. Šī politika ir konfidenciāla un paredzēta valdei. Personas datu aizsardzībai papildus piemēro Vispārīgo datu aizsardzības regulu (VDAR).

1.8. Informācijas aktīvs šajā politikā ir informācija un informācijas sistēma, kuru SIA Paraugs izmanto savā darbībā. Informācijas aktīvu aizsargā neatkarīgi no tā, vai tas ir elektronisks vai papīra formā. Informācijas aktīvu, kas nav iekļauts uzskaitē, aizsargā tāpat kā uzskaitītu aktīvu.

1.9. Kiberincidents šajā politikā ir notikums, kas apdraud informācijas aktīva pieejamību, integritāti vai konfidencialitāti. Par kiberincidentu uzskata arī pamatotu aizdomu, ka šāds apdraudējums ir iestājies. Kiberincidentu slēpt vai atlikt tā paziņošanu nav pieļaujams.

1.10. Daudzfaktoru autentifikācija šajā politikā ir piekļuves pārbaude ar paroli un vēl vienu no valdes noteiktajiem līdzekļiem. Šajā sabiedrībā otrais līdzeklis ir autentifikācijas lietotne. Piekļuve bez daudzfaktoru autentifikācijas nav pieļaujama.

1.11. Piekļuves tiesības šajā politikā ir atļauja izmantot noteiktu informācijas aktīvu noteiktā apjomā. Piekļuves tiesības piešķir amatam, nevis personai vispār. Tiesības, kas pārsniedz amata pienākumu, piešķirt nav pieļaujams.

1.12. Rezerves kopija šajā politikā ir informācijas aktīva kopija, no kuras aktīvu var atjaunot. Rezerves kopiju glabā atdalīti no pamata aktīva. Rezerves kopijas dzēšana bez valdes rakstveida atļaujas nav pieļaujama.

2. Atbildība

2.1. Valde apstiprina šo politiku un nodrošina tās izpildei nepieciešamos resursus. Valde politikas izpildi pārbauda ne retāk kā reizi gadā. Politiku atstāt bez apstiprinājuma nav pieļaujams.

2.2. Valde nosaka personu, kura ikdienā uzrauga informācijas drošības prasību izpildi. Šī persona ziņo valdei par kiberincidentiem un par neizpildītām prasībām. Uzraudzību nodot personai, kurai nav šim nolūkam piešķirtu pilnvaru, nav pieļaujams.

2.3. Tiešais vadītājs nodrošina, ka viņam padotie darbinieki zina šīs politikas prasības, kas attiecas uz viņu amatu. Vadītājs pārbauda, vai piekļuves tiesības atbilst amatam. Vadītājs nedrīkst dot norādījumu, kas ir pretrunā ar šo politiku.

2.4. Katrs darbinieks aizsargā sabiedrības informācijas aktīvus un par kiberincidentu vai aizdomīgu notikumu ziņo tiešajam vadītājam šajā politikā noteiktajā termiņā. Darbinieks nepilda norādījumu, kas acīmredzami pārkāpj šo politiku, un par to ziņo valdei. Noklusēt zināmu pārkāpumu nav pieļaujams.

2.5. Piekļuves tiesības piešķir atbilstoši amatam. Tās atbilst darba pienākumam un netiek piešķirtas visiem pēc noklusējuma. Tiesības, kas vairs neatbilst amatam, valde atceļ, kad amats mainās vai darba tiesiskās attiecības izbeidzas.

2.6. Persona, kura pārkāpj šo politiku, atbild saskaņā ar darba līgumu un piemērojamiem tiesību aktiem. Valde pārkāpumu fiksē rakstveidā. Pārkāpuma noklusēšana neatbrīvo no atbildības.

2.7. Ikdienas informācijas drošības pasākumus organizē valdes norīkota persona kopā ar ārējo IT pakalpojumu sniedzēju, kas vismaz reizi ceturksnī ziņo valdei.

2.8. Ārējā IT pakalpojumu sniedzēja pienākumus nosaka līgums. Atbildība par šīs politikas izpildi paliek valdei.

2.9. Valde ieceļ kiberdrošības pārvaldnieku, kurš organizē šīs politikas izpildi, uztur saziņu ar CERT.LV un Nacionālo kiberdrošības centru (NKC) un ziņo valdei. Pienākumu var uzticēt ārpakalpojuma sniedzējam, bet atbildība paliek valdei.

2.10. Ja sabiedrība ir būtisks vai svarīgs subjekts, valde pārliecinās par tās reģistrāciju Nacionālajā kiberdrošības centrā (NKC) un norīko kontaktpersonu.

3. Riska pārvaldība

3.1. Valde informācijas drošības riskus novērtē vismaz reizi gadā, kā arī pēc būtiskām izmaiņām sabiedrības darbībā, infrastruktūrā vai piegādātājos un pēc būtiska kiberincidenta. Novērtējumu ieraksta riska reģistrā.

3.2. Novērtējums aptver šādus informācijas aktīvus un apstākļus: klientu un darbinieku personas dati, maksājumu karšu un finanšu dati; infrastruktūra: mākoņpakalpojumi, darbstacijas; mākoņdatošanas pakalpojumi: Microsoft 365, Amazon Web Services; darba modelis: hibrīddarbs.

3.3. Katram riskam nosaka varbūtību un ietekmi skalā no 1 līdz 3. Riska līmenis ir to reizinājums. Risku ar līmeni 6 vai augstāku samazina ar pasākumu, kuram rīcības plānā ir noteikts termiņš un atbildīgā persona.

3.4. Risku, kuru valde nolemj pieņemt, pieņem ar rakstveida lēmumu, kurā norāda pamatojumu un nākamās pārskatīšanas datumu.

3.5. Šai politikai pievienotā trūkumu analīze un rīcības plāns ir sākotnējais risku novērtējums. Valde rīcības plāna izpildi pārbauda vismaz reizi ceturksnī.

4. Piekļuve un paroles

4.1. Daudzfaktoru autentifikācija ir obligāta visām piekļuvēm sabiedrības informācijas sistēmām. Otrais līdzeklis ir autentifikācijas lietotne. Piekļuvi bez šī līdzekļa valde nepiešķir.

4.2. Parole atbilst šādām minimālajām prasībām: vismaz 12 simboli, iekļauti vārdi vai frāzes, lielie un mazie burti, simboli. Paroli, kas šīm prasībām neatbilst, sistēmā nepieņem. Darbinieks paroli izveido pats un to nevienam nenodod.

4.3. Paroli neizpauž un neizmanto privātajos kontos. Paroles nodošana citai personai, tostarp kolēģim, nav pieļaujama. Ja parole ir kļuvusi zināma citai personai, darbinieks to nekavējoties nomaina un ziņo tiešajam vadītājam.

4.4. Atbilstoši mērķa standartam (ES NIS2 direktīva un Latvijas Nacionālais kiberdrošības likums) valde piekļuves tiesības pārskata reizi ceturksnī. Pārskatā valde salīdzina piešķirtās tiesības ar amata pienākumu. Tiesības, kas vairs nav nepieciešamas, atceļ, kad persona maina lomu vai izbeidz darba tiesiskās attiecības.

4.5. Jaunu piekļuvi piešķir tikai pēc tiešā vadītāja rakstveida pieprasījuma un valdes vai tās norīkotas personas apstiprinājuma. Piekļuvi piešķir tādā apjomā, kāds nepieciešams pienākuma izpildei. Pagaidu piekļuvei nosaka beigu datumu, un pēc šā datuma piekļuvi atceļ.

4.6. Kopīgu kontu, kuru lieto vairākas personas ar vienu paroli, neizveido. Katrs darbinieks lieto savu kontu. Kopīga konta lietošana nav pieļaujama, izņemot gadījumu, kad valde to ir rakstveidā atļāvusi un noteikusi atbildīgo personu.

5. Iekārtas un attālinātais darbs

5.1. Darba modelis ir hibrīddarbs. Iekārtu kārtība ir šāda: tikai uzņēmuma iekārtas. Darbinieks lieto tikai tādu iekārtu un tādu darba veidu, kādu šī politika atļauj. Citu iekārtu pieslēgšana sabiedrības sistēmām nav pieļaujama.

5.2. Darba iekārtu bloķē, kad tā netiek lietota. Darbinieks iekārtu bloķē, pirms atstāj darbavietu, arī uz īsu brīdi. Atstāt atvērtu sesiju bez uzraudzības nav pieļaujams.

5.3. Attālinātā darbā lieto tikai apstiprinātus kontus un sabiedrības noteikto pieslēguma veidu. Darbinieks attālināto darbu veic vietā, kur ekrāns un dokumenti nav redzami nepiederošām personām. Publiska tīkla lietošana bez valdes noteiktā pieslēguma nav pieļaujama.

5.4. Elektroniskos dokumentus nesūta pa personīgiem saziņas līdzekļiem, kurus sabiedrība nav apstiprinājusi. Tas attiecas arī uz tūlītējo ziņojumapmaiņu un personīgo elektronisko pastu. Nosūtīšanu, kas jau notikusi, darbinieks nekavējoties paziņo tiešajam vadītājam.

5.5. Darba iekārtā uzstāda tikai programmatūru, kuru sabiedrība ir atļāvusi. Darbinieks drošības atjauninājumus neatliek. Neatļautas programmatūras uzstādīšana nav pieļaujama.

5.6. Zaudētu vai nozagtu iekārtu darbinieks nekavējoties, bet ne vēlāk kā vienas stundas laikā no konstatēšanas brīža, paziņo tiešajam vadītājam. Vadība piekļuvi no šīs iekārtas atceļ. Iekārtas meklēšanu darbinieks turpina tikai pēc vadības norādījuma.

6. Fiziskā drošība

6.1. Personas datus vai finanšu informāciju saturošus papīra dokumentus glabā aizslēgtā skapī ar ierobežotu piekļuvi, un atslēgu vai kodu tur tikai valdes norīkota persona.

6.2. Apmeklētāju neatstāj bez uzraudzības telpā, kurā ir redzami ekrāni vai dokumenti. Darbinieks, kurš apmeklētāju pieņem, viņu uzrauga visu vizītes laiku un piekļuvi informācijas sistēmai nepiešķir.

6.3. Darba dienas beigās darbinieks pirms telpas atstāšanas atbrīvo darbavietu no dokumentiem un iekārtu novieto aizslēgtā vietā.

6.4. Telpu vai skapi, kurā atrodas serveri, tur aizslēgtu, un atslēga ir tikai norīkotām personām. Citu personu šajā telpā ielaiž tikai norīkotas personas klātbūtnē, un apmeklējumu fiksē.

6.5. Izdrukas, kas satur datus, iznīcina tā, lai saturu nevarētu atjaunot, un neizmet sadzīves atkritumos.

6.6. Ja papīra dokuments ir nozaudēts, darbinieks par to ziņo tiešajam vadītājam nekavējoties, bet ne vēlāk kā vienas stundas laikā no konstatēšanas brīža. Vadība nosaka, vai dokuments satur personas datus vai citu aizsargājamu informāciju.

7. Informācijas sistēmu droša lietošana

7.1. Saiti vai pielikumu neatver, ja sūtītājs vai saturs ir neparasts. Darbinieks šādu ziņojumu pārsūta tiešajam vadītājam un gaida norādījumu.

7.2. Darba iekārtā uzstāda tikai apstiprinātu programmatūru. Drošības atjauninājumu, ko sistēma piedāvā, darbinieks uzstāda tajā pašā darba dienā.

7.3. Darbinieks, kurš iekārtu lieto, ekrānu bloķē ikreiz, kad atstāj darbavietu.

7.4. Darba paroli un autentifikācijas kodu nepieraksta un nenodod tūlītējā ziņojumapmaiņā vai elektroniskajā pastā. Ja kods ir nosūtīts, darbinieks par to nekavējoties ziņo tiešajam vadītājam un kodu nomaina.

7.5. Par aizdomīgu elektroniskā pasta ziņojumu ziņo vadībai tajā pašā darba dienā, tajā norādītās saites neatverot.

7.6. Sabiedrības kontu nepieslēdz ārējai lietotnei, kuru valde nav apstiprinājusi, un šādas lietotnes pieprasījumu pēc paroles vai piekļuves datiem darbinieks noraida.

7.7. Mākslīgā intelekta rīku kārtība ir šāda: atļauti tikai valdes apstiprināti mākslīgā intelekta rīki, un tajos ievada tikai publiski pieejamu informāciju. Pieprasījumu, kas pārsniedz šo kārtību, darbinieks noraida un par to ziņo tiešajam vadītājam.

8. Kriptogrāfija un šifrēšana

8.1. Portatīvo datoru, planšetu un telefonu, kuros glabā vai apstrādā sabiedrības informāciju, atmiņu aizsargā ar pilna diska šifrēšanu, ko ieslēdz pirms iekārtas nodošanas lietošanā.

8.2. Informāciju ārpus sabiedrības tīkla pārraida tikai pa šifrētu savienojumu, piemēram, TLS 1.2 vai jaunāku protokolu vai virtuālo privāto tīklu. Sabiedrības tīmekļa vietnes un pakalpojumi izmanto derīgu sertifikātu.

8.3. Konfidenciālu informāciju ārējai personai nosūta šifrētā datnē vai koplietošanas saitē ar ierobežotu piekļuvi. Paroli datnes atvēršanai nodod pa citu saziņas kanālu.

8.4. Rezerves kopijas, kuras glabā ārpus sabiedrības telpām vai mākoņdatošanas pakalpojumā, šifrē.

8.5. Šifrēšanas un atkopšanas atslēgas glabā atsevišķi no šifrētajiem datiem, un tās pārvalda valdes norīkota persona kopā ar ārējo IT pakalpojumu sniedzēju. Atslēgas nozaudēšanu vai izpaušanu uzskata par kiberincidentu.

8.6. Darbinieki darba paroles glabā valdes apstiprinātā paroļu pārvaldniekā. Sistēmas paroles glabā tikai sāļotu jaucējvērtību veidā.

9. Ievainojamības, atjauninājumi un žurnalēšana

9.1. Operētājsistēmām, pārlūkprogrammām, biroja un drošības programmatūrai ieslēdz automātisku drošības atjauninājumu uzstādīšanu. Kritisku ievainojamību novērš 14 dienu laikā, citas — 30 dienu laikā no atjauninājuma publicēšanas.

9.2. Programmatūru, kurai ražotājs vairs nesniedz drošības atjauninājumus, sabiedrības sistēmās nelieto. Ja to nevar aizstāt nekavējoties, valde nosaka aizstāšanas termiņu, un līdz tam sistēmu nošķir no interneta.

9.3. Visās darba iekārtās darbojas ļaunatūras aizsardzība ar automātiski atjauninātu datubāzi. Darbinieks to neizslēdz.

9.4. Sabiedrības tīklu aizsargā ugunsmūris, viesu bezvadu tīklu nošķir no darba tīkla, un administratīvās saskarnes no interneta nav pieejamas. Noklusētās paroles nomaina pirms iekārtas lietošanas, serveru un tīkla iekārtu konfigurāciju dokumentē, un sistēmu pulksteņus sinhronizē ar uzticamu laika avotu.

9.5. Valdes norīkota persona kopā ar ārējo IT pakalpojumu sniedzēju uztur pieteikšanās, administratora darbību un drošības notikumu žurnālus, glabā tos vismaz 12 mēnešus un aizsargā pret grozīšanu.

9.6. Mākoņdatošanas pakalpojumos (Microsoft 365, Amazon Web Services) ieslēdz audita žurnālu un brīdinājumus par aizdomīgu pieteikšanos, piemēram, no neparastas valsts vai pēc atkārtotiem neveiksmīgiem mēģinājumiem.

9.7. Valde vismaz reizi gadā nodrošina no interneta pieejamo sistēmu ievainojamību skenēšanu un konstatēto iekļauj rīcības plānā.

10. Informācijas aktīvi un rezerves kopijas

10.1. SIA Paraugs par informācijas aktīviem atzīst informāciju, kas nepieciešama šai darbībai: Sniedz grāmatvedības un algu aprēķina pakalpojumus mazajiem uzņēmumiem un glabā klientu finanšu un darbinieku datus. Valde šos aktīvus uzskaita un norāda, kurš par katru aktīvu atbild. Aktīvu, kas nav uzskaitīts, tas neatbrīvo no aizsardzības pienākuma.

10.2. Izmantotā infrastruktūra ir šāda: mākoņpakalpojumi, darbstacijas. Sabiedrība šajā infrastruktūrā glabā un apstrādā tikai tos informācijas aktīvus, kuri nepieciešami darbībai. Infrastruktūru, kas šajā punktā nav minēta, pieslēgt bez valdes atļaujas nav pieļaujams.

10.3. Ja sabiedrība izmanto mākoņdatošanas pakalpojumus, pakalpojuma līgumā saglabā piegādātāja pienākumu aizsargāt sabiedrības datus. Valde pirms līguma noslēgšanas pārliecinās, ka piegādātājs nodrošina piekļuves ierobežošanu un rezerves kopijas. Līgumu bez šāda pienākuma neslēdz.

10.4. Rezerves kopijas izgatavo reizi dienā. Par izgatavošanu atbild valdes norīkota persona. Kopijas termiņa nokavējumu valde fiksē rakstveidā.

10.5. Atbilstoši mērķa standartam (ES NIS2 direktīva un Latvijas Nacionālais kiberdrošības likums) valde atjaunošanu no kopijas pārbauda reizi ceturksnī. Pārbaudi fiksē rakstveidā un norāda, vai atjaunošana izdevās. Atjaunošanas pārbaudi aizstāt ar pieņēmumu, ka kopija ir derīga, nav pieļaujams.

10.6. Rezerves kopiju glabā tā, lai tā nebūtu iznīcināma ar to pašu notikumu, kas iznīcina pamata aktīvu. Piekļuve rezerves kopijai ir tikai valdes norīkotām personām. Kopijas nodošana piegādātājam bez līgumā noteikta aizsardzības pienākuma nav pieļaujama.

11. Darbības nepārtrauktība un krīzes vadība

11.1. Valde nosaka sabiedrības kritiskos procesus un sistēmas un katrai nosaka pieļaujamo dīkstāves laiku (RTO) un pieļaujamo datu zudumu (RPO). RPO nepārsniedz rezerves kopiju intervālu, kas ir reizi dienā.

11.2. Rīcību traucējuma gadījumā nosaka šai politikai pievienotais darbības nepārtrauktības un atjaunošanas plāns. Plānā norāda atjaunošanas secību, krīzes komandu un ārkārtas kontaktus.

11.3. Vismaz vienu rezerves kopiju glabā nošķirti: bezsaistē vai nemainīgā krātuvē, kuru nevar izdzēst vai šifrēt ar tiem pašiem piekļuves datiem, ar kuriem piekļūst pamatsistēmai.

11.4. Krīzes gadījumā valde sasauc krīzes komandu un saziņai izmanto kanālu, kas nav atkarīgs no skartās sistēmas, piemēram, iepriekš sagatavotu tālruņu sarakstu.

11.5. Plānu pārbauda vismaz reizi gadā ar galda vingrinājumu vai atjaunošanas testu. Rezultātu un konstatētos trūkumus fiksē, un plānu atjauno.

11.6. Mākoņdatošanas pakalpojumu (Microsoft 365, Amazon Web Services) datiem veido rezerves kopijas arī tad, ja pakalpojuma sniedzējs datus dublē, jo dublēšana neaizsargā pret nejaušu vai ļaunprātīgu dzēšanu.

12. Piegādātāji un piegādes ķēde

12.1. Valde uztur to piegādātāju sarakstu, kuri piekļūst sabiedrības informācijai vai sniedz IT un mākoņdatošanas pakalpojumus (tostarp Microsoft 365, Amazon Web Services), un katram nosaka kritiskumu.

12.2. Pirms līguma noslēgšanas ar kritisku piegādātāju valde novērtē tā drošību ar šai politikai pievienoto piegādātāju drošības anketu.

12.3. Līgumā ar piegādātāju, kurš piekļūst sabiedrības informācijai, nosaka konfidencialitātes pienākumu, pienākumu bez kavēšanās, bet ne vēlāk kā 24 stundu laikā ziņot par kiberincidentu, datu glabāšanas vietu, apakšuzņēmēju piesaisti tikai ar sabiedrības piekrišanu un datu atdošanu vai dzēšanu pēc līguma izbeigšanas.

12.4. Ja piegādātājs apstrādā personas datus sabiedrības uzdevumā, ar to noslēdz datu apstrādes līgumu, kas atbilst VDAR 28. pantam.

12.5. Piegādātāja piekļuvi sabiedrības sistēmām piešķir personalizētu, ar daudzfaktoru autentifikāciju un uz noteiktu laiku. Piekļuvi atceļ, tiklīdz darbs ir pabeigts.

12.6. Kritisko piegādātāju atbilstību līgumam un šai politikai pārskata vismaz reizi gadā.

12.7. Ārējais IT pakalpojumu sniedzējs ievēro šo politiku tajā apjomā, kādā tas pārvalda sabiedrības sistēmas. Atbildība par politikas izpildi paliek valdei.

13. Personāla drošība un apmācības

13.1. Pirms piekļuves piešķiršanas darbinieks paraksta konfidencialitātes saistības un apliecina, ka ir iepazinies ar darbinieku instrukciju. Apliecinājumu glabā kopā ar iepazīšanās lapu.

13.2. Jaunais darbinieks informācijas drošības ievadapmācību iziet pirmās darba nedēļas laikā. Visi darbinieki atkārtotu apmācību iziet vismaz reizi gadā; tā ietver pikšķerēšanas atpazīšanu un incidentu ziņošanu.

13.3. Valdes locekļi regulāri iziet apmācību par kiberdrošības riskiem un to pārvaldību atbilstoši mērķa standartam (ES NIS2 direktīva un Latvijas Nacionālais kiberdrošības likums).

13.4. Katru apmācību ieraksta apmācību uzskaitē, norādot datumu, tēmu un dalībniekus.

13.5. Mainot amatu, piekļuves tiesības pielāgo jaunajam amatam. Izbeidzot darba tiesiskās attiecības, piekļuves tiesības atceļ ne vēlāk kā pēdējā darba dienā, un darbinieks atdod iekārtas un informācijas nesējus.

13.6. Konfidencialitātes pienākums ir spēkā arī pēc darba tiesisko attiecību izbeigšanas. Par šīs politikas pārkāpumu piemēro disciplināro atbildību saskaņā ar darba līgumu un piemērojamiem tiesību aktiem.

14. Incidenti

14.1. Šīs sadaļas termiņus skaita no brīža, kad fakts kļūst zināms, ja nav noteikts vēlāks sākuma brīdis. Termiņa nokavējums neatbrīvo no ziņošanas pienākuma.

14.2. Darbinieks nekavējoties, bet ne vēlāk kā vienas stundas laikā no konstatēšanas brīža, ziņo tiešajam vadītājam, kas noticis, kad, kuru sistēmu incidents skāris un vai dati ir bijuši pieejami nepiederošai personai. Darbinieks vispirms ziņo un notikumu patstāvīgi nenovērš.

14.3. Darbinieks aizdomīgo iekārtu nekavējoties atvieno no tīkla un to atkārtoti neieslēdz, kamēr vadība nav devusi norādījumu.

14.4. Elektroniskā pasta ziņojumus, žurnāluzskaiti un ekrānuzņēmumus saglabā kā pierādījumus arī tad, ja to dzēšanu lūdz persona, kura uzdodas par palīdzības dienestu.

14.5. Izspiešanas pieprasījumu neapmaksā un datus tālāk nenodod. Maksājuma lēmumu ir tiesīga pieņemt tikai valde, un šajā politikā tāds maksājums nav paredzēts.

14.6. Vadība četru stundu laikā no ziņojuma saņemšanas novērtē incidentu, pieņem lēmumu par ierobežošanu un fiksē laiku, skarto sistēmu un veiktās darbības.

14.7. Valde vai tās norīkota persona, nevis darbinieks, sniedz kompetentajai iestādei agrīno brīdinājumu 24 stundu laikā, paziņojumu 72 stundu laikā un noslēguma ziņojumu viena mēneša laikā saskaņā ar Nacionālo kiberdrošības likumu. Valde paziņojuma nosūtīšanu fiksē rakstveidā.

14.8. Ja kiberincidents skar personas datus, valde rīkojas arī saskaņā ar 15. sadaļu.

15. Personas datu aizsardzība

15.1. Sabiedrība apstrādā šādus datus: klientu un darbinieku personas dati, maksājumu karšu un finanšu dati. Personas datu apstrādei piemēro Vispārīgo datu aizsardzības regulu (VDAR), un šī sadaļa papildina mērķa standarta prasības.

15.2. Valde uztur personas datu apstrādes darbību reģistru, kurā norāda apstrādes mērķi, datu kategorijas, saņēmējus un glabāšanas termiņu.

15.3. Personas datus apstrādā tikai noteiktam mērķim un glabā ne ilgāk, kā tas nepieciešams šim mērķim. Pēc tam datus dzēš vai anonimizē.

15.4. Ja kiberincidents skar personas datus un var radīt risku fizisku personu tiesībām, valde par to paziņo Datu valsts inspekcijai 72 stundu laikā no brīža, kad pārkāpums kļuvis zināms. Ja risks ir augsts, valde informē arī skartās personas.

15.5. Pirms jaunas augsta riska apstrādes, piemēram, liela apjoma īpašu kategoriju datu apstrādes vai sistemātiskas uzraudzības, valde veic novērtējumu par ietekmi uz datu aizsardzību un izvērtē, vai jāieceļ datu aizsardzības speciālists.

15.6. Maksājumu karšu datus sabiedrības sistēmās neglabā, ja maksājumus apstrādā sertificēts maksājumu pakalpojumu sniedzējs. Ja karšu datus glabā, piemēro maksājumu karšu nozares drošības standartu (PCI DSS).

16. Informācijas klasifikācija

16.1. Informāciju iedala trīs klasēs. Šī politika ir konfidenciāla un paredzēta valdei. Šā dokumenta atzīme ir: Konfidenciāls.

16.2. Klasi nosaka valde vai tās norīkota persona brīdī, kad informācija rodas vai kad to saņem. Informāciju bez klases uzskata par konfidenciālu, līdz klase ir noteikta.

16.3. Klasi norāda uz dokumenta. Klasi maina vai pazemina tikai valde vai tās norīkota persona, un maiņu fiksē.

16.4. Informāciju nodod tikai personai, kurai attiecīgā klase to atļauj. Ja notikusi nodošana, ko klase neatļauj, darbinieks par to nekavējoties ziņo tiešajam vadītājam.

16.5. Ja informācija ir nonākusi pie personas, kurai tā nav paredzēta, darbinieks tālāku izplatīšanu aptur, un vadība nosaka, vai ir iestājies kiberincidents.

Publisks

16.6. Dokumentu ir tiesīga iepazīt jebkura persona, tostarp ārpus sabiedrības. Šo klasi piešķir tikai informācijai, kuras izpaušana sabiedrībai kaitējumu nerada.

16.7. Dokumentu glabā vietā, kas paredzēta publiskai informācijai. To neglabā kopā ar konfidenciālu informāciju.

16.8. Dokumentu nosūta pa sabiedrības apstiprinātajiem saziņas līdzekļiem. Nosūtīšana pati par sevi klasi nemaina.

16.9. Novecojušu publicētu versiju aizstāj ar aktuālo versiju. Novecojušo versiju par aktuālu neuzrāda.

16.10. Publisku informāciju neapzīmē ar augstāku klasi, lai ierobežotu tās pieejamību. Šādu apzīmējumu valde atceļ.

Iekšējs

16.11. Dokumentu ir tiesīgi iepazīt tikai sabiedrības darbinieki un norīkotie partneri. Personai, kas šim lokam nepieder, dokumentu neizsniedz.

16.12. Dokumentu glabā darba vietā, kas nav publiski pieejama. To nepublicē publiski pieejamā vietnē.

16.13. Dokumentu nosūta tikai uz darba elektroniskā pasta adresi vai pa apstiprinātu saziņas līdzekli.

16.14. Ja dokuments nonāk ārpus sabiedrības, par to ziņo vadībai un kopiju atsauc. Līdz atsaukšanai tālāku izplatīšanu aptur.

16.15. Iekšēju informāciju nenodod personai, kura nav darbinieks vai norīkots partneris. Ja vadība to pieprasa, nodošanu fiksē.

Konfidenciāls

16.16. Dokumentu ir tiesīgas iepazīt tikai personas, kurām tas nepieciešams darba pienākumu izpildei.

16.17. Dokumentu glabā aizsargātā vietā ar ierobežotu piekļuvi. Piekļuvi šai vietai piešķir valde.

16.18. Dokumentu nosūta tikai šifrētā vai apstiprinātā saziņas līdzeklī, nekad uz personīgo elektronisko pastu.

16.19. Ja dokuments nonāk pie nepiederošas personas, par to nekavējoties ziņo vadībai un tālāku izplatīšanu aptur. Vadība nosaka turpmāko kārtību.

16.20. Konfidenciālas informācijas kopiju izgatavo tikai ar vadības atļauju. Atļauto kopiju uzskaita un pēc pienākuma izpildes iznīcina vai atdod.

17. Efektivitātes novērtēšana un pārskatīšana

17.1. Valde šo politiku pārskata vismaz reizi gadā, kā arī pēc būtiska kiberincidenta vai būtiskām izmaiņām sabiedrības darbībā vai piemērojamos tiesību aktos.

17.2. Politikas efektivitāti vērtē pēc šādiem rādītājiem: daudzfaktoru autentifikācijas pārklājums, drošības atjauninājumu uzstādīšanas laiks, veiksmīgo atjaunošanas testu skaits, apmācīto darbinieku īpatsvars, kiberincidentu skaits un reaģēšanas laiks, rīcības plāna pasākumi, kas izpildīti termiņā.

17.3. Valdes norīkota persona kopā ar ārējo IT pakalpojumu sniedzēju vismaz reizi gadā iesniedz valdei pārskatu par šiem rādītājiem. Valde pārskatu izskata un lēmumu fiksē protokolā.

17.4. Valde vismaz reizi gadā veic pašnovērtējumu par šīs politikas un Nacionālā kiberdrošības likuma prasību izpildi. Pašnovērtējumu un, ja likums to prasa, neatkarīgu auditu valde iesniedz Nacionālajam kiberdrošības centram (NKC) likumā un uz tā pamata izdotajos normatīvajos aktos noteiktajā kārtībā un termiņos.

17.5. Konstatēto neatbilstību fiksē, iekļauj rīcības plānā ar termiņu un atbildīgo un pēc novēršanas pārbauda, vai pasākums ir efektīvs.

18. Atbilstības tabula

18.1. Šī tabula sasaista politikas sadaļas ar mērķa standarta (ES NIS2 direktīva un Latvijas Nacionālais kiberdrošības likums) prasībām. Personas datu aizsardzības prasības sedz 15. sadaļa.

18.2. Tabula neaizstāj auditu un neapliecina, ka sabiedrība ir sertificēta vai atbilst tiesību aktam. Ja tabulas rinda ir šaurāka par tiesību aktu, piemēro tiesību aktu.

18.3. Valde tabulu salīdzina ar faktisko praksi vismaz reizi gadā un atšķirību iekļauj trūkumu analīzē un rīcības plānā.

Prasība	Politikas sadaļa	Ieraksts vai pielikums
20. pants — vadības atbildība un apmācības	2. un 13. sadaļa	Valdes lēmums; apmācību uzskaite
21. panta 2. punkta a) apakšpunkts — riska analīze un informācijas sistēmu drošības politika	1. un 3. sadaļa	Riska reģistrs
21. panta 2. punkta b) apakšpunkts — incidentu apstrāde	14. sadaļa	Kiberincidentu reģistrs
21. panta 2. punkta c) apakšpunkts — darbības nepārtrauktība, rezerves kopijas, krīzes vadība	10. un 11. sadaļa	Nepārtrauktības plāns; atjaunošanas protokols
21. panta 2. punkta d) apakšpunkts — piegādes ķēdes drošība	12. sadaļa	Piegādātāju drošības anketa
21. panta 2. punkta e) apakšpunkts — drošība iegādē, izstrādē un uzturēšanā, ievainojamību pārvaldība	9. un 12. sadaļa	Rīcības plāns
21. panta 2. punkta f) apakšpunkts — pasākumu efektivitātes novērtēšana	17. sadaļa	Trūkumu analīze un rīcības plāns
21. panta 2. punkta g) apakšpunkts — pamata drošības prakse un apmācības	7. un 13. sadaļa	Darbinieku instrukcija; apmācību uzskaite
21. panta 2. punkta h) apakšpunkts — kriptogrāfija un šifrēšana	8. sadaļa	Aktīvu reģistrs
21. panta 2. punkta i) apakšpunkts — personāla drošība, piekļuves kontrole, aktīvu pārvaldība	4., 10. un 13. sadaļa	Piekļuves tiesību žurnāls; aktīvu reģistrs
21. panta 2. punkta j) apakšpunkts — daudzfaktoru autentifikācija, droša un ārkārtas saziņa	4., 8. un 11. sadaļa	Nepārtrauktības plāns
23. pants — ziņošanas pienākumi	14. sadaļa	Kiberincidentu reģistrs

19. Noslēguma jautājumi

19.1. Dokuments ir melnraksts no sabiedrības sniegtajām atbildēm. Valde to neuzskata par apstiprinātu, kamēr nav parakstījusi apstiprinājumu. Melnraksta piemērošana pirms apstiprināšanas nav pieļaujama, izņemot gadījumu, kad valde to ir rakstveidā noteikusi.

19.2. Pirms apstiprināšanas dokumentu pārskata valdes norīkota persona. Šī persona pārbauda, vai fakti atbilst sabiedrības darbībai. Ja fakti neatbilst, politiku labo un pārskata atkārtoti.

19.3. Tas nav juridiska konsultācija un neapliecina atbilstību auditam. Dokuments nenovērš valdes pienākumu piemērot tiesību aktus. Atsauce uz šo dokumentu neatbrīvo no atbildības par tiesību akta pārkāpumu.

19.4. Politiku groza valde. Grozījumu izdara rakstveidā un norāda datumu, no kura grozījums stājas spēkā. Mutisku grozījumu par spēkā esošu neatzīst.

19.5. Ja šīs politikas punkts ir pretrunā ar piemērojamu tiesību aktu, piemēro tiesību aktu. Pārējos punktus turpina piemērot. Pretrunu valde novērš nākamajā politikas redakcijā.