					Šeit ievadiet reģistrētās juridiskās personas nosaukumu						
Dokumenta numurs: P30					Dokumenta nosaukums: **Incidentu reaģēšanas politika**						
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:						
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts, 9. punkts	Strukturēti procesi risku pārvaldībai un incidentu reaģēšanai
ISO/IEC 27002:2022	5.25–5.27 kontroles pasākumi	Lomas, ziņošana, reaģēšana un pilnveide incidentu pārvaldībā
NIST SP 800-53 Rev.5	IR-1 līdz IR-9	Visaptverošs incidentu reaģēšanas dzīves cikls
ES GDPR	33. panta 1. daļa, 33. panta 3. daļas a)–d) apakšpunkts, 34. panta 1. daļa, 34. panta 2. daļas a)–c) apakšpunkts	Pārkāpumu paziņošanas termiņi, ziņošana un saziņa ar datu subjektiem
ES NIS2	23. panta 1.–4. daļa	Paziņošana valsts kompetentajai iestādei un strukturēta ziņošana
ES DORA	17. panta 1.–3. daļa	Būtisku ar IKT saistītu incidentu ziņošana finanšu subjektiem
COBIT 2019	DSS02, DSS04, MEA	Nosaka, uzrauga un izvērtē incidentu pārvaldību, darbības nepārtrauktību un izvērtēšanu

1. Mērķis

1.1 Šī politika nosaka formālu ietvaru organizāciju ietekmējošu informācijas drošības incidentu identificēšanai, ziņošanai, analīzei, ierobežošanai, reaģēšanai, atjaunošanai un pēcincidenta izvērtēšanai.

1.2 Tā nodrošina savlaicīgu, koordinētu un efektīvu reaģēšanu, lai mazinātu darbības traucējumus, finanšu zaudējumus, reputācijas kaitējumu un normatīvās atbilstības pārkāpumu risku.

1.3 Politika veicina arī nepārtrauktu organizācijas kiberdrošības noturības pilnveidi, integrējot gūtās mācības un pēcincidenta konstatējumus pārvaldībā, rīkos un apmācību programmās.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visu personālu, tostarp darbiniekiem, līgumslēdzējiem, konsultantiem un trešo pušu pakalpojumu sniedzējiem;

2.1.2 visām informācijas sistēmām, lietojumprogrammām, infrastruktūru, tīkliem un datiem neatkarīgi no tā, vai tie atrodas lokāli, mākoņvidē vai hibrīdvidē;

2.1.3 visu veidu drošības incidentiem, tostarp, bet ne tikai:

2.1.3.1 nesankcionētai piekļuvei vai privilēģiju paaugstināšanai;

2.1.3.2 ļaunatūras un izspiedējprogrammatūras uzbrukumiem;

2.1.3.3 pakalpojuma atteices (DoS/DDoS) uzbrukumiem;

2.1.3.4 datu zudumam, noplūdei vai neatļautai datu iznesei;

2.1.3.5 iekšējai neatbilstošai lietošanai vai politikas pārkāpumiem;

2.1.3.6 fiziskās drošības pārkāpumiem, kas ietekmē digitālos aktīvus.

2.2 Politika aptver atklāšanu, triāžu, izmeklēšanu, eskalāciju, ierobežošanu, pierādījumu apstrādi, paziņošanu, atjaunošanu un pamatcēloņa analīzi.

3. Mērķi

3.1 Izveidot atkārtojamu un mērogojamu incidentu reaģēšanas spēju, kas nodrošina ātru drošības incidentu atklāšanu, klasificēšanu un mazināšanu.

3.2 Samazināt drošības incidentu ietekmi uz darbību, izmantojot strukturētas ierobežošanas, izskaušanas un sistēmu atjaunošanas procedūras.

3.3 Nodrošināt, ka incidentu ziņošana un reaģēšana atbilst tiesiskajām, regulatīvajām un līgumiskajām prasībām, jo īpaši attiecībā uz pārkāpumu paziņošanas termiņiem un pierādījumu apstrādi.

3.4 Veicināt pārredzamību un pārskatatbildību, nodrošinot pienācīgu žurnālfiksēšanu, dokumentēšanu un metriku uzskaiti visiem drošības incidentiem.

3.5 Veicināt nepārtrauktu pilnveidi, izmantojot pēcincidenta pārskatīšanu, korektīvās darbības un iesaistīto pušu apmācību.

4. Lomas un pienākumi

4.1 Galvenais informācijas drošības vadītājs (CISO)

4.1.1 Ir incidentu reaģēšanas ietvara īpašnieks, nodrošina politikas ievērošanu un pārrauga incidentu koordinēšanu visā organizācijā.

4.1.2 Pilda galvenā kontaktpunkta funkciju saziņā ar regulatoriem, izpildvadību un ārējiem juridiskajiem konsultantiem būtisku incidentu laikā.

4.2 Incidentu reaģēšanas koordinators

4.2.1 Koordinē starpfunkcionālās reaģēšanas komandas, pārvalda darbplūsmas un uzrauga ierobežošanas un atjaunošanas statusu.

4.2.2 Ierosina un vada pēcincidenta pārskatīšanu (PIR) un nodrošina, ka korektīvās darbības tiek reģistrētas un īstenotas.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika jāpārskata vismaz reizi gadā un, ja nepieciešams, jāgroza, lai iekļautu:

9.1.1 izmaiņas apdraudējumu vidē, incidentu veidos vai uzbrukumu vektoros;

9.1.2 no būtiskiem incidentiem, gandrīz notikušiem gadījumiem vai regulatīvajiem konstatējumiem gūtās mācības;

9.1.3 atjauninājumus piemērojamajos tiesību aktos un regulējumā (piemēram, GDPR, DORA, NIS2);

9.1.4 atsauksmes no incidentu reaģēšanas mācībām un pēcincidenta pārskatīšanām.

9.2 CISO ir atbildīgs par pārskatīšanas procesa ierosināšanu un koordinēšanu, konsultējoties ar:

9.2.1.1 juridisko konsultantu un datu aizsardzības speciālistu;

9.2.1.2 SOC un IT operāciju komandām;

9.2.1.3 darbības nepārtrauktības un risku pārvaldības komandām;

9.2.1.4 izpildvadību.

9.3 Politikas grozījumiem:

9.3.1 jābūt dokumentētiem repozitorijā, kas tiek pārvaldīts ar versiju kontroli;

9.3.2 jābūt paziņotiem visām ietekmētajām komandām un atspoguļotiem informētības apmācībā;

9.3.3 jābūt validētiem, izmantojot scenāriju vai praktiskās incidentu reaģēšanas mācības trīs mēnešu laikā pēc apstiprināšanas.

9.4 Steidzami atjauninājumi, ko izraisa jauni riski, audita konstatējumi vai jaunizdotas tiesiskās prasības, jāievieš nekavējoties un jāatspoguļo politikas grozījumu vēsturē.

10. Saistītās politikas un sasaiste

10.1 Šo politiku atbalsta un ar to ir saistītas šādas organizācijas politikas:

10.1.1 P1 – Informācijas drošības politika: nosaka vispārīgas prasības uz risku balstītai pieejai un incidentiem gatavai darbībai.

10.1.2 P5 – Izmaiņu pārvaldības politika: nodrošina, ka ierobežošanas un atjaunošanas darbības, kas saistītas ar infrastruktūru vai pakalpojumiem, tiek veiktas saskaņā ar formālām procedūrām.

10.1.3 P13 – Datu klasifikācijas un marķēšanas politika: atbalsta incidenta smaguma pakāpes klasificēšanu, pamatojoties uz datu sensitivitāti.

10.1.4 P15 – Rezerves kopiju veidošanas un atjaunošanas politika: nodrošina atjaunošanu pēc izspiedējprogrammatūras vai destruktīviem uzbrukumiem, saglabājot integritāti.

10.1.5 P18 – Kriptogrāfisko kontroles pasākumu politika: nosaka šifrēšanas pasākumus, kas samazina incidenta ietekmi un datu ekspozīcijas riskus.

10.1.6 P22 – Žurnālfiksēšanas un uzraudzības politika: nosaka notikumu redzamības, brīdināšanas un audita žurnālu glabāšanas pamatprasības efektīvai atklāšanai un digitālajai kriminālistikai.

10.1.7 P29 – Testa datu un testa vides politika: nodrošina, ka incidenti, kas skar neprodukcijas sistēmas, arī tiek apstrādāti strukturēti un droši.

10.1.8 P33 – Audita un atbilstības uzraudzības politika: validē incidentu gatavību un reaģēšanas efektivitāti, izmantojot strukturētus auditus un atbilstības izvērtēšanu.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001:2022, 8. punkts – darbības plānošana un kontrole: strukturēti procesi risku pārvaldībai un incidentu reaģēšanas plānošanai.

11.2 ISO/IEC 27002:2022 – 5.25–5.27 kontroles pasākumi: pienākumi incidentu pārvaldībā, ziņošanā, reaģēšanā, saziņā un pilnveidē.

11.3 NIST SP 800-53 Rev.5: IR-1 līdz IR-9, AU-6, PL-2: visaptverošas prasības incidentu reaģēšanas dzīves ciklam, auditam un drošības plānošanai.

11.4 ES GDPR: 33. un 34. pants: pienākumi ziņot uzraudzības iestādēm un prasības paziņošanai datu subjektiem (ar noteiktiem izņēmumiem).

11.5 ES NIS2 direktīva (2022/2555): 23. pants: obligāta valsts līmeņa ziņošana ar starpposma un galīgās ziņošanas pienākumiem.

11.6 ES DORA (2022/2554): 17. pants: finanšu iestāžu prasības ziņošanai iestādēm par IKT incidentiem.

11.7 COBIT 2019: DSS02, DSS04, MEA01: pakalpojumu incidentu un darbības nepārtrauktības pārvaldība, kā arī veiktspējas un atbilstības uzraudzība.