					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P12					Dokumenta nosaukums: **Aktīvu pārvaldības 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**

1. Mērķis

1.1 Šī politika nosaka obligātās organizatoriskās prasības informācijas aktīvu identificēšanai, klasificēšanai, pārvaldībai un aizsardzībai visā to dzīves ciklā. Tā nosaka prasības aparatūras, programmatūras, datu, mākoņpakalpojumu un nemateriālo informācijas aktīvu pārvaldībai visā organizācijā, tostarp mobilajās, attālinātajās un trešo pušu pārvaldītajās vidēs.

1.2 Šīs politikas mērķis ir nodrošināt pilnīgu pārskatāmību par organizācijas informācijas aktīvu kopumu, lai īstenotu efektīvus drošības kontroles pasākumus, noteiktu īpašumtiesības, nodrošinātu atbilstību prasībām un veiktu kontrolētu izņemšanu no ekspluatācijas vai likvidēšanu.

1.3 Politika ir saskaņota ar ISO/IEC 27001:2022 A pielikuma 5.9. kontroli, nosakot prasību uzturēt centralizētu informācijas un ar to saistīto aktīvu uzskaiti. Tā nodrošina pārskatatbildību, piesaistot katram aktīvam īpašnieku un piemērojot klasifikācijā balstītu aizsardzību atbilstoši darbības sensitivitātei un normatīvajām prasībām.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visiem darbiniekiem, līgumslēdzējiem, trešo pušu piegādātājiem un pakalpojumu sniedzējiem, kuri pārvalda, izmanto, piekļūst, glabā vai apstrādā organizācijai piederošus vai tās kontrolētus informācijas aktīvus.

2.2 Piemērošanas joma ietver visas aktīvu kategorijas, tai skaitā:

2.2.1 Fiziskie aktīvi: klēpjdatori, galddatori, mobilās ierīces, noņemamie datu nesēji, printeri, tīkla iekārtas

2.2.2 Digitālie aktīvi: programmatūra, lietotnes, sistēmu attēli, datubāzes, rezerves kopiju dati, šifrēšanas atslēgas

2.2.3 Informācijas aktīvi: strukturēti un nestrukturēti dati, pārskati, e-pasti, intelektuālais īpašums

2.2.4 Mākoņpakalpojumu un virtuālie aktīvi: IaaS, SaaS, PaaS vides, virtuālās mašīnas, konteineri

2.2.5 Loģiskie aktīvi: domēna vārdi, licences, lietotāju konti, pamatkonfigurācijas

2.3 Politika attiecas arī uz aktīviem, kas tiek izmantoti attālinātā darba, hibrīdvidēs vai ārpakalpojumu vidēs, nodrošinot aizsardzību un pārskatāmību arī tad, ja aktīvi fiziski neatrodas organizācijas telpās.

3. Mērķi

3.1 Uzturēt pilnīgu, precīzu un aktuālu visu organizācijas informācijas aktīvu uzskaiti, norādot to īpašnieku, klasifikāciju un atrašanās vietu.

3.2 Noteikt aktīvu īpašniekus, kuri ir atbildīgi par to pārziņā esošo aktīvu klasificēšanu, apstrādi un aizsardzību atbilstoši datu pārvaldības un drošības politikām.

3.3 Piemērot visiem aktīviem atbilstošu klasifikāciju un marķējumu, pamatojoties uz sensitivitāti, kritiskumu un normatīvajām prasībām.

3.4 Aizsargāt aktīvus atbilstoši to klasifikācijai un saistītajai pakļautībai riskam, tostarp glabāšanas, piekļuves, pārsūtīšanas un likvidēšanas laikā.

3.5 Nodrošināt aktīvu atdošanas un drošas likvidēšanas procedūru ievērošanu darbinieka atiešanas procesa, līguma izbeigšanas vai aktīva dzīves cikla noslēguma laikā.

3.6 Atbalstīt atbilstību tādiem ietvariem kā ISO/IEC 27001, GDPR, NIS2, DORA un COBIT 2019, izmantojot strukturētu aktīvu pārvaldību un auditējamību.

4. Lomas un pienākumi

4.1 Izpildvadība

4.1.1 Apstiprina Aktīvu pārvaldības politiku un nodrošina resursu piešķiršanu tās pilnīgai ieviešanai.

4.1.2 Uzņemas galīgo pārskatatbildību par to, ka organizācijas aktīvi tiek aizsargāti un pārvaldīti atbilstoši normatīvajām un līgumiskajām prasībām.

4.2 Galvenais informācijas drošības vadītājs (CISO)

4.2.1 Ir Aktīvu pārvaldības politikas īpašnieks un nodrošina tās integrāciju organizācijas informācijas drošības pārvaldības sistēmā.

4.2.2 Pārskata izņēmumus un atkāpes no šīs politikas un nosaka uz risku balstītus mazināšanas pasākumus.

4.2.3 Uzrauga periodiskus aktīvu klasifikācijas, aktīvu uzskaites integritātes un aktīvu dzīves cikla atbilstības auditus.

[... 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 vai, reaģējot uz:

9.1.1 izmaiņām tiesiskajos vai normatīvajos pienākumos, kas ietekmē aktīvu klasifikāciju vai uzskaites prasības;

9.1.2 jaunu aktīvu kategoriju vai pārvaldības platformu ieviešanu (piemēram, mākoņvidē izvietotas CMDB);

9.1.3 iekšējā audita konstatējumiem vai drošības incidentiem, kas saistīti ar neatbilstošu aktīvu pārvaldību;

9.1.4 organizatoriskām pārmaiņām, kas ietekmē īpašumtiesības vai dzīves cikla kontroles pasākumus.

9.2 Pārskatīšanas process jāuzsāk IT aktīvu pārvaldniekam un jāsaskaņo ar CISO, Iepirkumu, Juridisko lietu un atbildīgajiem struktūrvienību vadītājiem.

9.3 Starpposma pārskatīšanu var ierosināt arī:

9.3.1 biznesa vienību iegāde vai atsavināšana;

9.3.2 piegādātāju izmaiņas, kas ietekmē trešo pušu pārvaldītos aktīvus;

9.3.3 tehnoloģiju atjaunošana, kas saistīta ar masveida izņemšanu no ekspluatācijas vai piešķiršanu.

9.4 Visiem šīs politikas grozījumiem:

9.4.1 jābūt pārvaldītiem ar versiju kontroli un glabātiem IDPS repozitorijā;

9.4.2 jābūt apstiprinātiem Izpildvadībā;

9.4.3 jāietver izmaiņu kopsavilkums un pamatojums;

9.4.4 jābūt paziņotiem visām skartajām iesaistītajām pusēm, tostarp jānodrošina atjauninātas procedūras vai sistēmu apmācības, ja piemērojams.

10. Saistītās politikas un sasaiste

10.1 Šī politika darbojas kopā ar turpmāk minētajām saistītajām politikām un atbalsta to ievērošanu:

10.1.1 P4 - Piekļuves kontroles politika: nodrošina, ka aktīvu pārskatāmība ir saskaņota ar piekļuves tiesībām un kontroles mehānismiem visās sistēmās un datu vidēs.

10.1.2 P7 - Darba tiesisko attiecību uzsākšanas un izbeigšanas politika: nosaka savlaicīgu fizisko un loģisko aktīvu piešķiršanu un atdošanu personāla pāreju laikā.

10.1.3 P13 - Datu klasifikācijas un marķēšanas politika: nosaka obligātos aktīvu klasifikācijas noteikumus, kas nosaka marķēšanas, apstrādes un likvidēšanas procedūras.

10.1.4 P14 - Datu glabāšanas un likvidēšanas politika: nosaka drošas likvidēšanas termiņus un metodes digitāliem un fiziskiem aktīviem, kas satur informāciju.

10.1.5 P22 - Žurnālfiksēšanas un uzraudzības politika: nodrošina aktīvu piekļuves un izmantošanas izsekojamību, izmantojot sistēmu žurnālfiksēšanu, galapunktu pārskatāmību un uzvedības analītiku.

10.1.6 P30 - Incidentu reaģēšanas politika: atbalsta ātru ierobežošanu un izmeklēšanu aktīvu incidentu gadījumā, piemēram, nozaudētu klēpjdatoru vai neuzskaitītu datu nesēju gadījumos.

10.2 Šīs politikas veido vienotu pārvaldības struktūru, kas nodrošina drošu aktīvu pārvaldību, precīzu uzskaiti un atbilstošu apstrādi visā to dzīves ciklā.

11. Atsauces standarti un ietvari

11.1 Šī politika ir saskaņota ar starptautiski atzītiem informācijas drošības standartiem un normatīvajiem ietvariem, kas visā dzīves ciklā prasa robustu aktīvu pārvaldību.

11.2 ISO/IEC 27001:

11.2.1 Punkts 8.1 - pieprasa organizācijām plānot, ieviest un kontrolēt procesus, kas nepieciešami informācijas drošības prasību izpildei, tostarp aktīvu dzīves cikla pārvaldībai.

11.3 ISO/IEC 27002:2022 - kontroles pasākumi 5.9 līdz 5.11

11.3.1 Punkts 5.9 - informācijas un citu saistīto aktīvu uzskaite: pieprasa aktuālu un pilnīgu visu informācijas apstrādei nozīmīgo aktīvu uzskaiti.

11.3.2 Punkts 5.10 - informācijas un aktīvu pieļaujama izmantošana: tiek nodrošināta ar lietošanas noteikumiem, īpašumtiesībām un atdošanas procesiem.

11.3.3 Punkts 5.11 - aktīvu atdošana: tiek īstenota ar formālām nodošanas un izņemšanas no ekspluatācijas procedūrām.

11.3.4 Šie kontroles pasākumi nosaka strukturētas prasības organizācijas aktīvu identificēšanai, marķēšanai, uzturēšanai un uzskaitei, paredzot attiecīgus pienākumus īpašniekiem un turētājiem visā dzīves ciklā.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - sistēmas komponentu uzskaite: atspoguļota centralizētā aktīvu pārvaldībā, reāllaika pārskatāmībā un sasaistē ar darbības konfigurācijām.

11.4.2 RA-3 - risku izvērtēšana: aktīvu uzskaite kalpo kā pamatkomponents apdraudējumu modelēšanai un riska izvērtēšanai.

11.4.3 MP-6 - datu nesēju sanitizācija: tiek nodrošināta ar drošām likvidēšanas metodēm, kas noteiktas aktīvu dzīves cikla kontroles pasākumos un Datu likvidēšanas politikā.

11.5 ES GDPR (2016/679):

11.5.1 Pants 30 - apstrādes darbību ieraksti: pieprasa organizācijām dokumentēt sistēmas, ierīces un repozitorijus, kuros tiek glabāti vai apstrādāti personas dati.

11.5.2 Pants 32 - apstrādes drošība: ir saskaņots ar aktīvos balstītu risku izvērtēšanu un drošības pasākumiem, kas pielāgoti klasificētiem aktīviem un kritiskajai infrastruktūrai.

11.6 ES NIS2 direktīva (2022/2555):

11.6.1 Pants 21(2)(a, b): nosaka aktīvu pārskatāmību un uzskaiti kā pamatu riska analīzei, aizsardzībai un kiberdrošības incidentu reaģēšanai.

11.6.2 Pants 21(3): pastiprina nepieciešamību pēc strukturētas aktīvu pārvaldības kā organizācijas drošības kultūras sastāvdaļas.

11.7 ES DORA (2022/2554):

11.7.1 Pants 5 - IKT pārvaldība un iekšējā kontrole: pieprasa finanšu iestādēm kontrolēt IKT aktīvus, nosakot skaidras uzskaites, īpašumtiesību un aizsardzības prasības.

11.7.2 Pants 9 - IKT risku pārvaldības ietvars: nosaka, ka aktīvu pārvaldības procesiem jāatbalsta apdraudējumu mazināšana, darbības nepārtrauktības plānošana un pakalpojumu noturība.

11.8 COBIT 2019:

11.8.1 BAI09 - aktīvu pārvaldība: tieši atbilst strukturētai uzņēmuma aktīvu identificēšanai, klasificēšanai, izmantošanai un likvidēšanai.

11.8.2 DSS01 - pārvaldītas operācijas: atbalsta tādu kontroles pasākumu ieviešanu, kas nodrošina aktīvu aizsardzību un nepārtrauktu darbības pārvaldību.

11.8.3 MEA03 - atbilstības uzraudzība, novērtēšana un izvērtēšana: nodrošina regulāru aktīvu pārvaldības kontroles pasākumu un to efektivitātes auditēšanu normatīvās atbilstības nodrošināšanai.