					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P22					Documenttitel: **Logging- en monitoringbeleid**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

1. Doel

1.1 Het doel van dit beleid is het vaststellen van duidelijke en afdwingbare vereisten voor het genereren, beschermen, beoordelen en analyseren van logboeken waarin belangrijke systeem- en beveiligingsgebeurtenissen binnen de IT-omgeving van de organisatie worden vastgelegd.

1.2 Logging en monitoring zijn essentieel voor detectie van anomalieën, respons op dreigingen, forensisch onderzoek, auditgereedheid en naleving van wet- en regelgeving. Dit beleid waarborgt dat alle door systemen gegenereerde gebeurtenissen correct worden vastgelegd, bewaard en gecorreleerd met nauwkeurige, tijdgesynchroniseerde tijdstempels.

1.3 Dit beleid is essentieel ter ondersteuning van ISO/IEC 27001, clausule 8.1, en Annex A-beheersmaatregelen 8.15 (Logging), 8.16 (Monitoring) en 8.17 (Kloksynchronisatie), en is direct gekoppeld aan verplichtingen uit de AVG, NIS2, DORA en COBIT 2019.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle systemen, diensten en omgevingen die gegevens opslaan, verwerken of verzenden die binnen het managementsysteem voor informatiebeveiliging (ISMS) vallen, waaronder:

2.1.1 on-premises infrastructuur, cloudgehoste diensten (bijv. IaaS, PaaS, SaaS) en hybride omgevingen

2.1.2 besturingssystemen, databases, applicaties en netwerkapparatuur

2.1.3 beveiligingssystemen zoals SIEM-systemen, firewalls, platforms voor endpointdetectie en -respons (EDR), VPN-concentrators en identiteitsproviders

2.2 De volgende stakeholders vallen binnen de reikwijdte:

2.2.1 interne gebruikers met systeemrechten of beheerdersrechten

2.2.2 infrastructuurpersoneel en IT-beheer

2.2.3 het Security Operations Center (SOC) en teams voor dreigingsdetectie

2.2.4 softwareontwikkelaars en applicatie-eigenaren

2.2.5 externe dienstverleners die systemen beheren die logboeken genereren

3. Doelstellingen

3.1 Waarborgen dat alle kritieke systemen logboeken van beveiligingsgebeurtenissen en registraties van systeemactiviteiten genereren die worden bewaard overeenkomstig wettelijke, regelgevende en contractuele vereisten.

3.2 De minimale gebeurtenistypen en de minimale loginhoud vaststellen die nodig zijn om ongeautoriseerde activiteiten te detecteren, gebruikershandelingen te herleiden en forensisch onderzoek te ondersteunen.

3.3 Beheersmaatregelen afdwingen om manipulatie van logboeken, ongeautoriseerde verwijdering of ongecontroleerde toegang tot loggegevens te voorkomen.

3.4 Gecentraliseerde logging- en waarschuwingssystemen (bijv. SIEM) inrichten om verdachte activiteiten nagenoeg realtime te aggregeren, te correleren en te escaleren.

3.5 Kloksynchronisatie waarborgen om nauwkeurige correlatie tussen systemen en incidentanalyse mogelijk te maken.

3.6 Continue verbetering en naleving mogelijk maken door monitoring van logboeken te integreren met audit-, risicobeheer- en incidentbeheerprocessen.

4. Rollen en verantwoordelijkheden

4.1 Chief Information Security Officer (CISO)

4.1.1 Is eigenaar van dit beleid en borgt afstemming op de risicohouding van de organisatie, auditvereisten en ISMS-verplichtingen.

4.1.2 Keurt de loggingreikwijdte voor gereguleerde systemen of systemen met een hoog risico goed en houdt toezicht op nalevingsrapportages.

4.2 SOC-manager

4.2.1 Beheert en onderhoudt gecentraliseerde platforms voor logbeheer (bijv. SIEM).

4.2.2 Definieert regels voor logaggregatie, drempelwaarden voor waarschuwingen en escalatieprocedures voor incidenttriage.

4.2.3 Beoordeelt dagelijkse rapportages en ziet erop toe dat anomalieën worden geanalyseerd, gedocumenteerd en waar nodig geëscaleerd.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Eisen voor herziening en actualisering

9.1 Dit beleid moet jaarlijks worden beoordeeld, of eerder naar aanleiding van:

9.1.1 majeure wijzigingen in de systeemarchitectuur of logginginfrastructuur (bijv. migratie van het SIEM)

9.1.2 wijzigingen in regelgevende vereisten voor logging (bijv. loggingverplichtingen uit NIS2 en DORA)

9.1.3 bevindingen uit audits of evaluaties na incidenten

9.1.4 opkomende dreigingen die verscherpte monitoring vereisen (bijv. insiderdreigingen, compromittering van de toeleveringsketen)

9.2 Het beoordelingsproces wordt geleid door de SOC-manager, in afstemming met de CISO, risicobeheer, compliance en IT-infrastructuurteams.

9.3 Goedgekeurde wijzigingen moeten onder versiebeheer worden opgenomen in het ISMS-documentbeheerregister en worden gecommuniceerd aan:

9.3.1 alle stakeholders die verantwoordelijk zijn voor het beheer van loggingsystemen

9.3.2 applicatie- en systeemeigenaren

9.3.3 externe partijen met taken op het gebied van telemetrie of SIEM-integratie

9.4 Alle vervallen versies moeten veilig worden gearchiveerd, waarbij toegang is beperkt tot geautoriseerde ISMS-beheerders voor audit- en juridische doeleinden.

10. Gerelateerd beleid en samenhang

10.1 P1 – Informatiebeveiligingsbeleid. Legt de fundamentele toezegging vast om systemen en gegevens te beschermen, waarbinnen logging en monitoring kritieke detectieve beheersmaatregelen en responsmogelijkheden ondersteunen.

10.2 P4 – Toegangsbeheerbeleid. Borgt dat geprivilegieerde toegang, gebruikersaanmeldingen en autorisatiegebeurtenissen in logboeken worden vastgelegd en worden bewaakt op misbruik of afwijkend gedrag.

10.3 P5 – Wijzigingsbeheerbeleid. Verplicht logging van systeemwijzigingen, uitrol van patches en configuratie-updates die risico's of ongeautoriseerde wijzigingen kunnen introduceren.

10.4 P21 – Netwerkbeveiligingsbeleid. Vereist logging op netwerkniveau (bijv. firewalllogboeken, IDS/IPS-waarschuwingen, VPN-activiteit) en integratie met het SIEM voor zicht op verkeersafwijkingen en perimeterbeveiliging.

10.5 P23 – Beleid inzake kloksynchronisatie. Dwingt consistente systeemtijd af, wat essentieel is voor betrouwbare logging en correlatie van beveiligingsgebeurtenissen over meerdere omgevingen heen.

10.6 P30 – Incidentresponsbeleid (P30). Steunt op loggegevens en waarschuwingsmechanismen om beveiligingsincidenten te identificeren, te onderzoeken en erop te reageren, en borgt tevens het behoud van forensische artefacten voor evaluatie na incidenten.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 8.1 – Operationele planning en beheersing: vereist beheersmaatregelen voor het monitoren van operaties en het beschermen tegen ongeautoriseerde toegang en misbruik van systemen.

11.2 ISO/IEC 27002:2022 – Beheersmaatregelen 8.15, 8.16, 8.17

11.2.1 Definieert gedetailleerde vereisten voor logging, waaronder welke gebeurtenissen moeten worden vastgelegd, hoe logboeken moeten worden beschermd en geanalyseerd en hoe de betrouwbaarheid van tijdstempels tussen systemen moet worden gewaarborgd.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-2 tot en met AU-12: omvat gebeurtenisselectie, logging, bescherming, auditbeoordeling, respons op auditfouten en bewaring van auditregistraties.

11.3.2 SI-4 – Systeemmonitoring: vereist actieve systeemmonitoring met waarschuwingen op basis van afwijkende activiteiten.

11.3.3 SC-45 – Systeemtijdsynchronisatie: versterkt tijdsnauwkeurigheid ten behoeve van de traceerbaarheid van gebeurtenissen en incidentcorrelatie.

11.4 AVG (Verordening (EU) 2016/679)

11.4.1 Artikel 32 – Beveiliging van de verwerking: vereist technische beheersmaatregelen zoals logging en monitoring om beveiliging en verantwoordingsplicht te waarborgen, in het bijzonder voor toegang tot persoonsgegevens.

11.5 EU NIS2-richtlijn (2022/2555)

11.5.1 Artikel 21(2)(e): verplicht systemen voor gebeurtenislogging en monitoring ten behoeve van snelle detectie van en respons op beveiligingsincidenten.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – ICT-risicobeheer: vereist mechanismen om afwijkende activiteiten te detecteren, incidenten te loggen en forensische gegevens te bewaren.

11.6.2 Artikel 11 – Testen van ICT-bedrijfscontinuïteitsplannen: benadrukt continuïteitsmonitoring en validatie van de beschikbaarheid van logboeken tijdens operationele verstoringen.

11.7 COBIT 2019

11.7.1 DSS01.05 – Beheer van beveiligingslogboeken: vereist implementatie van loggingmogelijkheden voor alle kritieke infrastructuur.

11.7.2 DSS05.04 – Monitoring van beveiligingsgebeurtenissen: verplicht realtime monitoring en analyse van logboeken om gebeurtenissen te detecteren en erop te reageren.

11.7.3 MEA03 – Monitoren, evalueren en beoordelen van naleving: vereist periodieke beoordeling van loggingpraktijken en afstemming op doelstellingen van beheersmaatregelen.