					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P22S					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**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 8	Operationele beheersmaatregelen, waaronder logging
ISO/IEC 27002:2022	Beheersmaatregelen 8.15, 8.16, 8.17	Gebeurtenisregistratie, bescherming van loggegevens en monitoring
NIST SP 800-53 Rev.5	AU-2 tot en met AU-12, SI-4	Inhoud en beoordeling van auditlogs, bewaring, anomaliedetectie en alertering
AVG	Artikelen 5(1)(f), 32, 33	Vertrouwelijkheid en integriteit van gegevens, technische maatregelen en melding van inbreuken
NIS2	Artikelen 21(2)(d), 23	Loggingmechanismen voor anomaliedetectie en incidentmelding binnen 24 uur
DORA	Artikelen 10, 15	Operationele weerbaarheid, monitoring en logging van dienstverleners
COBIT 2019	DSS01.03, DSS05.02	Traceerbaarheid van activiteiten en bescherming door middel van logging en monitoring

1. Doel

1.1 Dit beleid stelt verplichte maatregelen voor logging en monitoring vast om de beveiliging, verantwoordingsplicht en operationele integriteit van de IT-systemen van de organisatie te waarborgen.

1.2 Het beleid beschrijft welke typen gebeurtenissen moeten worden gelogd, hoe loggegevens worden opgeslagen, hoe deze worden beoordeeld en welke verantwoordelijkheden gelden voor personeel en dienstverleners.

1.3 Logging en monitoring ondersteunen dreigingsdetectie, naleving van wet- en regelgeving, incidentrespons en forensisch onderzoek.

1.4 Dit beleid stelt de organisatie in staat te voldoen aan de vereisten voor operationele beheersmaatregelen van ISO/IEC 27001 en ondersteunt het vermogen om naleving aan te tonen, het vertrouwen van klanten te behouden en te voldoen aan de AVG, NIS2 en DORA.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle systemen en gebruikers binnen de organisatie, waaronder:

2.1.1 Werkstations, laptops, servers, firewalls, switches, routers en draadloze toegangspunten

2.1.2 Clouddiensten die worden gebruikt voor de bedrijfsvoering, zoals e-mail, bestandsopslag, back-ups en samenwerkingstools

2.1.3 Loggingfunctionaliteit in antivirussoftware, applicaties, besturingssystemen en netwerkapparatuur

2.1.4 Alle werknemers, contractanten en managed service providers (MSP's) die systemen gebruiken of beheren

2.1.5 Iedere locatie waar bedrijfs-IT-systemen worden gebruikt, waaronder omgevingen voor thuiswerken, hybride werken of Bring Your Own Device (BYOD)

2.2 Dit beleid is tevens van toepassing op loggegevens die door diensten van derden worden gegenereerd wanneer de organisatie beschikt over administratieve toegang of auditrechten.

3. Doelstellingen

3.1 Waarborgen dat systeemactiviteiten worden gelogd, waaronder authenticatie, configuratiewijzigingen, toegang tot gevoelige gegevens en beveiligingswaarschuwingen

3.2 Veilige en accurate loggegevens bijhouden om beleidsovertredingen, systeemfouten of ongeautoriseerde handelingen te detecteren

3.3 Tijdige beoordeling van loggegevens tijdens incidenten, onderzoeken en audits mogelijk maken

3.4 Tijdsynchronisatie ondersteunen om de integriteit en correlatie van loggegevens te waarborgen

3.5 Loggegevens beschermen tegen manipulatie, verlies of voortijdige verwijdering

3.6 Voldoen aan wettelijke en regelgevende verplichtingen inzake systeemverantwoordingsplicht, traceerbaarheid en respons op inbreuken

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 Keurt dit beleid goed en ziet toe op de implementatie ervan binnen alle bedrijfssystemen

4.1.2 Beoordeelt waarschuwingen met hoge ernst en ernstige auditbevindingen die door IT of privacyfuncties worden gerapporteerd

4.1.3 Verleent formele goedkeuring aan uitzonderingen wanneer logging of bewaring technisch niet kan worden afgedwongen

4.2 IT-supportdienstverlener / interne IT-functie

4.2.1 Implementeert en configureert logging voor besturingssystemen, netwerkapparatuur, antivirussoftware en kritieke applicaties

4.2.2 Zorgt ervoor dat loggegevens worden bewaard, in back-ups worden opgenomen en tegen wijziging worden beschermd

4.2.3 Beoordeelt loggegevens volgens planning en onderzoekt verdachte of ongeautoriseerde activiteiten

4.2.4 Beheert alerteringssystemen die afwijkend gedrag of indicatoren van compromittering signaleren

[... 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 actualisatie

9.1 Jaarlijkse herziening

9.1.1 Dit beleid moet ten minste jaarlijks worden herzien door de Algemeen directeur (GM), met ondersteuning van de IT-supportdienstverlener en de Privacycoördinator.

9.2 Aanleidingen voor herziening

9.2.1 Niet-geplande herzieningen moeten worden uitgevoerd naar aanleiding van:

9.2.1.1 Bevindingen met betrekking tot loggegevens uit interne of externe audits

9.2.1.2 Beveiligingsincidenten waarbij loggegevens ontbraken, corrupt waren of ontoereikend bleken

9.2.1.3 Materiële wijzigingen in de IT-infrastructuur, zoals migratie naar cloudgehoste loggingplatforms

9.2.1.4 Wijzigingen in wettelijke of regelgevende verplichtingen, zoals AVG, NIS2 en DORA

9.3 Versiebeheer

9.3.1 Alle wijzigingen in dit beleid moeten worden vastgelegd met versienummer, datum en samenvatting van de herzieningen

9.3.2 Eerdere versies moeten worden gearchiveerd en ten minste 3 jaar worden bewaard

9.3.3 Geactualiseerd beleid moet worden gecommuniceerd aan betrokken belanghebbenden, in het bijzonder aan personen met toegang op systeemniveau

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid ondersteunt rechtstreeks en wordt ondersteund door de volgende mkb-beleidslijnen voor informatiebeveiliging:

10.1.1 P17S – Beleid inzake gegevensbescherming en privacy: Waarborgt dat loggegevens die persoonsgegevens bevatten worden beheerd met passende waarborgen voor integriteit, bewaring en toegang, in lijn met de vereisten van de AVG.

10.1.2 P21S – Netwerkbeveiligingsbeleid: Biedt de basis voor het vastleggen van loggegevens met betrekking tot firewalls, draadloze toegang, VPN's en monitoring van segmentatie.

10.1.3 P24S – Beleid inzake veilige ontwikkeling: Waarborgt dat applicatielogs, bijvoorbeeld voor aanmeldpogingen, fouten en uitzonderingen, worden meegenomen in softwareontwerp en beheer.

10.1.4 P30S – Incidentresponsbeleid: Steunt op accurate en volledige loggegevens om informatiebeveiligingsgebeurtenissen te detecteren, analyseren en daarop te reageren.

10.1.5 P23S – Beleid inzake tijdsynchronisatie: Zorgt voor consistente en traceerbare tijdstempels in alle systemen, zodat loggegevens tijdens onderzoeken kunnen worden gecorreleerd.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 8.1 – Vereist de implementatie van operationele beheersmaatregelen om informatiebeveiligingsrisico's te beperken, waaronder logging.

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 8.15 – Vereist gebeurtenisregistratie ter ondersteuning van anomaliedetectie en verantwoordingsplicht.

11.2.2 Beheersmaatregel 8.16 – Vereist bescherming van loggegevens tegen manipulatie en ongeautoriseerde toegang.

11.2.3 Beheersmaatregel 8.17 – Vereist monitoring van systemen op ongebruikelijke activiteiten en bevestiging van de doeltreffendheid van monitoringmaatregelen.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 tot en met AU-12 – Omvatten de inhoud van auditlogs, beoordeling, bewaring en geautomatiseerde alertering.

11.3.2 SI-4 – Vereist detectie van systeemanomalieën en rapportage van verdachte gebeurtenissen.

11.4 AVG

11.4.1 Artikel 5(1)(f) – Vereist integriteit en vertrouwelijkheid van persoonsgegevens, waaronder logging van toegang.

11.4.2 Artikel 32 – Schrijft technische en organisatorische maatregelen voor om beveiliging te waarborgen, waaronder logging en monitoring.

11.4.3 Artikel 33 – Vereist tijdige melding van inbreuken, ondersteund door loggegevens die root cause analysis mogelijk maken.

11.5 NIS2-richtlijn

11.5.1 Artikel 21(2)(d) – Vereist loggingmechanismen die anomalieën detecteren en ondersteuning bieden tijdens incidentonderzoeken.

11.5.2 Artikel 23 – Schrijft melding van incidenten binnen 24 uur voor, afhankelijk van accurate en tijdige loggegevens.

11.6 DORA

11.6.1 Artikel 10 – Vereist digitale operationele weerbaarheid, waaronder traceerbaarheid van ICT-gerelateerde incidenten door middel van logging.

11.6.2 Artikel 15 – Verplicht monitoring van dienstverleners, waaronder rechten op toegang tot loggegevens en beoordeling daarvan.

11.7 COBIT 2019

11.7.1 DSS01.03 – Vereist traceerbaarheid van systeemactiviteiten door middel van logging en monitoring.

11.7.2 DSS05.02 – Behandelt logging als een essentiële beheersmaatregel ter bescherming tegen malware en andere ongeautoriseerde activiteiten.