|  |
| --- |
| Standaard Logging en MonitoringTemplate |

|  |  |
| --- | --- |
| Auteur(s): |  |
| Versie: |  |
| Datum: | Kies of typ een datum |
| Kenmerk: |  |
|  |  |
|  |  |

**Documentinformatie**

Dit document maakt onderdeel uit van een complete set (beleidspiramide) met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Dit document heeft betrekking op de laag Standaard in de beleidspiramide.



**Versiebeheer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Verwerking** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Distributielijst**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Ontvanger** | **Doel** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Vastgesteld door** | **Vastgesteld op** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Samenhang met andere documenten**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Bovenliggend** | **Gelijk niveau** | **Onderliggend** |
| [INFORMATIEBEVEILIGINGSBELEID] | x |  |  |
| [RICHTLIJN LOGGING EN MONITORING] |  |  | x |
|  |  |  |  |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | SM.01, SM.02, SM.03, SM.04, SM.05, SM.06, SM.07, SM.08, SM.09, SM.10, SM.11, SM.12, SM.13  |
| ISO27001:2022 | A5.1, A8.1, A8.15, A8.16, A8.17, A8.18, A9.4, A8.19, A8.20, A8.21, A8.22, A5.3, A5.4, A8.23, A8.24, A9.3 |

**Creative Commons**

Dit template is een product van het SURF Security Expertise Centrum en beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal. <https://creativecommons.org/licenses/by/4.0/deed.nl>

Inhoudsopgave

|  |
| --- |
| [Samenvatting 4](#_Toc191940270)[1 Inleiding 5](#_Toc191940271)[1.1 Doel 5](#_Toc191940272)[1.2 Toepassingsgebied en reikwijdte 5](#_Toc191940273)[2 Standaard Monitoring en Logging 6](#_Toc191940274)[2.1 Principes 6](#_Toc191940275)[2.2 Authenticatie en autorisatie 6](#_Toc191940276)[2.3 Loggegevens 6](#_Toc191940277)[2.4 Beveiliging en integriteit 7](#_Toc191940278)[2.5 Automatisering en SIEM 7](#_Toc191940279)[2.6 Real-time Monitoring vs. Periodieke Monitoring 8](#_Toc191940280)[2.7 Incident Respons en Escalatie 8](#_Toc191940281)[3 Taken en verantwoordelijkheden 10](#_Toc191940282)[3.1 Security Operations Center (SOC) 10](#_Toc191940283)[3.2 Privacy & Security Team 10](#_Toc191940284)[3.3 Computer Security Incident Response Team (CSIRT) 10](#_Toc191940285)[3.4 Beheer en Ondersteuning 10](#_Toc191940286)[3.5 Management 11](#_Toc191940287)[3.6 Medewerkers 11](#_Toc191940288)[4 Implementeren, borgen en evalueren 12](#_Toc191940289)[4.1 Implementatie 12](#_Toc191940290)[4.2 Borging 12](#_Toc191940291)[4.3 Evaluatie 13](#_Toc191940292)[5 Retentie, Compliance en Auditing 14](#_Toc191940293)[5.1 Bewaartermijnen en retentie 14](#_Toc191940294)[5.2 Periodieke evaluatie 15](#_Toc191940295)[5.3 Audit 15](#_Toc191940296)[6 Vaststelling 16](#_Toc191940297) |

Samenvatting

Hier komt een samenvatting, op zichzelf leesbaar, van de inhoud van dit document in max. 1 A4.

# Inleiding

Logging en monitoring zijn belangrijke onderdelen van ons Strategisch Informatiebeveiligings-beleid. Ze bieden inzicht in het functioneren van systemen en applicaties, ondersteunen bij de detectie van beveiligingsincidenten en helpen te voldoen aan wet- en regelgeving. Door loggegevens op een gestructureerde en veilige manier te verzamelen en te beheren, kunnen risico’s beter worden beheerst en kan de integriteit, beschikbaarheid en vertrouwelijkheid van informatie worden gewaarborgd.

## Doel

Deze standaard beschrijft de principes, eisen en kaders voor logging en monitoring binnen onze instelling en sluit aan bij het SURFaudit toetsingskader en de richtlijnen van ISO 27001:2022. Het doel is om een uniforme en effectieve werkwijze te waarborgen voor het vastleggen, beheren en beveiligen van loggegevens, zodat deze optimaal kunnen worden ingezet voor informatiebeveiliging, incidentdetectie en compliance.

## Toepassingsgebied en reikwijdte

De beschreven principes, eisen en kaders zijn van toepassing op alle ICT-systemen, netwerken en applicaties beheerd door of voor onze instelling en gelden voor medewerkers, studenten, externe partners en derden met toegang tot deze systemen.

# Standaard Logging en Monitoring

## Principes

Onze standaard voor logging en monitoring is gebaseerd op de volgende principes.

* **Controleerbaarheid**

Mechanismen voor logging moeten integriteit, beschikbaarheid en vertrouwelijkheid van loggegevens waarborgen.

* **Minimale gegevensvastlegging**

Alleen relevante gebeurtenissen worden gelogd, volgens privacyregelgeving en het proportionaliteitsbeginsel.

* **Beperkte toegang**

Loggegevens zijn uitsluitend toegankelijk voor geautoriseerd personeel, volgens het least privilege-principe. Voor toegang tot kritieke of gevoelige loggegevens is het vier-ogen principe geborgd.

* **Retentie en opschoning**

Loggegevens worden bewaard volgens wettelijke en organisatorische vereisten, waarbij periodieke opschoning en gecontroleerde verwijdering plaatsvindt.

* **Standaardisatie en compliance**

Logging- en monitoringsystemen moeten voldoen aan erkende best practices en normen, zoals ISO 27001:2022 en Algemene verordening gegevensbescherming (AVG).

## Authenticatie en autorisatie

Authenticatie en autorisatie voor toegang tot logging- en monitoringgegevens zijn ingericht volgens de standaarden Identiteit- en Toegangsbeheer en Gegevensbeheer (incl. classificatie). Toegangsrechten worden periodiek herzien, gelogd en gerapporteerd aan de CISO.

## Loggegevens

Logging is ingeregeld op alle relevante systemen, werkplekken en applicaties. Dit omvat o.a.:

* Gebruikersactiviteiten (aan- en afmeldingen, gebruik van autorisaties).
* Systeem- en applicatiegebeurtenissen (fouten, wijzigingen in configuraties).
* Netwerkactiviteiten (verbindingspogingen, firewall-logs).
* Toegangs- en wijzigingspogingen tot vertrouwelijke gegevens.

Kortom loggegevens moeten inzicht geven in: wat gebeurde er, waar, wanneer, waarom en wie waren hierbij betrokken. Een verdere uitwerking is opgenomen in de ‘Richtlijn Logging en Monitoring’.

Alle loggegevens die over een netwerk worden verzonden, moeten worden versleuteld conform de ‘Standaard Cryptografie’ om afluisteren en manipulatie te voorkomen. Dit geldt zowel voor interne als externe netwerken.

## Centralisatie van loggegevens

Alle loggegevens worden centraal opgeslagen in een beveiligd en beheerd logmanagementsysteem. Logging dient te worden vastgelegd in gestandaardiseerde formaten (zoals JSON, syslog of CEF) om uniformiteit, doorzoekbaarheid en analyse te ondersteunen.

Het centrale logplatform moet:

* Automatische verzameling en opslag van logs uit systemen, applicaties en netwerkcomponenten ondersteunen, inclusief IaaS, PaaS en SaaS-omgevingen.
* Gebruik maken van standaard logformaten om compatibiliteit met monitoring- en SIEM-oplossingen te garanderen.
* Toegangscontrole en integriteit bewaken om ongeautoriseerde wijziging of verwijdering van logs te voorkomen.

## Beveiliging en integriteit

**Bescherming tegen wijziging**

Loggegevens worden beveiligd tegen ongewenste toegang, aanpassingen of verwijdering. Hiervoor worden technieken zoals hashing en digitale handtekeningen toegepast, in lijn met de ‘Standaard Cryptografie’.

**Beschikbaarheid en opslag**

Loggegevens worden opgeslagen op beveiligde locaties met adequate opslagcapaciteit en redundant bewaard om gegevensverlies te voorkomen. Back-up- en herstelprocedures volgen de ‘Standaard Back-up en Herstel’.

**Tijdsynchronisatie**

Alle systemen die loggegevens genereren, gebruiken een gesynchroniseerde tijdsbron (NTP) om consistente tijdstempels te garanderen. Dit draagt bij aan een betrouwbare reconstructie van gebeurtenissen.

## Automatisering en SIEM

Het verwerken en analyseren van loggegevens gebeurt waar mogelijk geautomatiseerd om de efficiëntie en effectiviteit van monitoring en detectie te verhogen. Security Information en Event Management (SIEM) speelt hierin een centrale rol door loggegevens uit verschillende bronnen te verzamelen, te correleren en real-time analyses mogelijk te maken.

**Geautomatiseerde verwerking en detectie**

Door middel van automatisering worden loggegevens continu geanalyseerd op afwijkingen en potentiële beveiligingsincidenten. Dit minimaliseert de afhankelijkheid van handmatige controles en versnelt detectie en respons.

**Gebruik van SIEM**

Een SIEM-platform verzamelt loggegevens uit diverse systemen, applicaties en netwerken en stelt beveiligingsteams in staat om bedreigingen sneller te identificeren. Correlatieregels en gedragsanalyses helpen bij het herkennen van patronen en afwijkingen.

**Alerting en incidentrespons**

Het SIEM genereert meldingen bij verdachte activiteiten en ondersteunt geautomatiseerde responsacties waar mogelijk. Dit draagt bij aan een gestructureerde aanpak voor incidentbeheer en verkleint de reactietijd bij beveiligingsincidenten.

**Integratie met andere beveiligingsmaatregelen**

SIEM wordt geïntegreerd met andere beveiligingsoplossingen, zoals Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) en Endpoint Detection and Response (EDR), om een breder inzicht in dreigingen te krijgen en gecoördineerde maatregelen te faciliteren.

**Logbeheer en retentie**

De opslag en verwerking van loggegevens binnen een SIEM-oplossing volgen de geldende bewaartermijnen en beveiligingsrichtlijnen. Gevoelige gegevens worden geclassificeerd en beveiligd volgens het strategisch informatiebeveiligingsbeleid.

## Real-time Monitoring vs. Periodieke Monitoring

Onze instelling maakt gebruik van zowel real-time monitoring als periodieke monitoring om de beveiliging van informatie en systemen te waarborgen.

**Real-time Monitoring**

Real-time monitoring maakt gebruik van geautomatiseerde systemen zoals SIEM om loggegevens continu te analyseren en direct meldingen te genereren bij afwijkingen. Dit wordt toegepast voor kritieke systemen en gevoelige gegevens, waar snelle detectie en respons op beveiligingsincidenten noodzakelijk is.

**Periodieke Monitoring**

Niet alle systemen en processen vereisen real-time analyse. Periodieke monitoring, zoals handmatige logreviews en geautomatiseerde rapportages, wordt toegepast voor minder kritieke systemen of als aanvulling op real-time monitoring. Dit helpt trends en patronen te identificeren en biedt inzicht in mogelijke risico’s die niet direct als incident worden gedetecteerd.

## Incident Respons en Escalatie

Logging en monitoring spelen een belangrijke rol bij het detecteren, analyseren en ondersteunen van de afhandeling van beveiligingsincidenten. Loggegevens bieden inzicht in de aard, omvang en impact van een incident en ondersteunen een snelle en effectieve respons. De afhandeling van incidenten volgt onze standaard Incidentbeheer en onderliggende procedures.

**Detectie en signalering**

Logging- en monitoringmechanismen genereren meldingen bij afwijkingen die kunnen wijzen op een beveiligingsincident. Deze meldingen worden geanalyseerd en geclassificeerd om te bepalen of escalatie noodzakelijk is.

**Onderzoek en analyse**

Loggegevens worden gebruikt om de oorzaak en impact van een incident vast te stellen. Dit omvat het correleren van loginformatie uit verschillende bronnen om aanvalspatronen te identificeren en de mogelijke gevolgen in kaart te brengen.

**Escalatie en opvolging**

Incidenten worden afgehandeld volgens de procedures in de standaard Incidentbeheer. Afhankelijk van de ernst en impact kan escalatie nodig zijn naar gespecialiseerde teams of externe partijen.

**Forensisch onderzoek en rapportage**

Loggegevens vormen een cruciale bron voor forensische analyse na een incident. Ze ondersteunen de reconstructie van gebeurtenissen en leveren bewijs voor interne evaluaties en eventuele juridische stappen.

**Continue verbetering**

Gegevens uit incidentonderzoeken en analyses worden gebruikt om logging- en monitoringprocessen te verbeteren, bijvoorbeeld door het aanscherpen van detectieregels in SIEM-systemen of het aanpassen van de logretentie.

# Taken en verantwoordelijkheden

Dit hoofdstuk beschrijft de taken en verantwoordelijkheden met betrekking tot logging en monitoring binnen onze instelling. De verdeling van taken is afgestemd op bestaande beleidsdocumenten en standaarden, zoals het Strategisch Informatiebeveiligingsbeleid en de standaard Incidentbeheer.

## Security Operations Center (SOC)

Het Security Operations Center (SOC) is verantwoordelijk voor het operationeel beheer van logging- en monitoringactiviteiten. Indien uitbesteed aan een externe dienstverlener, blijft onze instelling verantwoordelijk voor regie en toezicht. De belangrijkste taken van het SOC omvatten:

* Continu toezicht op loggegevens en beveiligingsevenementen.
* Detecteren van afwijkingen en verdachte activiteiten door middel van geautomatiseerde systemen zoals SIEM.
* Escaleren en initiëren van incidentrespons bij geconstateerde beveiligingsincidenten.
* Samenwerken met het Computer Security Incident Response Team (CSIRT) bij de afhandeling van incidenten.

## Privacy & Security Team

Het Privacy & Security Team is verantwoordelijk voor de beleidsmatige en strategische aspecten van logging en monitoring. Dit team draagt zorg voor naleving van wet- en regelgeving en beveiligingsstandaarden, waaronder ISO 27001. Taken zijn onder andere:

* Ontwikkelen en actualiseren van deze ‘Standaard logging en monitoring’ (thema-beleid).
* Controleren van naleving door middel van audits en periodieke beoordelingen.
* Ondersteunen bij incidentonderzoek en forensische analyse in samenwerking met het SOC en CSIRT.

## Computer Security Incident Response Team (CSIRT)

Het CSIRT coördineert de afhandeling van beveiligingsincidenten en speelt een centrale rol bij het voorkomen van herhaling. De verantwoordelijkheden omvatten:

* Identificeren van beveiligingsincidenten, in samenwerking met het SOC en externe partijen zoals SURFcert.
* Coördineren van de afhandeling van beveiligingsincidenten binnen de instelling.
* Rapporteren van trends en incidenten aan het management en relevante autoriteiten.

## Beheer en Ondersteuning

IT-beheerteams spelen een sleutelrol in de implementatie en het onderhoud van logging- en monitoringmechanismen. Hun verantwoordelijkheden zijn onder andere:

* Configureren en beheren van logging- en monitoringtools op alle relevante systemen en applicaties.
* Waarborgen dat de juiste loggegevens worden vastgelegd volgens de standaarden.
* Ondersteunen bij technische problemen of aanpassingen in monitoringsystemen.
* Beheren van toegangsrechten tot logbestanden en monitoringtools volgens het least privilege-principe.

## Management

Het management is verantwoordelijk voor het waarborgen van voldoende middelen en ondersteuning voor logging en monitoring. Taken omvatten:

* Toewijzen van middelen voor de implementatie en het onderhoud van logging- en monitoringtools.
* Goedkeuren van beleidswijzigingen op basis van aanbevelingen van het Privacy & Security Team.
* Zorgen voor naleving van wettelijke verplichtingen en interne beleidsregels.

# Implementeren, borgen en evalueren

Een effectieve implementatie en handhaving van logging en monitoring vereist een gestructureerde aanpak. Dit hoofdstuk beschrijft hoe deze standaard binnen onze instelling wordt geïmplementeerd, geborgd en geëvalueerd.

## Implementatie

Om logging en monitoring effectief toe te passen, worden de volgende stappen doorlopen:

**Toewijzen van rollen en verantwoordelijkheden**

De taken en bevoegdheden binnen logging en monitoring worden belegd bij de relevante teams, zoals het Security Operations Center (SOC), CSIRT, IT-beheer, Privacy & Security Team en Management.

**Bewustwording en opleiding**

Medewerkers en beheerders worden getraind in het belang van logging en monitoring, het herkennen van beveiligingsincidenten en de juiste opvolging hiervan.

**Technische implementatie**

Logging- en monitoringsystemen, zoals SIEM-oplossingen, worden ingericht om loggegevens te verzamelen, te analyseren en afwijkingen te detecteren.

**Operationele procedures en werkinstructies**

Er worden richtlijnen opgesteld voor logbeheer, inclusief logformaten, bewaartermijnen, toegangsbeheer en beveiligingsmaatregelen. Deze sluiten aan bij de Standaarden voor Identiteit- en Toegangsbeheer, Cryptografie en Incidentbeheer.

**Risicobeoordeling en afstemming op dreigingen**

Mechanismen voor logging en monitoring worden periodiek beoordeeld op hun effectiviteit en afgestemd op actuele dreigingen en beveiligingseisen.

## Borging

De naleving en effectiviteit van logging en monitoring worden gewaarborgd door:

**Regelmatige monitoring en rapportage**

Dashboards en rapportages bieden inzicht in logactiviteiten en detecteren trends en afwijkingen.

**Audits en compliance-controles**

Jaarlijkse audits en compliance-checks, uitgevoerd door het Privacy & Security Team, beoordelen de naleving van interne richtlijnen en externe normen zoals ISO 27001 en het SURFaudit toetsingskader.

**Incidentmanagement en escalatie**

Geconstateerde afwijkingen of overtredingen worden opgevolgd volgens de procedures uit de Standaard Incidentbeheer.

**Handhaving en bijsturing**

Niet-naleving van de ‘Standaard logging en monitoring’ kan leiden tot escalatie naar het management en het doorvoeren van verbetermaatregelen.

## Evaluatie

Logging- en Monitoringprocessen worden periodiek geëvalueerd om de effectiviteit en compliance te waarborgen. Dit omvat:

* **Analyse van detectieresultaten en incidenten**

De effectiviteit van monitoring wordt beoordeeld op basis van gedetecteerde afwijkingen en de afhandeling van beveiligingsincidenten.

* **Beoordeling van compliance en normenkaders**

Loggingpraktijken worden getoetst aan relevante regelgeving en kaders, zoals het SURFaudit toetsingskader en ISO 27001.

* **Stakeholderfeedback en verbeterinitiatieven**

Inbreng van betrokken partijen, zoals SOC, IT-beheer en management, wordt gebruikt om verbeterpunten te identificeren.

* **Aanpassing en doorontwikkeling**

Op basis van evaluatieresultaten worden verbeteringen doorgevoerd in de implementatiestrategie, werkwijzen en technische oplossingen.

# Retentie, Compliance en Auditing

Het vastleggen en beheren van loggegevens moet voldoen aan geldende wet- en regelgeving en interne beleidskaders. Dit hoofdstuk beschrijft de bewaartermijnen, compliance-eisen en auditprocessen die van toepassing zijn op logging en monitoring binnen onze instelling.

## Bewaartermijnen en retentie

Loggegevens worden bewaard volgens vastgestelde bewaartermijnen en wettelijke verplichtingen. De standaard bewaartermijn voor logbestanden binnen de organisatie varieert van één dag tot één jaar, tenzij specifieke regelgeving anders vereist.

* **Transactielogs**
Worden bewaard totdat de juiste en volledige verwerking van (batch)transacties is vastgesteld of totdat de mogelijkheid om een roll-back uit te voeren is verstreken; maximaal één dag.
* **Technische logs**
Worden bewaard totdat is vastgesteld dat er zich geen verstoringen in het systeem hebben voorgedaan; maximaal één week.
* **Auditing en forensische logs**
Logging die relevant is voor auditdoeleinden en onderzoek naar oneigenlijk gebruik wordt maximaal één jaar bewaard. De noodzaak hiervan wordt onderbouwd in de use case administratie.
* **Systeemoptimalisatielogs**
Worden bewaard zolang nodig is om trends te analyseren en prestatieverbeteringen door te voeren.

Afwijkingen van de standaard retentieperioden zijn toegestaan indien noodzakelijk, bijvoorbeeld bij een lopend onderzoek. Dit moet worden onderbouwd met een risicoanalyse volgens het geldende risicomanagementbeleid.

## Periodieke evaluatie

De vastgelegde loggegevens en monitoringmechanismen worden periodiek beoordeeld door het Privacy & Security Team in samenwerking met de beheerteams. Dit moet aantoonbaar worden uitgevoerd om ervoor te zorgen dat:

* De juiste gegevens worden gelogd en beveiligd.
* Monitoringmethoden up-to-date blijven en aansluiten op actuele beveiligingsdreigingen.

De evaluatie omvat:

* **Beoordeling van monitoringtools**
Controleren of logging- en SIEM-systemen effectief functioneren en voldoen aan de eisen.
* **Aanpassing van detectiemechanismen**
Updaten van waarschuwingsdrempels, correlatieregels en escalatieprocedures.
* **Identificatie van nieuwe risico’s**
Analyseren van nieuwe dreigingen en beoordelen of aanvullende monitoring nodig is.

## Audit

Een gestructureerde audittrail is noodzakelijk om de betrouwbaarheid van logging te waarborgen en om incidentonderzoek en forensische analyse te ondersteunen.

* **Toegangsbeheer tot auditlogs**
Alleen geautoriseerd personeel heeft toegang tot auditlogs. Dit wordt beheerd volgens het least privilege-principe en onderliggende toegangsbeheerstandaarden.
* **Beveiliging en integriteit van logs**
Auditlogs worden beschermd tegen ongeoorloofde wijziging en worden versleuteld opgeslagen volgens de ‘Standaard voor Cryptografie’.
* **Forensisch onderzoek en incidentanalyse**
Loggegevens worden gebruikt voor reconstructie van gebeurtenissen bij incidenten. Procedures voor forensisch onderzoek volgen de richtlijnen uit de ‘Standaard Incidentbeheer’.

# Vaststelling

Deze standaard is aldus vastgesteld.

[Plaats], [Datum].

[NAAM]

[FUNCTIE].

[Na (her)vaststelling, ook de tabel op p.2 bijwerken]