Inhoud

Inhoudsopgave

1 Inleiding

De standaard technische logging IV is onderdeel van het beleidsdocument (informatie)beveiliging.

1.1 Scope

Dit document beschrijft de minimale eisen met betrekking tot technische en audit logging van beveiligingsgebeurtenissen[1]. Deze standaard is verplicht voor alle ICT-diensten die door de IV-organisatie geleverd worden met uitzondering van zelfbouw applicaties[2]. In scope zijn dus het netwerk, storage, servers, OS, middleware, runtime, systeemhulpmiddelen[3] en COTS applicaties waarvan de IV-organisatie eigenaar is.

1.2 Doelstelling

Het doel van deze standaard is duidelijke regels neer te leggen die in relatie tot logging nagekomen moeten worden binnen de IV-organisatie.

1.3 Doelgroep

Dit document is van belang voor eigenaren van infrastructurele componenten en systemen en de Security Officers.

1.4 Referentie

1.4.1 Relevante wet- en regelgeving

- Baseline Informatiebeveiliging Rijksdienst 2017
  - 9.4.4.2 Het gebruik van systeemhulpmiddelen wordt gelogd.
  - 12.4.1 Gebeurtenissen registreren.
  - 12.4.1.1 Eisen wat een logregel minimaal moet bevatten.
  - 12.4.1.2 Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
  - 12.4.1.3 De omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen.
  - 12.4.1.5 De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd.
  - 12.4.2 Beschermen van informatie in logbestanden.
  - 12.4.2.1 Er is een overzicht van logbestanden die worden gegenereerd.
  - 12.4.2.2 Ten behoeve van de loganalyse is op basis van risicoafweging de bewaarperiode van de logging bepaald.
  - 12.4.2.3 Er is een audit procedure die toetst op het ongewijzigd bestaan van logbestanden.
  - 12.4.2.4 Oneigenlijk wijzigen of verwijderen van loggegevens worden gemeld als beveiligingsincident.
  - 12.4.3 Logbestanden van beheerders en operators.
  - 12.4.4 Kloksynchronisatie.
  - 16.1.7.1 De bewaartermijn van gelogde incidentinformatie is minimaal drie jaar.
- Algemene Verordening Gegevensbescherming (AVG)
- IT Beleid Logging en Monitoring Financiën v. 0.92

1 Alle gebeurtenissen die kunnen leiden tot een inbreuk op de Integriteit, Vertrouwelijkheid en Beschikbaarheid van gegevens of de continuïteit van de dienstverlening in gevaar kan brengen.
2 Er komt een aparte standaard technische beveiligingslogging voor zelfbouw applicaties.
3 Systeemhulpmiddelen zijn middelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen.

1.4.2 Relevante documentatie

Aanwijzing Logging; Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO), Informatie beveiligingsdienst.

2 Normen m.b.t. logging

2.1 Gebeurtenissen die gelogd moeten worden

Alle systemen en applicaties moeten minimaal de volgende gebeurtenissen loggen:

1. **Authenticatie/autorisatie pogingen, inloggen en uitloggen:**
   1.1. Opvoeren en afvoeren van gebruikers
   1.2. Het toekennen en intrekken van rechten
   1.3. Wachtwoord reset
   1.4. Inloggen en uitloggen
2. **Acties die betrekking hebben op gebruikersprofielen, bestanden en databases of systeemservices:**
   2.1. Het toekennen en intrekken van rechten
   2.2. Wachtwoord reset
   2.3. Inloggen en uitloggen
3. **Transacties tussen systemen:**
   3.1. Hierbij wordt gelogd: het bericht-ID, datum en tijd, aanroepend en verzendend systeem en -proces.
4. **Activatie en/of de-activatie van beveiligingsfunctionaliteit:**
   4.1. Uitgifte en intrekken van cryptosleutels
5. **Niet gespecificeerd gedrag van systemen en applicaties (uitzonderingen, fouten en storingen):**
   5.1. het vollopen van queues;
   5.2. systeemfouten
   5.3. afbreken tijdens executie van programmatuur, systeem- en securityservices
   5.4. het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen
6. **Beveiligingsincidenten:**
   6.1. de aanwezigheid van malware
   6.2. testen op vulnerabilities
   6.3. foutieve inlogpogingen
   6.4. overschrijding van autorisatiebevoegdheden
   6.5. geweigerde pogingen om toegang te krijgen
   6.6. Indicatoren die kunnen bepalen of er een DdoS aanval gaande is.
   6.7. Malware/Spyware en andere ongewenste software (hieronder valt ook bittorrent software)
   6.8. Toevoegen van rogue accesspoints binnen de Belastingdienst infrastructuur
   6.9. Plaatsen van niet-geauthoriseerde apparatuur binnen de infrastructuur van de Belastingdienst, 802.1x meldingen
   6.10. Omzeilen van gemaakte beveiligingsmaatregelen, denk daarbij aan bijvoorbeeld SQL-injection aanvallen, Java Serialization attacks.

2.2 In het log op te nemen gegevens

Voor elke hierboven beschreven gebeurtenis moeten minimaal de volgende gegevens gelogd worden:

1. Datum en tijd
2. IP-adres of hostnaam van het device dat de informatie logt
3. IP-adres van het remote systeem (indien met een ander systeem wordt gecommuniceerd)
4. Identificatie van de gebruiker of het proces
5. Identificatie van het subject waarop de gebeurtenis betrekking heeft
6. Beschrijving van de activiteit of de gebeurtenis
7. Het resultaat van de activiteit of de gebeurtenis

Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden of de privacy kunnen schaden, zoals bijvoorbeeld wachtwoorden, BSN's, NAW-gegevens van Belastingplichtigen, Aangiftes.
Debug logs mogen dan ook niet in de centrale logomgeving worden opgenomen tenzij dit expliciet is ontworpen en toegestaan.

2.3 Gebeurtenissen die moeten leiden tot meldingen en alarmeringen

1. **De producteigenaar of de eigenaar van een systeem of applicatie moet:**
   1.1. definiëren en documenteren welke gebeurtenissen moeten leiden tot welk type alarmering.
   1.2. definiëren en documenteren met welke prioriteit op het alarm gereageerd dient te worden.

2. **Minimaal de volgende gebeurtenissen en/of activiteiten moeten leiden tot het genereren van een alarm:**
   2.1. Meerdere onsuccesvolle inlogpogingen binnen een vastgestelde tijdsduur;
   2.2. Aanpassing, vollopen of verwijderen van logbestanden;
   2.3. Het niet (meer) kunnen opslaan van gegenereerde logregels;
   2.4. Aanmaak van (beheerders) 'privileged' ID's of accounts;
   2.5. Het gebruik van 'privileged' ID's of accounts;
   2.6. Benaderen, aanpassen of verwijderen van, als zodanig aangemerkte, gevoelige of kritische middelen (bijvoorbeeld mappen, bestanden of programma's);
   2.7. Stoppen, starten of afbreken tijdens executie van securityservices
   2.8. Pogingen tot omzeilen van beveiligingsmaatregelen, denk hierbij aan bijvoorbeeld SQL-injection.

2.4 Logformat

1. Loggegevens worden als key-value pairs, JSON of XML aangeleverd aan de centrale logvoorziening.

2.5 Integriteit van logging op de centrale logvoorziening

1. Logging moet op een dusdanige wijze worden geïmplementeerd dat dit kan worden gebruikt als bewijs in juridische procedures. Een belangrijke voorwaarde hierbij is dat de gegevens rechtmatig zijn verkregen. De integriteit en beschikbaarheid moeten dan ook zeker worden gesteld en manipulatie van log gegevens moet voorkomen worden.

2.6 Verzamelen van loggegevens

1. Alle systemen en applicaties die logregels genereren moeten gebruik maken van de centrale tijdssynchronisatie service.
2. Logregels die aangemaakt worden moeten zo snel mogelijk (bij voorkeur binnen 5 minuten) na aanmaak van de logregel doorgestuurd zijn naar de enterprise logomgeving of de lokale logomgeving.
3. Er moeten maatregelen getroffen worden om verlies van loggegevens tegen te gaan in het geval de loggegevens niet verzonden kunnen worden naar de centrale logomgeving.
4. Eenmaal opgeslagen logregels mogen niet worden aangepast.

2.7 Centrale logging

1. Toegang tot loggegevens mag enkel plaatsvinden op basis van 'need to know'. Medewerkers mogen enkel die autorisaties hebben en die loggegevens inzien, die nodig zijn om hun werk te kunnen uitvoeren.
2. Binnen elke omgeving dient een centrale logserver aanwezig te zijn. Hieronder vallen expliciet ook OTA omgevingen.
3. Het moet mogelijk zijn om vanuit 1 beheersomgeving alle centrale logservers. raadplegen.
4. Tijdens opslag van loggegevens moet de integriteit geborgd zijn.

5. Indien de centrale (enterprise) log functionaliteit (nog) niet is geïmplementeerd dan is het gebruik van een lokale logomgeving binnen toegestaan als wordt voldaan aan de volgende voorwaarden:

   5.1. De lokale logomgeving moet bestaan uit een systeem waar de afzonderlijke logs van systemen en applicaties naar toe worden verzonden.
   5.2. De loggegevens moeten op een veilige manier vanaf de bron doorgestuurd worden naar de logfaciliteit zodat de loggegevens niet aangepast of gemanipuleerd kunnen worden.
   5.3. Er dient door de systeem- en/of applicatie eigenaar:

      5.3.1. Gemotiveerd te worden waarom geen aansluiting op de centrale logfaciliteit is of wordt gerealiseerd (Hiervoor dient gebruik te worden gemaakt van de Explain procedure);
      5.3.2. Gespecificeerd te worden op welke wijze de Beschikbaarheid, Integriteit en Vertrouwelijkheid van deze omgeving en de logbestanden gegarandeerd wordt. Deze maatregelen dienen opgenomen te worden in het risicoregister;
      5.3.3. Toestemming voor de uitzondering verkregen te worden door de portefeuillehouder Security & Continuity van de IV organisatie.

2.8 Automatische analyse van loggegevens en generatie van meldingen

1. Op de centrale logomgeving dienen (indien mogelijk) de meldingen en alarmeringen conform de eisen die zijn vastgesteld onder 2.3 (Gebeurtenissen die moeten leiden tot meldingen en alarmeringen) automatisch te worden gegenereerd. Opvolging van de gebeurtenissen (incidentresponse) moet in samenspraak met de product-, systeemeigenaar worden bepaald en dient gebruik te maken van de reeds hiervoor ingerichte procedures en processen..

2.9 Handmatige analyse van logbestanden en alarmering

1. De systeemeigenaar dient, in samenspraak met het SOC, gebeurtenissen te definiëren op basis waarvan use cases worden gedefinieerd welke leiden tot de juiste alarmering en afhandeling. (Incident response)
2. Indien geen gebruik gemaakt kan worden van de centrale log omgeving, dan moet de logging minimaal dagelijks geanalyseerd worden. De analyse dient uitgevoerd te worden op basis van de onder 2.3 (Gebeurtenissen die moeten leiden tot meldingen en alarmeringen) vastgestelde criteria.
3. De resultaten van deze analyse dienen gedocumenteerd te worden.

2.10 Uitvoeren van trendanalyses

1. Afdelingen die toezicht houden op logbestanden moeten de loggegevens maandelijks analyseren om na te gaan of nieuwe gebeurtenissen of patronen voorkomen die kunnen wijzen op incidenten waarop geacteerd dient te worden. Primair is deze verantwoordelijkheid belegd bij het SOC.
2. De resultaten van de analyse dienen besproken te worden met de eigenaar van de applicatie of het systeem waarop de bevindingen betrekking hebben.
3. Als er verdachte gebeurtenissen opgemerkt worden tijdens de analyse van de logging dan dienen deze in samenwerking met het SOC en de eigenaar van het systeem of de applicatie opgevolgd te worden, conform de daarvoor geldende procedures.
4. De eigenaar van de applicatie of het systeem dient, indien nodig, hier actie op te ondernemen. Het besluit omtrent de te ondernemen actie(s) dient vastgelegd te worden.
5. Indien er gebruik wordt gemaakt van een lokale logomgeving dan moeten deze analyses gedeeld worden met de afdeling die de analyse uitvoert voor de centrale logomgeving.

2.11 Bewaartermijn van loggegevens

Net als bij gegevens uit en bij de primaire processen geldt ook voor loggegevens dat de (proces)eigenaar de bevoegdheid heeft en de verantwoordelijkheid draagt voor de gegevens. Ook het bepalen van de bewaartermijn van loggegevens valt onder deze verantwoordelijkheid.

Voor loggegevens afkomstig uit technische logging en bedoeld voor gebruik in de context van beveiligingsincidenten, kunnen de termijnen uit onderstaande tabel als (voorlopige) richtlijn gelden. Deze termijnen sluiten aan bij ervaringen van zowel SOC als ADR.

De verantwoordelijkheid voor beveiliging is gekoppeld aan de (proces-) verantwoordelijkheid bij de primaire processen. De Directie IV draagt zorg voor de feitelijke handelingen, maar is niet zelfstandig bevoegd de aard van de gegevens-verwerking te bepalen. Afwijking van voorgestelde termijnen behoort dus in overleg met de juridisch bevoegde proceseigenaar plaats te vinden.

De bewaartermijnen voor loggegevens op de centrale logserver moeten voldoen aan onderstaande bewaartermijnen.

	Bewaartermijnen (in maanden)		
Type gegevens	richtlijn	SOC[5]	bij (vermoed) beveiligings-incident
Technische (beveiligings-) logregel bevat persoonsgegevens[4] die vallen onder de AVG.	6	Max.18	36
Technische (beveiligings-) logregel bevat géén persoonsgegevens[4] die onder de AVG vallen.	Min. 6 & Max.18	Max.18	36

De bewaartermijnen voor loggegevens op de bronsystemen moeten voldoen aan onderstaande bewaartermijnen.

	Bewaartermijnen (in dagen)
Type gegevens	
Technische (beveiligings-) logregel bevat persoonsgegevens[4] die vallen onder de AVG.	Max. 10
Technische (beveiligings-) logregel bevat géén persoonsgegevens[4] die onder de AVG vallen.	Max. 10

In Bijlage A is aanvullende informatie beschikbaar met betrekking tot bovenstaande bewaartermijnen.

2.12 Opslag van (forensische) loggegevens n.a.v. een beveiligingsincident

Bij een beveiligingsincident dienen de loggegevens geïsoleerd te worden en op een dusdanige wijze opgeslagen en behandeld te worden dat de integriteit van deze gegevens niet ter discussie kan worden gesteld.

De Security Officer zal in dit geval aanwijzingen geven hoe met deze gegevens om te gaan. Deze loggegevens kunnen bij een mogelijk strafrechtelijk feit als bewijsmateriaal worden aangemerkt waarbij andere bewaartermijnen en opslageisen gelden.

4 Persoonsgegevens: Informatie die direct over iemand gaat, ofwel naar deze persoon te herleiden is zoals o.a. NAW-gegevens of IP-adres/hostname van een device van een gebruiker.

5 Medewerkers die niet werkzaam zijn bij het SOC maar wel toegang moeten hebben tot deze technische beveiligingslogging van/voor het SOC, mogen enkel toegang hebben tot loggegevens die maximaal 6 maanden oud zijn.

2.13 BIO 1.04

Deze standaard voldoet aan de eisen die beschreven zijn in de BIO 1.04 op het vlak van logging. Detailinformatie is te vinden in Bijlage B.

3 Rollen en verantwoordelijkheden

De rollen en verantwoordelijkheden zijn beschreven over de as van de regulieren PDCA-cyclus:

3.1 Eigenaar van een dienst of product.

- Bepalen en vaststellen van rollen en bijbehorende rechten m.b.t. de toegang tot de gegenereerde logbestanden en logregels.
- Verantwoordelijk voor het laten implementeren van de maatregelen die benodigd zijn voor het voldoen aan de gestelde eisen.
- Verantwoordelijk voor het (laten) aansluiten van zijn of haar systemen en/of applicaties die nodig zijn om de dienst te laten functionerenop de enterprise logfaciliteit of lokale logomgeving.
- Door middel van de comply or explain procedure (Statement of Applicability) eventuele daartoe voor in aanmerking komende uitzonderingen te motiveren.
- Risico's die voortvloeien uit explains op te nemen in het risicoregister voor het product of de dienst.
- Dient het risicoregister en het Statement of Applicability up-to-date te houden.
- Dient de in het risicoregister opgenomen risico's te monitoren en, indien de risico's buiten de acceptabele grenzen vallen, hier actie op te ondernemen.
- Dient minimaal halfjaarlijks interne audits te laten uitvoeren die zijn gericht op het aantonen dat de vorm van de logbestanden ongewijzigd is.
- Informeren van de Security Officer over de bevindingen die voortkomen uit de uitgevoerde audits.
- verantwoordelijk voor het uit (laten) voeren van de analyse zoals beschreven in 2.10
- verantwoordelijk voor het delen van de resultaten van de analyse met het SOC
- Verantwoordelijk voor het ondernemen van (eventuele) acties die voortvloeien uit deze analyses.
- verantwoordelijk voor het opvolgen van verdachte gebeurtenissen conform de vastgestelde procedures

3.2 Beheerder van een systeem of applicatie

- Implementeren van de maatregelen die het resultaat zijn van de uitgevoerde risicoanalyse.
- Configuratie van de systemen of applicaties zodat de vastgestelde gebeurtenissen worden vastgelegd in de te genereren logs.
- Verantwoordelijk voor het op de juiste manier configureren van de logbestanden.
- Treffen van maatregelen om verlies van loggegevens tegen te gaan.
- De beheerder van de centrale (of lokale) logfaciliteit op de hoogte stellen indien het logformaat gewijzigd gaat worden.

3.3 Beheerder van de centrale logfaciliteit

Naast de verantwoordelijkheden die een beheerder van een systeem of applicatie heeft, heeft de beheerder van de centrale logfaciliteit een aantal aanvullende verantwoordelijkheden.

- Verantwoordelijk voor het inrichten van de centrale logfaciliteit conform de relevante normen zoals gesteld in hoofdstuk 2.
- Uitvoeren van de werkzaamheden die het gevolg zijn van de te implementeren vastgestelde maatregelen die voortvloeien uit de uitgevoerde risicoanalyse
- Verantwoordelijk voor het faciliteren van een veilig transportmechanisme waarmee loggegevens overgebracht kunnen.
- Monitoren van de beschikbaarheid van de lokale logomgeving
- Verantwoordelijk voor het bewaken van de benodigde opslagruimte die benodigd is voor de opslag van logbestanden.

- Verantwoordelijk voor het verwijderen van loggegevens na de door de product-diensteigenaar vastgestelde bewaartermijnen.

3.4 Beheerder van de lokale logomgeving

- Verantwoordelijk voor het inrichten van de lokale logfaciliteit conform de relevante normen zoals gesteld in hoofdstuk 2.
- Uitvoeren van de werkzaamheden die het gevolg zijn van de te implementeren vastgestelde maatregelen die voortvloeien uit de uitgevoerde risicoanalyse.
- Configuratie van de centrale logfaciliteit zodat de vastgestelde gebeurtenissen worden vastgelegd in de te genereren logs.
- Het geven van advies en ondersteuning aan beheerders van systemen en applicaties bij het configureren van de logbestanden.
- Verantwoordelijk voor het faciliteren van een veilig transportmechanisme waarmee loggegevens waarmee de loggegevens overgebracht kunnen.
- Ter beschikking stellen van de loggegevens aan de Security Officer of de producteigenaar indien zij daarom verzoeken.
- Monitoren van de beschikbaarheid van de lokale logomgeving
- Verantwoordelijk voor het bewaken van de benodigde opslagruimte die benodigd is voor de opslag van logbestanden.
- Verantwoordelijk voor het verwijderen van loggegevens na de vastgestelde bewaartermijnen.
- Verantwoordelijk voor het aanleveren van de benodigde loggegevens die benodigd zijn voor onderzoeken.
- Bewaken van de beschikbaarheid van de lokale logomgeving.

3.5 CTO Office team Security, Continuity & Privacy

- Adviseren over, en faciliteren van, de risicoanalyse en de privacy impact analyse.
- Adviseren met betrekking tot gedefinieerde explains.
- Beoordelen van de uitgevoerde audits.
- Adviseren over additionele activiteiten die gelogd moeten worden
- Geeft, in geval van een (vermoeden van) beveiligingsincident opdracht tot het veilig stellen van de benodigde loggegevens aan de beheerder van de logfaciliteit.
- Geeft opdracht tot vernietiging van de loggegevens indien deze niet meer bewaard hoeven te worden.

3.6 Security Operations Center

- Advisering over de wijze waarop de gegevens opgeslagen, aangeleverd en bewaard dienen te worden.
- Ondersteuning bieden bij het vaststellen van gebeurtenissen, te hanteren drempelwaarden en severity level.
- Analyseren van de gebeurtenissen die gelogd zijn op de centrale logomgeving.
- Ter beschikking stellen van de loggegevens aan de Security Officer of de producteigenaar indien zij daarom verzoeken in het kader van een onderzoek naar mogelijke inbreuken op de beveiliging.
- Rapporteren van trends aan eigenaren van systemen en applicaties
- Informeren van de Security Officer over trends
- Melden van verdachte gebeurtenissen aan de eigenaar van het systeem of applicatie
- Informeren van de Security Officer en de product-. Diensteigenaar over geconstateerde verdachte gebeurtenissen, waarbij gebruik gemaakt wordt van de hiervoor ingerichte beheersprocessen.
- Het SOC is de eigenaar van het proces Security Monitoring & Respons (SM&R). Op basis hiervan onderzoekt het SOC geconstateerde verdachte gebeurtenissen en betrekt daar waar nodig de product-, diensteigenaar en security officer hierbij.

3.7 Auditor

- Op verzoek van de producteigenaar uitvoeren van audits op de logging

Bijlage A: Toelichting bewaartermijnen

De technische beveiligingslogging bevat persoonsgegevens*
*Gegevens die vallen onder de AVG (persoonsgegevens) moeten 6 maanden bewaard worden (en niet langer). Een uitzondering hierop vormt de technische beveiligingslogging die door het SOC primair gebruikt wordt voor de bestrijding van misbruik en oneigenlijk gebruik **. Deze logging mag maximaal 18 maanden bewaard worden (en niet langer).* In de voor de rijksoverheid verplichte BIO (12.4.1) wordt verwezen naar een handreiking*** voor het gebruik van logging door organisaties binnen de Rijksoverheid. In deze handreiking is te lezen dat logging minimaal een half jaar beschikbaar moet zijn voor onderzoek. In het Vrijstellingsbesluit WBP wordt gesproken over een maximale bewaartermijn van logging van internetgebruik en het netwerk van 6 maanden. Deze eis is inmiddels komen te vervallen als gevolg van de komst van de AVG; deze waardes kunnen echter nog steeds als referentie gebruikt worden. Op basis van bovenstaande gaan we uit van een bewaartermijn van logging met persoonsgegevens van 6 maanden. De IV organisatie "verwerkt geen persoonsgegevens" op basis van eigen verwerkings-verantwoordelijkheid, maar steeds in opdracht van (en onder (verwerkings)-verantwoordelijkheid van) de uitvoering. Het is aan de opdrachtgever om de PIA te laten opstellen met betreffende bewaartermijnen.
Het Security Operations Center (SOC) maakt als proceseigenaar gebruik van logging voor de bestrijding van misbruik. Hiervoor is het noodzakelijk dat de logging 18 maanden beschikbaar is. Door gebruik te maken van logging over 18 maanden beschikt men over gegevens van twee aangiftecampagnes die men met elkaar kan vergelijken. Er is een PIA 'SOC Security Monitoring' beschikbaar.
* Persoonsgegevens: Informatie die direct over iemand gaat, ofwel naar deze persoon te herleiden is zoals o.a. NAW-gegevens of IP-adres/hostname van een device van een gebruiker.
** Medewerkers die niet werkzaam zijn bij het SOC maar wel toegang moeten hebben tot deze technische beveiligingslogging van/voor het SOC, mogen enkel toegang hebben tot loggegevens die maximaal 6 maanden oud zijn.
*** Handreiking: https://www.cip-overheid.nl/category/producten/handreikingen/

De technische beveiligingslogging bevat geen persoonsgegevens
Gegevens die niet vallen onder de AVG moeten minimaal 6 maanden bewaard worden en maximaal 18 maanden.
In de voor de rijksoverheid verplichte BIO (12.4.1) wordt verwezen naar een handreiking* voor het gebruik van logging door organisaties binnen de Rijksoverheid. In deze handreiking is te lezen dat logging minimaal een half jaar beschikbaar moet zijn voor onderzoek en maximaal twee jaar (uitgaande van het standaard niveau van de BIO te weten BBN2).
Binnen DCS wordt momenteel voor het centrale logsysteem een standaard bewaartermijn van 18 maanden gehanteerd. Door gebruik te maken van 18 maanden beschikt men over gegevens van twee aangiftecampagnes die men met elkaar kan vergelijken. Voor de meeste eigenaren van de logging is een langere periode ook niet nodig. Daarom gaan we uit van een bewaartermijn van minimaal 6 maanden en maximaal 18 maanden.
* Handreiking: https://www.cip-overheid.nl/category/producten/handreikingen/

(vermoed) beveiligingsincident
Indien er sprake is van een (vermoed) beveiligingsincident dan is de bewaartermijn van de gelogde incidentinformatie drie jaar.
Bovenstaande is afkomstig uit de BIO (hoofdstuk 16.1.7.1)

Bronsystemen
Logging op bronsystemen die in scope zijn van dit document mogen maximaal 10 dagen bewaard worden.
Logging op bronsystemen moet minimaal een week bewaard worden op de bronsystemen om er zeker van te zijn dat deze (binnen die tijdspanne) beschikbaar zijn op het centrale logsysteem. De logging op de bronsystemen wordt regelmatig gebruikt in het kader van incident management. De

logging moet vergeleken kunnen worden met de logging van een week oud. Op basis van bovenstaande gaan we uit van een bewaartermijn van maximaal 10 dagen op de bronsystemen.

Bijlage B: BIO-eisen m.b.t. logging

In onderstaand overzicht wordt aangegeven in welke paragraaf van dit document de control met betrekking tot de BIO 1.04 beschreven is:

Controlnr.	Control tekst	Hoofdstuk
9.4.4.2	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	1.1 & 2.12
12.4.1	Gebeurtenissen registreren. Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	2.1, 2.2, 2.7
12.4.1.1	Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis	2.2
12.4.1.2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	2.2
12.4.1.3	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectievoorzieningen, zoals het Nationaal Detectie Netwerk, die worden ingezet op basis van een risico-inschatting, mede aan de hand van en de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	2.10
12.4.1.5	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	2.9
12.4.2	Beschermen van informatie in logbestanden Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	2.7
12.4.2.1	Er is een overzicht van logbestanden die worden gegenereerd.	3.1
12.4.2.2	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	2.12
12.4.2.3	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	3.1
12.4.2.4	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via	2.3

	de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16 van de Baseline Informatiebeveiliging Overheid (BIO).	
12.4.3	Logbestanden van beheerders en operators Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.	2.1, 2.7, 2.9
12.4.4	Kloksynchronisatie De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	2.6
16.1.7.1	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van gelogde incidentinformatie minimaal 3 jaar.	2.12