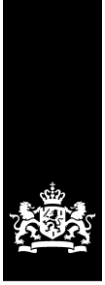

Justitiële Informatiedienst
Ministerie van Justitie en Veiligheid

Dienstenbeschrijving Valideringsdienst

Justitiële Informatiedienst

Versie 1.3

Datum	14 februari 2017
Status	Definitief

Colofon

Afzendgegevens	**Justitiële Informatiedienst**
	Egbert Gorterstraat 6 7607 GB Almelo Postbus 337 7600 AH Almelo www.justid.nl
Contactpersoon	Justitiële Informatienst
	T 088 99 89000 info@justid.nl
Auteurs	Justitiële Informatiedienst

Inhoud

Documentbeheer

Versie	Datum	Wijziging
1.2	23-01-2017	Definitieve versie
1.3	14-02-2018	Naamsverandering J&V doorgevoerd en document geactualiseerd

Inleiding

De Justitiële Informatiedienst is opgericht in 2006. De dienst is onderdeel van het Ministerie van Veiligheid en Justitie. Onder de diensten die Justid levert valt ook de Valideringsdienst, de validatie van elektronisch ondertekende of elektronisch verzegelde data zoals PDF documenten. Met deze Valideringsdienst kan de integriteit en authenticiteit worden aangetoond van de elektronisch ondertekende of elektronisch verzegelde data. Voorbeelden hiervan zijn documenten van de Rechtspraak die in elektronische vorm beschikbaar worden gesteld.

Deze Dienstenbeschrijving beschrijft de practices die door de Justitiële Informatiedienst worden gevolgd voor de Valideringsdienst. Het verschaft vertrouwen aan de Afnemers en Derden die gebruik maken van de dienstverlening.

Deze Dienstenbeschrijving beschrijft niet waaraan Afnemers of Derden moeten voldoen om gebruik te kunnen maken van de Valideringsdienst.

Deze Dienstenbeschrijving kan op elk gewenst moment worden aangepast, in lijn met de Nederlandse wetgeving, Europese regelgeving en internationale standaarden.

Voor het beschrijven van de criteria waaraan de Justitiële Informatiedienst moet voldoen, gaat zij uit van de normatieve referenties zoals deze zijn opgenomen in hoofdstuk 2.

1 Regelgeving

Deze Dienstenbeschrijving Valideringsdienst van de Justitiële Informatiedienst beschrijft de processen, procedures en maatregelen waaronder de Justitiële Informatiedienst de Valideringsdienst aanbiedt. Voor het beschrijven van de criteria hanteert de Justitiële Informatiedienst de kaders zoals deze zijn vastgelegd in de normatieve en informatieve referenties.

2 Referenties

2.1 Normatieve referenties

ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures".

[ISO27001] ISO/IEC 27001: "Information technology - Security techniques - Information security management systems - Requirements".

[BIR] Baseline Informatiebeveiliging Rijksoverheid.

2.2 Informatieve Referenties

[eIDAS] Regulation (EU) No 910/2014 of European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

3 Definities en afkortingen

3.1 Definities

Begrip	Definitie
Authenticatie	Een elektronisch proces dat de bevestiging mogelijk maakt of een persoon of organisatie daadwerkelijk is wie hij of zij beweert te zijn. Dat wil zeggen: daadwerkelijk de identiteit bezit die hij of zij opgeeft.
Authenticatiemiddel	Een middel dat persoonsidentificatiegegevens bevat en dat gebruikt wordt voor authenticatie bij een onlinedienst. Het authenticatiemiddel kan verschillende verschijningsvormen hebben, bijvoorbeeld een combinatie van gebruikersnaam en wachtwoord of een in software, op een smartcard of in andere specifieke hardware opgeslagen certificaat.
Associatie	De bundeling tussen enerzijds de verklaringen (authenticatie en attributie) en anderzijds het document of bewijsrecord.
Afnemers	Overheidspartijen die gebruik maken van de Valideringsdienst van de Justitiële Informatiedienst om derden (burgers, bedrijven, etc.) de mogelijkheid te geven elektronische data, zoals een PDF document, te valideren.
Derden	Personen die op eigen titel of als vertegenwoordiger van een (overheids)organisatie elektronische data, zoals een PDF document, ter validatie aanbieden aan de Valideringsdienst van Justitiële Informatiedienst.
Elektronische handtekening	Een handtekening die bestaat uit elektronische gegevens die gehecht zijn aan of logisch verbonden zijn met andere elektronische gegevens en die worden gebruikt door de ondertekenaar om te ondertekenen.
Persoonsidentificatiegegevens	Een reeks gegevens aan de hand waarvan de identiteit van een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, kan worden vastgesteld.
Bewijsrecords	De basisfunctie van bewijsrecords is het kunnen aantonen dat objecten (bijv. documenten) en de metagegevens door de tijd hun authenticiteit en integriteit behouden. Dit wordt gedaan door het

	documenteren van het aanmaken van het object en de metagegevens, evenals alle belangrijke activiteiten die daarna hebben plaatsgevonden ten aanzien van de entiteit of de metagegevens en onder wiens verantwoordelijkheid dat heeft plaatsgevonden.
Valideren	Valideren is het proces waarbij de integriteit en authenticiteit van elektronische data, zoals een PDF document, wordt gecontroleerd en indien aanwezig de geldigheid van een elektronische handtekening.
Dienstenbeschrijving	De beschrijving van de wijze waarop een Vertrouwensdienst de betrouwbare diensten aanbiedt.
Vertrouwensdienst	Een aanbieder van een of meer betrouwbare elektronische diensten.

3.2 Afkortingen

Afkorting	Beschrijving
ETSI	European Telecommunications Standards Institute
PDF	Portable Document Format
EBV	Elektronisch Berichtenverkeer
BIR	Baseline Informatiebeveiliging Rijksdienst

4 Algemene concepten

4.1 Vertrouwensdienst

De Valideringsdienst wordt aangemerkt als een Vertrouwensdienst. Als een zodanige dienst biedt de Justitiële Informatiedienst de mogelijkheid om elektronische data, zoals een PDF, te kunnen valideren. Hierdoor ontstaat extra zekerheid omtrent de integriteit (is de inhoud niet onbevoegd gewijzigd na het definitief worden) en authenticiteit (is het echt afkomstig van de organisatie die vermeld staat) van de elektronische data.

De Vertrouwensdienst zegt nadrukkelijk niets over de correctheid van de inhoud van elektronische data. Zo kan van bijvoorbeeld een PDF door de Valideringsdienst worden vastgesteld dat deze gewijzigd is na het definitief worden (controle op integriteit) maar niet wat er gewijzigd is.

4.2 Dienstenbeschrijving Valideringsdienst

In deze Dienstenbeschrijving staat beschreven welke processen, procedures en maatregelen Justitiële Informatiedienst hanteert om de Valideringsdienst, aan te bieden.
Deze Dienstenbeschrijving en eventuele aanvullende documenten zijn beschikbaar op https://validatie.justid.nl.

4.3 Beheer Dienstenbeschrijving Valideringsdienst

4.3.1 Organisatie verantwoordelijk voor het beheer van dit document

De verantwoordelijkheid voor het beheer van dit document ligt bij:

Justitiële Informatiedienst
Afdeling EBV
Egbert Gorterstraat 6
7606 GB Almelo

Postbus 337
7600 AH Almelo

Voor informatie en/of ondersteuning kan contact worden opgenomen via email: info@justid.nl of telefonisch met de Frontoffice van de Justitiële Informatiedienst onder nummer: 088 99 89 000.

4.3.2 Klachtenregeling

De Justitiële Informatiedienst heeft een eigen klachtenregeling. Deze regeling schrijft voor wat de Justitiële Informatiedienst moet doen als iemand een schriftelijke klacht heeft ingediend. Zie voor meer informatie: www.justid.nl.

4.3.3 Contactpersoon

De manager EBV van de Justitiële Informatiedienst is de contactpersoon. Zie hierboven bij paragraaf 4.3.1 voor contactgegevens. Het is de verantwoordelijkheid van de manager EBV voorgenomen wijzigingen in de dienstenbeschrijving te bespreken met de aangesloten Afnemers en na goedkeuring van de Dienstenbeschrijving (zie 4.3.4) opdracht geven de nieuwe versie van de Dienstenbeschrijving per direct op het portaal van de Valideringsdienst ter beschikking te stellen.

4.3.4 Goedkeuringsprocedures

Goedkeuring van de Dienstenbeschrijving vindt plaats in de Management Review waarbij de directeur Technologie en de manager EBV van de Justitiële Informatiedienst aanwezig zijn.

5 Verplichtingen en aansprakelijkheid

5.1 Verplichtingen

5.1.1 Algemeen

De Valideringsdienst die de Justitiële Informatiedienst als Vertrouwensdienst aanbiedt voldoet aan de processen, procedures en maatregelen zoals deze zijn opgenomen in deze Dienstenbeschrijving.

De Justitiële Informatiedienst zorgt ervoor dat alle processen, procedures en maatregelen zoals opgenomen in deze Dienstenbeschrijving zijn geïmplementeerd en dat hier blijvend aan wordt voldaan.

Het budget voor de dienstverlening worden aan Justid jaarlijks ter beschikking gesteld op basis van een jaarplan dat door Justid wordt opgesteld. De Nederlandse Overheid kent geen verzekeringen tegen aansprakelijkheid.

5.1.2 Verplichtingen t.o.v. Afnemers

Voordat Afnemers gebruik kunnen maken van de Valideringsdienst, moeten Afnemers voldoen aan bepaalde randvoorwaarden. Deze randvoorwaarden zijn opgenomen in de Dienstenniveau Overeenkomst tussen de Afnemer en de Justitiële Informatiedienst en wordt ondertekend door de Afnemer en de Justitiële Informatiedienst.

Deze Dienstenbeschrijving maakt integraal onderdeel uit van deze Dienstenniveau Overeenkomst.

De Justitiële Informatiedienst zal:

- De Dienstenbeschrijving Valideringsdienst beschikbaar stellen via een publiek toegankelijk datacommunicatie netwerk;
- De aansluitvoorwaarden ter beschikking stellen aan Afnemers;
- De informatie die haar ter beschikking wordt gesteld door een Afnemer om deze aan te kunnen sluiten vertrouwelijk behandelen en niet voor andere doeleinden gebruiken dan voor het doel waarvoor de informatie ter beschikking is gesteld;
- Alle informatie m.b.t. de Valideringsdienst bewaren totdat de Valideringsdienst wordt beëindigd;
- Geen informatie opslaan over derden die een document ter validatie aanbieden;
- Jaarlijks een audit laten uitvoeren door een daartoe geaccrediteerde organisatie om aan te tonen dat voldaan wordt aan de eisen die worden gesteld aan Vertrouwensdiensten.

5.2 Afnemers verplichtingen

Deze zijn opgenomen in de Dienstenniveau Overeenkomst tussen de Afnemer en de Justitiële Informatiedienst.

5.3 Verplichtingen Derden

Niet van toepassing.

5.4 Informatie voor derden

5.4.1 Aansprakelijkheid Justitiële Informatiedienst

De Justitiële Informatiedienst:

- Is aansprakelijk voor het nakomen van de verplichtingen zoals opgenomen in paragraaf 5.1. met inachtneming van geldende Nederlandse wet- en regelgeving dienaangaande;
- Heeft aanvullende voorzieningen getroffen die mogelijke schade kunnen compenseren die ontstaan is uit het niet nakomen van de verplichtingen zoals opgenomen in paragraaf 5.1.

De Justitiële Informatiedienst is niet aansprakelijk voor:

- Mogelijk misbruik van bewijsrecords, foutieve interpretatie door derden van de resultaten van een validatie of enige consequentie die het gevolg is van fouten of omissies in de Valideringsdienst;
- Het niet nakomen van de verplichtingen als dit wordt veroorzaakt door fouten die buiten de invloedsfeer van de Justitiële Informatiedienst liggen;
- Het niet nakomen van de verplichtingen als er sprake is van overmacht.

5.4.2 Naleving, geschilbeslechting en geschiloplossing

Alle geschillen in verband met deze Dienstenbeschrijving of met afspraken die daarmee samenhangen, worden in eerste instantie beslecht door interne escalatie bij de interne directie op achtereenvolgens operationeel-, tactisch- en strategisch niveau en dan via de bestuurlijke lijn naar het bestuursdepartement van Veiligheid en Justitie. Als uiterste middel kan worden gekozen voor arbitrage, mediation of bindend advies.

5.4.3 Publicatie van informatie

Alle informatie die rechtstreeks gerelateerd is aan het verlenen van de Valideringsdienst is beschikbaar in het publieke domein op https://validatie.justid.nl.

Tenminste de volgende informatie wordt beschikbaar gesteld:

- Dienstenbeschrijving Valideringsdienst.

De ingangsdatum van de nieuwe versie kan niet eerder zijn dan 30 dagen na publicatie.

5.4.4 Compliance Audit

Het informatiesysteem, de standaarden en richtlijnen, facilitaire voorzieningen, het personeel en andere items die nodig zijn om de Valideringsdienst als vertrouwensdienst te kunnen aanbieden worden ge-audit. Hierbij worden de volgende richtlijnen gehanteerd:

- Het informatiesysteem, de standaarden en richtlijnen, facilitaire voorzieningen, het personeel en andere items die nodig zijn om de Valideringsdienst als vertrouwensdienst te kunnen aanbieden worden jaarlijks, of wanneer een omvangrijke wijziging in de dienstverlening plaatsvindt, ge-audit overeenkomstig het vastgestelde normenkader en de bijbehorende regelgeving.
- Alle aanvullingen of afwijkingen van het normkader worden vastgelegd.
- De externe auditor moet geregistreerd staan bij de Nederlandse Raad voor Accreditatie voor de norm ETSI 319 401.
- De auditor is volledig onafhankelijk en op geen enkele manier verbonden met de partij die ge-audit wordt.
- Jaarlijks wordt door de Justitiële Informatiedienst zelf een interne audit uitgevoerd.

- De externe en interne auditor auditen ook de onderdelen van het informatiesysteem, de standaarden en richtlijnen, facilitaire voorzieningen, het personeel en andere items die nodig zijn om de Valideringsdienst als vertrouwensdienst te kunnen aanbieden voor zover dit is uitbesteed aan onderaannemers.
- Als gebreken en non-conformiteiten worden ontdekt door de auditor, worden correctieve maatregelen genomen door de Justitiële Informatiedienst. De correctieve maatregelen worden geverifieerd in de opvolgende audit.

5.4.5 Geheimhouding

5.4.5.1 Vertrouwelijke informatie
Alle informatie die de Justitiële Informatiedienst in haar bezit krijgt als gevolg van het aanbieden van de Valideringsdienst, wordt beschouwd als vertrouwelijke informatie. Het gebruik van deze informatie mag uitsluitend na schriftelijke toestemming van de rechtmatige eigenaar van deze vertrouwelijke informatie of na een gerechtelijk bevel.

5.4.5.2 Publieke informatie
Onder publieke informatie wordt verstaan de informatie die de Justitiële Informatiedienst verzamelt om de Valideringsdienst operationeel te houden of voor statistische doeleinden en de informatie zoals beschreven bij onderdeel 5.4.3.

6 Dienstenbeschrijving werking

6.1 Diensten Management en Operatie

6.1.1 Informatiebeveiliging

Met betrekking tot informatiebeveiliging hanteert de Justitiële Informatiedienst de geldende standaarden zoals de Baseline Informatiebeveiliging Rijksdienst.

Er is beleid voor informatiebeveiliging binnen Justitiële Informatiedienst vastgesteld, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten.

Alle medewerkers van de organisatie worden regelmatig attent gemaakt op het beveiligingsbeleid en de beveiligingsprocedures van de organisatie, voor zover relevant voor hun functie.

Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld.

Van softwarematige voorzieningen van de technische infrastructuur kan gecontroleerd worden of de laatste updates (patches) zijn doorgevoerd. Het doorvoeren van een wijziging vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de leverancier.

Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).

Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches worden ingepland bij de eerst volgende onderhoudsronde.

6.1.2 Bedrijfsmiddelen en informatieobjecten

Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit is een verantwoordelijke lijnmanager benoemd.

Er zijn regels voor acceptabel gebruik van bedrijfsmiddelen (vooral internet, e-mail en mobiele apparatuur). Het ARAR verplicht ambtenaren zich hieraan te houden. Voor extern personeel is dit in het contract vastgelegd. Zie ook 'Uitgangspunten online communicatie rijksambtenaren' (Ministerie van Algemene Zaken, 2010).

Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen. De toestemming kan generiek geregeld worden in het kader van de functieafspraken tussen manager en medewerker.

6.1.3 Personele beveiliging

De Justitiële Informatiedienst draagt er zorg voor dat alle interne medewerkers en ingehuurd personeel over de juiste kennis, expertise en opleidingsniveau beschikken dat noodzakelijk is voor het uitoefenen van hun functie. Voor alle functies is een functiebeschrijving opgesteld.

Alle Justitiële Informatiedienst medewerkers en ingehuurde medewerkers krijgen bij hun aanstelling hun verantwoordelijkheden ten aanzien van informatiebeveiliging ter inzage. De schriftelijk vastgestelde en voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging, die zij bij de vervulling van hun dienst hebben na te leven, worden op een gemakkelijk toegankelijke plaats ter inzage gelegd. Overeenkomstige voorschriften maken deel uit van de contracten met externe partijen. Ook voor hen geldt de toegankelijkheid van geldende regelingen en instructies.

Voor alle medewerkers van Justitiële Informatiedienst (eigen en ingehuurd personeel) geldt dat zij voordat zij hun dienstverband kunnen aanvangen een Verklaring Omtrent het Gedrag (VOG) moeten overleggen. De te onderzoeken antecedenten verschillen per functie en worden door Justitiële Informatiedienst bepaald. Ingehuurd personeel ondertekend voor aanvang van de werkzaamheden een geheimhoudingsverklaring; voor eigen personeel is de geheimhouding onderdeel van het afleggen van de eed/belofte bij aanstelling.

6.1.4 Fysieke en omgevingsbeveiliging

Er zijn toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) aangebracht om ruimten te beschermen waar zich informatie en ICT-voorzieningen bevinden.

Beveiligde zones zijn beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.

Er is fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten toegepast.

Medewerkers die zelf niet geautoriseerd zijn mogen alleen onder begeleiding van bevoegd personeel en als er een duidelijke noodzaak voor is toegang krijgen tot fysiek beveiligde ruimten waarin IT voorzieningen zijn geplaatst of waarin met vertrouwelijke informatie wordt gewerkt.

Medewerkers zijn geïnstrueerd om zodanig om te gaan met mobiele apparatuur en verwijderbare media dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt. Hierbij wordt o.a. aandacht besteed aan het risico van adreslijsten en opgeslagen boodschappen in mobiele telefoons.

6.1.5 Operations Management

De Justitiële Informatiedienst zorgt ervoor dat alle componenten van de Valideringsdienst veilig, correct en tegen een aanvaardbaar risico worden beheerd.

Bij de uitbesteding van het beheer van componenten aan externe partijen is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd.

De componenten van de Valideringsdienst worden beheerd volgens vastgestelde wijzigingsprocedures. Deze procedures houden o.a. in dat iedere wijziging wordt getest in afgeschermde omgeving alvorens deze wordt aangeboden voor acceptatietest om vervolgens in productie te worden genomen.

Alle kritische softwarecomponenten worden uitsluitend geïnstalleerd en van de benodigde updates voorzien vanaf betrouwbare bronnen. Er zijn interne procedures

die er voor zorgen dat de kritische softwarecomponenten beschermd zijn tegen virussen, onbetrouwbare en niet geautoriseerde software.

Serverruimtes, datacenters en daar aan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende best practices. Een goed voorbeeld van zo'n best practice is Telecommunication Infrastructure Standard for Data Centers (TIA-942).

Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de beheersorganisatie van de Justitiële Informatiedienst ingeleverd. De beheerorganisatie zorgt voor een verantwoorde afvoer zodat er geen data op het apparaat aanwezig of toegankelijk is. Als dit niet kan wordt het apparaat of de informatiedrager fysiek vernietigd. Het afvoeren of vernietigen wordt per bedrijfseenheid geregistreerd.

Niemand in de organisatie heeft op uitvoerend niveau rechten om een gehele cyclus van handelingen in een kritisch informatiesysteem te beheersen. Dit in verband met het risico dat hij of zij zichzelf of anderen onrechtmatig bevoordeelt of de organisatie schade toe brengt. Dit geldt voor zowel informatieverwerking als beheeracties.

6.1.6 System Access Management

Apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier. Dit geldt minimaal voor temperatuur en luchtvochtigheid, aarding, spanningsstabiliteit en overspanningsbeveiliging.

Reserve apparatuur en back-ups zijn op een zodanige afstand ondergebracht dat één en dezelfde calamiteit er niet voor kan zorgen dat zowel de hoofdlocatie als de back-up/reserve locatie niet meer toegankelijk zijn.

Er zijn minimaal logisch gescheiden systemen voor Ontwikkeling, Test, Acceptatie en Productie (OTAP). De systemen en applicaties in deze zones beïnvloeden systemen en applicaties in andere zones niet.

De uitwisseling van alle data op de Acceptatie- en Productieomgeving voor de Valideringsdienst op het netwerk van Justitiële Informatiedienst en met externe netwerken is versleuteld. Voor de encryptie wordt gebruik gemaakt van TLS certificaten die zijn uitgegeven onder PKIoverheid.

Taken en verantwoordelijkheidsgebieden zijn gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

Er zijn formele procedures voor het registreren en afmelden van gebruikers vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten. Op basis van een risicoafweging wordt bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven. Systeemprocessen draaien onder een eigen gebruikersnaam (een functioneel account), voor zover deze processen handelingen verrichten voor andere systemen of gebruikers.

Toegangsrechten van gebruikers worden periodiek, minimaal jaarlijks, geëvalueerd. Het interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau.

Reparatie en onderhoud van apparatuur (hardware) vindt op locatie plaats door bevoegd personeel, tenzij er geen data op het apparaat aanwezig of toegankelijk is.

Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de beheersorganisatie ingeleverd. De beheerorganisatie zorgt voor een verantwoorde afvoer zodat er geen data op het apparaat aanwezig of toegankelijk is. Als dit niet kan wordt het apparaat of de informatiedrager fysiek vernietigd. Het afvoeren of vernietigen wordt per bedrijfseenheid geregistreerd.

Hergebruik van apparatuur buiten de organisatie is slechts toegestaan indien de informatie is verwijderd met een voldoende veilige methode. Een veilige methode is Secure Erase voor apparaten die dit ondersteunen. In overige gevallen wordt de data twee keer overschreven met vaste data, één keer met random data en vervolgens wordt geverifieerd of het overschrijven is gelukt.

Het interne netwerk van de Justitiële Informatiedienst en de externe connecties wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau komt. Gegevensuitwisseling tussen vertrouwde en onvertrouwde zones wordt inhoudelijk geautomatiseerd gecontroleerd op aanwezigheid van malware. Bij transport van vertrouwelijke informatie over niet vertrouwde netwerken, zoals het internet, wordt altijd geschikte encryptie toegepast.

6.1.7 Betrouwbaar implementeren en beheren van informatiesystemen

Alleen geautoriseerd personeel kan functies en software installeren of activeren. Programmatuur wordt pas geïnstalleerd op een productieomgeving na een succesvolle test en acceptatie. Van updates wordt een log bijgehouden.

De toegang tot broncode wordt zoveel mogelijk beperkt om de code tegen onbedoelde wijzigingen te beschermen. Alleen geautoriseerde personen hebben toegang. Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen. Bij het instellen van besturingsprogrammatuur en programmapakketten wordt uitgegaan van de aanwijzingen van de leverancier.

6.1.8 Business Continuity Management en incidentafhandeling

Periodieke beveiligingsaudits worden uitgevoerd in opdracht van het lijnmanagement. Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd. Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.

Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, alsmede procedures over melding van incidenten.

Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.

In het geval van een calamiteit met de Valideringsdienst, licht Justitiële Informatiedienst de Afnemers onverwijld in (of tenminste binnen 24 uur na het ontstaan van de calamiteit) en doet een voorstel om de calamiteit te herstellen.

6.1.9 Beëindiging van de Valideringsdienst

De Valideringsdienst wordt beëindigd als:

- Daartoe wordt besloten door het management van de Justitiële Informatiedienst;
- Daartoe wordt besloten door de eigenaar van Justitiële Informatiedienst;
- De Justitiële Informatiedienst organisatie wordt opgeheven.

De Justitiële Informatiedienst draagt er zorg voor dat bij een beëindiging van de Valideringsdienst, de gevolgen hiervan voor Afnemers tot een minimum worden beperkt.

Voordat de Valideringsdienst wordt beëindigd, worden de volgende stappen doorlopen:

- De Justitiële Informatiedienst informeert alle aangesloten Afnemers die gebruik maken van de Valideringsdienst over de beëindiging van de Valideringsdienst. Daarop volgend zal ook op de website de beëindiging worden aangekondigd;
- De Justitiële Informatiedienst beëindigt alle contracten met onderaannemers die diensten uitvoeren om de Valideringsdienst operationeel te houden;
- De Justitiële Informatiedienst draagt er zorg voor dat de documentatie van de Valideringsdienst digitaal wordt gearchiveerd, conform vigerende Nederlandse wet- en regelgeving;
- De Justitiële Informatiedienst stelt alle hardware die onderdeel vormt van de Valideringsdienst buiten gebruik.

Er wordt een mededeling gedaan van de beëindiging van de Valideringsdienst in de Staatscourant.

De Justitiële Informatiedienst is niet aansprakelijk voor enige vorm van verlies en/of schade die het gevolg is van de beëindiging van de Valideringsdienst, mits Justitiële Informatiedienst de beëindiging ten minste 1 maand voorafgaand aan de beëindiging kenbaar heeft gemaakt in de Staatscourant.

6.1.10 Wet en regelgeving

De Justitiële Informatiedienst hanteert vigerende Nederlandse wet- en regelgeving betrekking heeft op het voorkomen van verlies, vernietiging of vervalsing van opgeslagen informatie.
Op de website van de Valideringsdienst staat aangegeven hoe Justitiële Informatiedienst omgaat met persoonsinformatie, het privacy statement.

6.1.11 Informatie m.b.t. de werking van de Valideringsdienst

De Justitiële Informatiedienst draagt er zorg voor dat alle relevante informatie die wordt opgeslagen om de werking van de Valideringsdienst aan te kunnen tonen en te borgen uitsluitend voor die doeleinden wordt gebruikt. Deze informatie bevat een audit trail van de werking van de Valideringsdienst. Deze audit trail heeft betrekking op:

- Alle activiteiten op het gebied van toegangsbeveiliging, zoals het toekennen van autorisaties of niet geslaagde inlogpogingen;
- Alle activiteiten van gebruikers met special rechten.

In de audit trail wordt van iedere activiteit een record vastgelegd met daarin minimaal:

- Datum en tijd van registratie van het record;
- Het soort activiteit;

- Het resultaat van de verwerking: success or failure;
- Locatienaam waar de activiteit is uitgevoerd;
- Identiteit (zoals een gebruikersnaam) van de persoon die de activiteit heeft uitgevoerd.

De audit trail is met een mechanisme beschermd tegen ongeautoriseerd lezen, wijzigen, verwijderen of enige andere vorm van manipulatie.

De audit trail vormt onderdeel van de reguliere wekelijkse back-up. De back-up wordt gespreid over 2 datacenters opgeslagen.

De media waarop de back-up is opgeslagen, alsmede de applicaties die nodig zijn om de back-up data te lezen worden ten minste operationeel gehouden gedurende de periode dat de back-up bewaard moet blijven.

6.1.12 Zonering van de technische infrastructuur

De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze staan.

Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.

Elke zone heeft een gedefinieerd beveiligingsniveau zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.

Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone. Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).

6.2 Organisatorische maatregelen

De Justitiële Informatiedienst draagt er zorg voor dat:

- Er met iedere Afnemer een Diensten Niveau Overeenkomst (DNO) is gesloten m.b.t. de afspraken over het niveau van dienstverlening;
- Iedere Afnemer de aansluitvoorwaarden heeft ondertekend;
- Afnemers en Derden via de website van de Valideringsdienst informatie kunnen verkrijgen waar ze met hun vragen m.b.t. de Valideringsdienst terecht kunnen.