

Handreiking

Veilige afvoer van ICT-middelen

Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

Colofon

Naam document

Handreiking Veilige afvoer van ICT-middelen

Versienummer

2.0

Versiedatum

Februari 2019

Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).



Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten (IBD) (2018)

Tenzij anders vermeld, is dit werk verstrekt onder een Creative Commons Naamsvermelding-Niet Commercieel-Gelijk Delen 4.0 Internationaal licentie. Dit houdt in dat het materiaal gebruikt en gedeeld mag worden onder de volgende voorwaarden: Alle rechten voorbehouden. Vervelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

1. De IBD wordt als bron vermeld;
2. Het document en de inhoud mogen commercieel niet geëxploiteerd worden;
3. Publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door de IBD en / of de Vereniging van Nederlandse Gemeenten;
4. Iedere kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Wanneer dit werk wordt gebruikt, hanteer dan de volgende methode van naamsvermelding: "Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten", licentie onder: CC BY-NC-SA 4.0.

Bezoek <http://creativecommons.org/licenses/by-nc-sa/4.0> voor meer informatie over de licentie.

Rechten en vrijwaring

De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Met dank aan

De expertgroepen en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie

Versie	Datum	Wijziging / Actie
1.0	April 2014	
1.0.1	Juli 2016	Taskforce BID verwijderd, GBA vervangen door BRP
2.0	Februari 2019	BIO update

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.



Leeswijzer

Dit product is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

Doel

Het doel van dit document is om handvatten te geven hoe om te gaan met het afvoeren van ICT-middelen

Doelgroep

Dit document is van belang voor de CISO en de ICT afdeling

Relatie met overige producten

- Baseline Informatiebeveiliging Overheid (BIO)
- Informatiebeveiligingsbeleid van de gemeente
- De verwerkersovereenkomst
- Handreiking Service Level Agreements
- Handreiking contractmanagement

Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

- 8.3.1.1 Er is een verwijderinstructie dat herbruikbare media die de organisatie verlaten onherstelbaar van de inhoud worden verwijderd
- 8.3.2 Verwijderen van media
- 11.2.7 Veilig verwijderen of hergebruiken van apparatuur

Wat is er veranderd ten opzichte van de BIG?

Er is weinig veranderd ten opzichte van de BIG, in de maatregelen en controls is er een kleine nuance.

Inhoudsopgave

1. Inleiding.....	5
1.1. Het belang van het veilig afvoeren van ICT-middelen.....	5
1.2. Uitgangspunten.....	5
2. Procedure afvoer ICT-middelen en gegevensdragers	7
2.1. Verantwoordelijkheid	7
2.2. Verzamelen ICT-apparaat.....	7
2.3. Verwijderen / schonen van programma's en gegevens	7
2.4. Reparatie van apparatuur.....	10
2.5. Controle en rapportage.....	10

1. Inleiding

Binnen de gemeente wordt veel gebruik gemaakt van ICT-middelen met gegevensdragers. Op deze gegevensdragers zijn vaak vertrouwelijke gegevens opgeslagen. Wanneer de ICT-middelen en losse gegevensdragers buiten gebruik worden gesteld moeten de gegevens veilig verwijderd worden. Dit kan door personeel van de gemeente gedaan worden maar ook door een leverancier van ICT-middelen als daar goede afspraken en controlemaatregelen voor bestaan en kunnen worden afgedwongen en gecontroleerd worden.

Dit document heeft tot doel om een handreiking te geven die kan leiden tot een proces dat door gemeenten gebruikt kan worden om ICT-middelen en gegevensdragers veilig te schonen en af te voeren.

1.1. Het belang van het veilig afvoeren van ICT-middelen

Het is van belang om ICT-middelen en gegevensdragers volgens een standaard proces veilig te verwijderen. De gemeente is een informatieverwerkende organisatie. Apparatuur en gegevensdragers kunnen vertrouwelijke gegevens bevatten die de gemeente als organisatie niet mogen verlaten, gebeurd dit wel dan kan dat lijden tot een datalek. Gegevens kunnen zich bevinden in veel verschillende apparaten en het is belangrijk dat gegevens van al deze apparaten op een veilige manier worden verwijderd.

1.2. Uitgangspunten

Op basis van de BIO kunnen voor de afvoer van ICT-middelen de volgende uitgangspunten worden gehanteerd:

- Alle ICT-middelen waarop zich programmatuur en gegevens (kunnen) bevinden moeten via een standaard werkwijze worden afgevoerd.
- Alle ICT-middelen worden voorafgaand aan het afvoeren geschoond van programmatuur en gegevens. Als het vernietigen gebeurd bij de gemeente dan hoeft het niet eerst geschoond te worden.
- Verwijdering van programmatuur en gegevens van de gegevensdrager(s) van de computerapparatuur, geschiedt door middel van het overschrijven van de gegevensdrager met een willekeurig bitpatroon¹.
- Alle activiteiten met betrekking tot de afvoer van ICT-middelen en het afvoeren of vernietigen van apparatuur van de gemeente dienen te worden geregistreerd.
- ICT-middelen dienen veilig te worden opgeslagen totdat schoning heeft plaatsgevonden.
- Indien het niet mogelijk is om programmatuur en gegevens te schonen van ICT-middelen en/of gegevensdragers, dienen de apparatuur en/of de gegevensdrager fysiek te worden vernietigd door de ICT-afdeling of door een goedgekeurde derde partij.
- Deze regels zijn ook van toepassing op gegevensdragers van derde partijen waar gemeentelijke informatie is opgeslagen.

Welke activiteiten zijn er op hoofdlijnen?

Afvoer van computerapparatuur omvat op hoofdlijnen de volgende activiteiten:

1. Het verzamelen / innemen van ICT-middelen door de ICT-afdeling.
2. Het schonen van de gegevensdrager(s) met betrekking tot programmatuur en gegevens.
3. Controleren van de schoning van programmatuur en gegevens.
4. Het afvoeren van de ICT-middelen.
5. Het controleren van de logboeken over het afvoeren van ICT-middelen.

¹ <https://www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/geveelueerde-producten>

Stap één tot en met 4 valt onder de verantwoordelijkheid van het hoofd ICT van de gemeente. De tweede stap moet worden uitgevoerd door daarvoor aangewezen ICT-beheerders van de gemeente of een externe beheerder waarmee over de schoning goede afspraken gemaakt zijn. De derde stap wordt verricht door de beheerder. De vierde stap wordt uitgevoerd door een ICT-beheerder of iemand van facilitaire zaken die belast is met afvoer van gemeentelijke middelen. Tenslotte vindt bij stap 5 de controleactiviteiten een onafhankelijke controle plaats door de afdeling Interne Controle, zonodig ondersteund door een externe accountant.

2. Procedure afvoer ICT-middelen en gegevensdragers

2.1. Verantwoordelijkheid

De verantwoordelijkheid om gemeentelijke ICT-middelen en gegevensdragers af te voeren ligt bij het hoofd ICT van de gemeente of een gelijkwaardige functionaris.

Het hoofd ICT is verantwoordelijk voor het actueel houden van de procedure afvoer ICT-middelen en gegevensdragers.

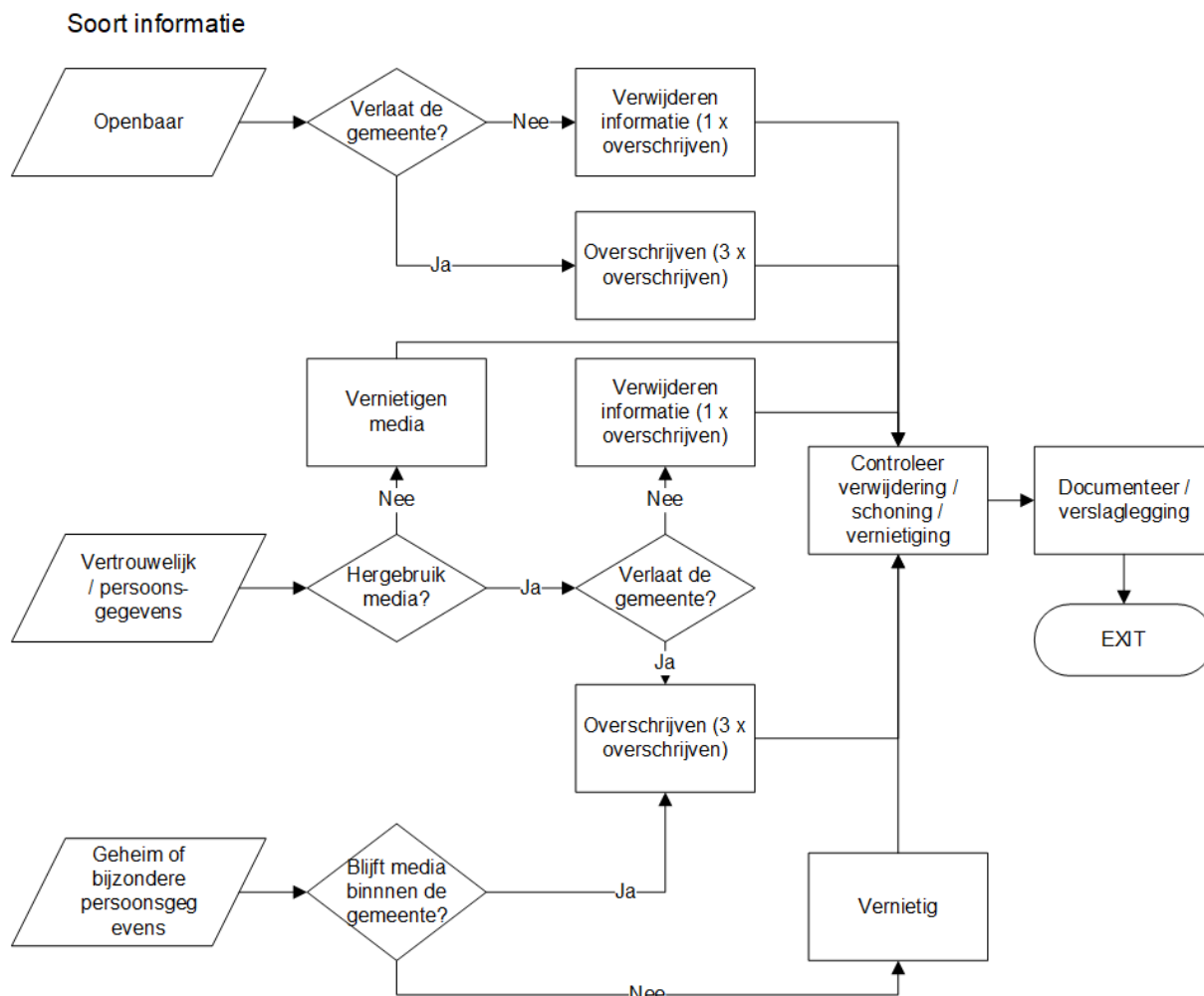
Van alle stappen in het proces wordt een logboek bijgehouden door de uitvoerenden en dit logboek dient ter controle van de uitgevoerde activiteiten.

2.2. Verzamelen ICT-apparatuur

1. Een medewerker doet een aanvraag bij de ICT-afdeling om één of meerdere computers of apparaten met mediadragers te laten afvoeren. De ICT-afdeling bepaalt zelf welke apparatuur moet worden afgevoerd.
2. In onderling overleg wordt afgesproken of de computerapparatuur wordt aangeleverd of wordt afgehaald en wanneer dit geschiedt.
3. De aanlevering van de computerapparatuur wordt geregistreerd in de CMDB (Configuration Management Database).
4. De afleverende medewerker ontvangt een bewijs van aflevering van de computerapparatuur.
5. De gegevensdragers dienen geschoond te worden in de apparatuur waar deze zich in bevindt, tenzij dit niet mogelijk is, in dat geval worden de gegevensdragers verwijderd uit de apparatuur.
6. De computerapparatuur en de gegevensdrager(s) worden in een beveiligde ruimte opgeslagen.

2.3. Verwijderen / schonen van programmatuur en gegevens

Het schema wat gehanteerd wordt bij het bepalen van hoe gegevens of de gegevensdrager vernietigd kunnen worden, dient eerst uit te gaan van het soort gegevens en vervolgens van de soort gegevensdrager. Op de volgende pagina wordt in een diagram en tabellen verder toelichten gegeven.



Figuur 1: Verwijderen van informatie en/of ICT middelen

Methoden

Methode	Omschrijving
Verwijderen informatie van de gegevensdrager	Verwijderen van informatie is de meest eenvoudige methode. Een format en/of het verwijderen van bestanden is niet goed genoeg. Informatie kan dan nog steeds op een eenvoudige manier worden teruggehaald. Het volstaat om de media eenmalig te overschrijven met een willekeurig patroon.
Overschrijven informatie op de gegevensdrager	Als de gegevens gevoelig zijn is enkelvoudig overschrijven niet goed genoeg. De media dient meervoudig overschreven te worden doormiddel van een 'nul' character, een 'één' character gevolgd door een willekeurig character of teken (niet binair). Als media niet overschreven kan worden dient bij magnetische gegevensdragers een degausser te worden gebruikt. Als ook dat niet kan is vernietiging de enige optie die overblijft (bijvoorbeeld een CD-ROM).
Vernietigen gegevensdrager	Vernietiging is nodig als het soort informatie extra gevoelig is of als andere methoden om gegevens te verwijderen niet kunnen worden gebruikt. Vernietiging is verschillend per soort media.

Tabel 1: Methoden voor verwijderen van informatie

Soort	Verwijderen	Overschrijven	Vernietigen
Papier			
Papier	Standaard oud papierbak	Zie vernietigen	Eerst zelf versnipperen (shred) gevolgd door afvoer in de papierbak voor gevoelige informatie ²
Mobiele apparaten			
Mobiele telefoons, smartphones	Handmatig verwijderen van alle informatie, gebruik daarna de functie om het apparaat terug te zetten naar fabrieksinstellingen	Zie verwijderen	Versnipperen van het apparaat of fysiek vernietigen of verbranden
Netwerk apparatuur			
	Terugzetten naar fabrieksinstellingen	Zie verwijderen	Versnipperen van het apparaat, of fysiek vernietigen of verbranden
Bureau-apparatuur			
Fax, printer	Terugzetten naar fabrieksinstellingen	Zie verwijderen	Versnipperen van het apparaat, of fysiek vernietigen of verbranden
kopieer drum (in een laserprinter of laserfax)	Print of kopieer 3 vellen met willekeurige niet sensitive tekst, daarna bij het juiste afval meegeven	Print of kopieer 3 vellen met willekeurige niet sensitive tekst, daarna bij het juiste afval meegeven	Versnipperen van het apparaat, of fysiek vernietigen of verbranden
Magnetische media			
Harddisks	Overschrijven met een willekeurig bitpatroon	3 x overschrijven met een bitpatroon, eerst met een 'nul' daarna met een 'één' tenslotte met een willekeurig teken	Versnipperen van het apparaat, of fysiek vernietigen of verbranden
USB-media	Overschrijven met een willekeurig bitpatroon	3 x overschrijven met een bitpatroon, eerst met een 'nul' daarna met een 'één' tenslotte met een willekeurig teken	Versnipperen van het apparaat, of fysiek vernietigen of verbranden
Geheugenkaarten	Overschrijven met een willekeurig bitpatroon	3 x overschrijven met een bitpatroon, eerst met een 'nul' daarna met een 'één' tenslotte met een willekeurig teken	Versnipperen van het apparaat, of fysiek vernietigen of verbranden
Tapes	Overschrijven met een willekeurig bitpatroon	3 x overschrijven met een bitpatroon, eerst met een 'nul' daarna met een 'één' tenslotte met een willekeurig teken	Versnipperen van het apparaat, of fysiek vernietigen of verbranden
Optische media			
CD / DVD	Beschrijfbaar laag kapot krassen of de CD/DVD kapot breken	Beschrijfbaar laag kapot krassen of de CD/DVD kapot breken	Beschrijfbaar laag verwijderen of versnipperen van de CD/DVD
Smartcards			
Smartcards (chip)	Chip uit de kaart stansen	Chip uit de kaart stansen	Versnipperen
Smartcards (magnetisch)	Overschrijven van de magneetstrip	Degaussen	Degaussen of versnipperen van het apparaat of fysiek vernietigen of verbranden

Tabel 2: Type informatieopslag en hoe omgegaan moet worden met het verwijderen, overschrijven en vernietigen

² Er wordt vanuit gegaan dat de gemeente gebruik maakt van een papier vernietig dienst waarbij er speciale afsluitbare bakken gebruikt worden.

Controleren van de schoning

Na het schonen van de mediadragers / apparatuur wordt er altijd een controle uitgevoerd of de schoning geslaagd is. Deze controle wordt vermeld in het logboek.

Vernietiging van mediadragers

Het vernietigen van mediadragers dient bij voorkeur door twee personen te gebeuren en na het vernietigen dient een proces-verbaal van vernietiging te worden opgemaakt waarop vermeld is wat er is vernietigd (omschrijving, serienummer) en hoe. Beide personen dienen dit proces-verbaal te tekenen en het proces-verbaal dient te worden bewaard.

2.4. Reparatie van apparatuur

Apparatuur die gebruikt wordt om informatie te verwerken kan een keer kapot gaan. Deze apparatuur kan gemeentelijke informatie bevatten en daarom dienen goede afspraken gemaakt te worden met de leveranciers die de apparatuur repareren³.

2.5. Controle en rapportage

Het hoofd ICT ziet erop toe dat alle computerapparatuur volgens de beschreven richtlijnen en procedures wordt geschoond en afgevoerd. Van alle activiteiten wordt een logboek bijgehouden.

De interne controle of CISO kan, zo nodig ondersteund door de externe accountant, gevraagd en ongevraagd de maatregelen voor de afvoer van computerapparatuur controleren. Hierover wordt gerapporteerd aan het hoofd ICT.

Controleren van de verwijdering van programmatuur en gegevens

1. De interne controle of CISO controleert steekproefsgewijs de volgende punten:
 - de aanwezigheid van computerapparatuur en de gegevensdrager(s) in de beveiligde opslagruimte.
 - de overeenkomst tussen de registratie en de daadwerkelijk opgeslagen computerapparatuur.
 - de juiste en volledige schoning van de aanwezige gegevensdragers.
 - de complete registratie van alle activiteiten.
 - De processen-verbaal van vernietiging.
2. De uitkomsten van de controle worden schriftelijk vastgelegd en zo nodig gerapporteerd aan het management.
3. Indien nodig worden verbetermaatregelen voorgesteld.

³ Voorbeeld hiervan is bijv. de 'keep your hard drive service' van verschillende hardware leveranciers.

Kijk voor meer informatie op:
www.informatiebeveiligingsdienst.nl

Nassaulaan 12
2514 JS Den Haag
CERT: 070 373 80 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl

