TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Veilige afvoer van ICT-middelen

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Veilige afvoer van ICT-middelen’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Doel

Dit document biedt een handreiking voor het veilig afvoeren van ICT-middelen door organisaties binnen de Rijksoverheid.

Doelgroep

Dit document is van belang voor de verantwoordelijke ICT-beheerder.

Reikwijdte

Dit document heeft voornamelijk betrekking op de maatregel 10.7.2.1 van de Baseline Informatiebeveiliging Rijksdienst (BIR). Het document gaat in op personele, organisatorische en technische informatiebeveiligingsaspecten die organisaties binnen de Rijksoverheid dienen te overwegen in relatie tot het afvoeren van ICT-middelen.

Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Informatiebeveiligingsbeleid

Inhoudsopgave

1 Inleiding

Overheidsorganisaties maken veel gebruik van ICT-middelen als gegevensdragers of als middelen waarin gegevensdragers worden toegepast. Op deze gegevensdragers kunnen vertrouwelijke gegevens opgeslagen zijn. Wanneer de ICT-middelen buiten gebruik worden gesteld, moeten de gegevens veilig verwijderd worden. Dit document biedt een handreiking voor het veilig schonen en afvoeren van ICT-middelen.

Het schonen en afvoeren kan door de overheidsorganisatie zelf gedaan worden, maar ook door een leverancier van ICT-middelen. Als het schonen en afvoeren door een leverancier wordt uitgevoerd, is het belangrijk duidelijke afspraken en controlemaatregelen in te richten die kunnen worden afgedwongen en kunnen worden gecontroleerd.

1.1 Het belang van het veilig afvoeren van ICT-middelen

Overheidsorganisaties kunnen gekwalificeerd worden als informatieverwerkende organisaties. ICT-middelen en gegevensdragers kunnen daardoor vertrouwelijke gegevens bevatten die de organisatie niet mogen verlaten. Het is daarom van belang om gegevensdragers volgens een standaard proces veilig te verwijderen.

Gegevens kunnen zich bevinden in:

- laptops en desktop computers
- mobiele apparaten, zoals smartphones en tablets
- printers
- scanners
- faxapparaten
- servers
- draagbare media (geheugenkaarten, USB-sticks)
- etc.

1.2 Uitgangspunten baseline

Op basis van de BIR 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.
- Verwijdering van programmatuur en gegevens van de gegevensdrager(s) van de computerapparatuur, geschiedt door middel van het overschrijven van de gegevensdrager met een willekeurig bitpatroon.
- Alle activiteiten met betrekking tot de afvoer van ICT-middelen en het verwijderen van gegevens van de organisatie 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 gegevensdragers, dienen de apparatuur en de gegevensdrager fysiek te worden vernietigd door de ICT-afdeling of door een goedgekeurde derde partij.
- Alle regels voor een veilige afvoer van ICT-middelen zijn ook van toepassing op gegevensdragers van derde partijen, waarop informatie van de overheidsorganisatie is opgeslagen.

1.3 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.

De stappen één tot en met vier behoren tot de verantwoordelijkheid van het hoofd ICT van de organisatie of een gelijkwaardige functionaris. De tweede stap moet worden uitgevoerd door daarvoor aangewezen ICT-beheerders van de organisatie of een externe beheerder waarmee goede afspraken over de schoning zijn gemaakt. De derde stap wordt verricht door de beheerder. De vierde stap wordt uitgevoerd door een ICT-beheerder of een medewerker van facilitaire zaken die belast is met de afvoer van middelen. Tenslotte vindt bij de controleactiviteiten een onafhankelijke controle plaats door een afdeling verantwoordelijk voor de interne controle, zonodig ondersteund door een externe accountant.

2 Procedure afvoer ICT-middelen en gegevensdragers

2.1 Verantwoordelijkheid

De verantwoordelijkheid om ICT-middelen en gegevensdragers af te voeren, behoort bij de verantwoordelijkheid van het hoofd ICT van de organisatie of een gelijkwaardige functionaris.

Het hoofd ICT is verantwoordelijk voor het actueel houden van de procedure voor het afvoeren van 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.

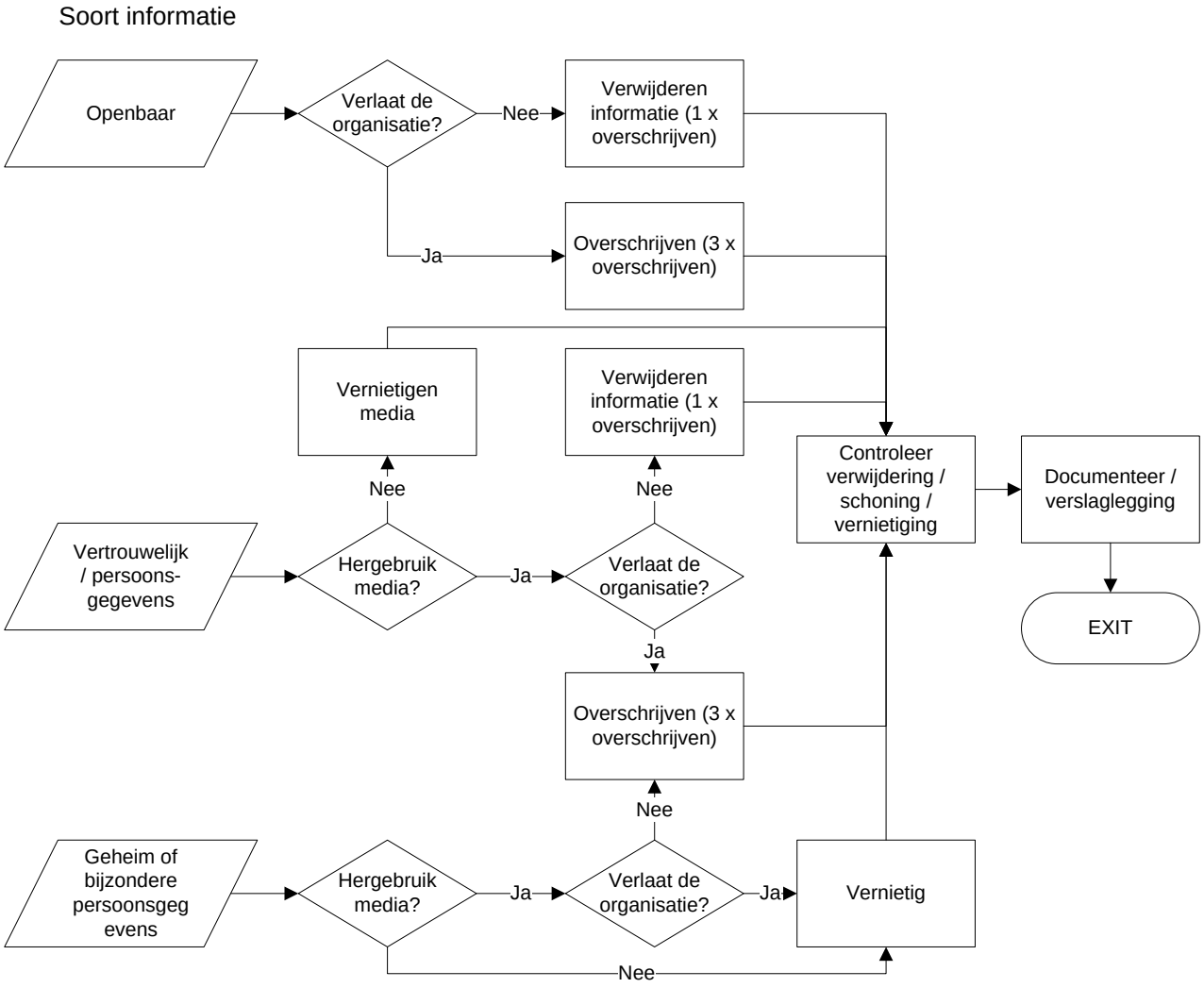
2.2 Verzamelen/innemen van ICT-middelen

Voor het verzamelen/innemen van ICT-middelen zijn de volgende stappen te onderscheiden:

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 plaatsvindt.
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 Schonen van programmatuur en gegevens

Voor een veilige schoning van programmatuur en gegevens dient een volgend keuzeschema te worden gehanteerd, waarbij uitgegaan moet worden van het soort gegevens en vervolgens van de soort gegevensdrager dat geschoond moet worden.



Voor het schonen van ICT-middelen zijn de volgende methoden te onderscheiden:

Methode	**Omschrijving**
Verwijderen informatie van de gegevensdrager	Verwijderen van informatie is de meest eenvoudige methode. Formatteren en/of het verwijderen van bestanden is niet voldoende. 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 voldoende. De media dient meervoudig overschreven te worden door middel 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.

De methode voor het schonen van ICT-middelen is afhankelijk van het soort middel waarop gegevens zijn opgeslagen. De drie hierboven onderscheiden methodieken zijn als volgt toe te passen op de volgende ICT-middelen:

ICT-middel	**Verwijderen**	**Overschrijven**	**Vernietigen**
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
Netwerkapparatuur			
	Terugzetten naar fabrieksinstellingen	Zie verwijderen	Versnipperen van het apparaat, of fysiek vernietigen of verbranden
Bureauapparatuur			
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 sensitieve tekst, daarna bij het juiste afval meegeven	Print of kopieer 3 vellen met willekeurige niet sensitieve 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	Versnipperen van het apparaat, of fysiek vernietigen of verbranden

ICT-middel	Verwijderen	Overschrijven	Vernietigen
		teken	
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	3 x overschrijven met een bitpatroon, eerst met een ‘nul’ daarna met een ‘één’ tenslotte met een willekeurig teken
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	3 x overschrijven met een bitpatroon, eerst met een ‘nul’ daarna met een ‘één’ tenslotte met een willekeurig teken
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	Beschrijfbare laag kapot krassen of de CD/DVD kapot breken	Beschrijfbare laag kapot krassen of de CD/DVD kapot breken	Beschrijfbare 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

Controleren van de schoning

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

Vernietiging afvoeren 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. Hierop wordt vermeld wat er is vernietigd (omschrijving, serienummer) en op welke manier. Beide personen dienen dit proces-verbaal te ondertekenen en het proces-verbaal dient te worden bewaard.

2.4 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.