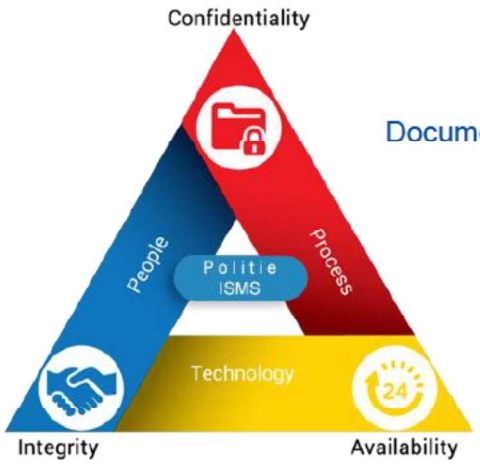
Addendum BIO: Politie-specifieke maatregelen

Beleid



Document referentienummer:	ISMS-A05.01.01-02
Document auteur:	Kwartier IB – Cluster Beleid
Document eigenaar:	Hoofd Kwartier IB
Status:	Definitief
Versie nummer:	1.1
Versie datum:	24 juni 2020
Geldigheidsduur:	2 jaar na ondertekening
Rubricering:	Pol. INTERN

« waakzaam en dienstbaar »

Documentinformatie

Document referentienummer:	ISMS-A05.01.01-02
Document auteur:	Kwartier IB – Cluster Beleid
Document eigenaar:	Hoofd Kwartier IB
Status:	Definitief
Versie nummer:	1.0
Versie datum:	24 juni 2020
Geldigheidsduur	2 jaar na ondertekening
Rubricering:	Pol. INTERN
Documentnaam	ISMS-A05.01.01-02-Addendum BIO-Politie Specifieke Maatregelen-v1.0.docx

Deze tabel vult automatisch

Deze versie vervangt alle voorgaande versies van dit document.

Accordering

Naam	Functie	Handtekening	Datum

Distributielijst

Versie	Datum	Verspreidingsvorm	Naam/Functie/Opmerking

Reviews

Versie	Datum	Door	Functie
0.9c	13-11-2019	5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e	Medewerkers Kwartier IB Domein Architect Informatiebeveiliging (TTA)

Versiegeschiedenis

Versie	Datum	Door	Opmerkingen
0.1	04-09-2019		Maatregelen Politie Intern en Confidentieel verwerkt
0.2	10-09-2019		Maatregelen Politie Geheim verwerkt
0.3	11-09-2019		Huidige addenda van de uitvoeringsregelingen opgenomen in het document.
0.4	17-09-2019		Kleuren conform rubriceringsregeling toegepast.
0.9	14-10-2019		Ontbrekende maatregelen toegevoegd en gereed gemaakt voor interne review.
0.9a	23-10-2019		Enkele kleine aanpassingen op paragrafen gedaan
0.9b	28-10-2019		Enkele kleine aanpassingen op paragrafen gedaan
0.9c	13-11-2019		Commentaar interne review verwerkt
0.9d	26-11-2019		Nummering van maatregelen Politie-specifiek gemaakt en enkele kleine wijzigingen doorgevoerd.
0.9e	10-12-2019		Enkele tekstuele aanpassingen.

0.9f	12-12-2019	De uitgangspunten overgenomen van uitvoeringsregelingen
0.9g	01-02-2020	Enkele aanvullingen diverse paragrafen
1.0	15-04-2020	Definitieve versie
1.1	24-06-2020	Aanpassing Bijlage A tbv TLS 1.3

Bijbehorende documenten

Versie	Datum	Omschrijving
1.04	04-11-2019	ISMS-A05.01.01-01-Baseline Informatiebeveiliging Overheid

De documenten, waarnaar als geheel of voor een onderdeel, in dit document hier boven normatief is verwezen, zijn onmisbaar voor de toepassing ervan. Bij gedateerde verwijzingen is alleen de aangehaalde uitgave van toepassing. Bij ongedateerde verwijzingen is de laatste uitgave van het document (met inbegrip van eventuele wijzigings- en correctiebladen) waarnaar is verwezen van toepassing

Inhoudsopgave

Lijst van Tabellen

Inleiding

Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van de overheid. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Het doorlopen van dit proces is een verantwoordelijkheid van het lijnmanagement. Om te voorkomen dat informatie en informatiesystemen te licht of te zwaar worden beveiligd, vormt risicomanagement een belangrijk onderdeel in dit proces.
De eerste stap in het beveiligingsproces is het maken van een risicoafweging. Daarbij wordt een inschatting gemaakt van mogelijke schade als informatiesystemen (tijdelijk) niet beschikbaar zijn, de informatie niet integer is en/of deze informatie in verkeerde handen valt. Ook wordt een inschatting gemaakt van de dreigingen waartegen beschermd moet worden. De inschatting van mogelijke schade en dreigingen leidt tot beveiligingseisen om het risico te beperken. Om deze eisen af te dekken worden passende maatregelen getroffen of wordt het (rest)risico geaccepteerd.

De Baseline Informatiebeveiliging Overheid (BIO) helpt het lijnmanagement bij het nemen van haar verantwoordelijkheid ten aanzien van informatiebeveiliging. Het ingewikkelde proces van risicomanagement wordt met de BIO vereenvoudigd. In de BIO zijn namelijk op basis van de generieke schades en dreigingen voor de overheid standaard basisbeveiligingsniveaus (BBN's) gedefinieerd met bijbehorende beveiligingseisen die moeten worden ingevuld. Per informatiesysteem bepaalt het lijnmanagement het BBN; de BIO biedt daarvoor een zogenaamde BBN-toets.

In de BIO staat per BBN beschreven aan welke controls uit de ISO 27002 (Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging) moet worden voldaan. Bij alle controls dient, op basis van een individuele risicoafweging, bepaald te worden hoe aan de beveiligingsdoelstelling van de control voldaan kan worden. Daarbij zijn de controls, waar van toepassing, gedeeltelijk uitgewerkt in verplichte, concrete overheidsmaatregelen. De controls zijn toebedeeld aan rollen, waarmee de verdeling over verantwoordelijken makkelijker is. Zo kan ook de dienstenleverancier die de expertise heeft, bepalen met welke concrete maatregelen hij de control in vult. Ten slotte moet verantwoording worden afgelegd over de risicoafweging en over de effectieve invulling van de controls. Deze verantwoording is onderdeel van de bestuurlijke verantwoording over de beveiliging van informatiesystemen. De wijze en mate van detail van de verantwoording hangt af van het BBN. Des te hoger het BBN, des te meer detail nodig is in verband met de hogere potentiële impact. Dienstenleveranciers leggen verantwoording af aan hun (gedeelde) opdrachtgever en er wordt verantwoording afgelegd aan de ketenpartners met wie afspraken over de beveiliging van informatie zijn gemaakt.

De opdrachtgever ziet erop toe dat de afgenomen diensten in overeenstemming met de gestelde eisen beveiligd zijn; de afnemers van de diensten mogen hierop vertrouwen en worden door de opdrachtgever geïnformeerd over uitzonderingssituaties. De BIO biedt hiermee de basis om te zorgen dat de beveiliging van informatie(systemen) bij alle bedrijfsonderdelen van de overheid bevorderd wordt. Deze bedrijfsonderdelen kunnen erop vertrouwen dat gegevens die worden verstuurd naar of worden ontvangen van andere onderdelen van de overheid in lijn met wet- en regelgeving passend beveiligd zijn. Waar naleving (nog) niet volledig mogelijk is, dienen de bedrijfsonderdelen via een 'explain' de eventuele risico's inzichtelijk te maken aan hun ketenpartners. De BIO is opgedeeld in twee delen waarbij het eerste deel de achtergrond weergeeft en het tweede deel het daadwerkelijk uit te voeren kader omvat.

Politie-specifieke maatregelen

De BIO beschrijft naast de maatregelen uit deel 1 en 2 tevens specifieke maatregelen voor bepaalde overheidslagen (Rijk, Overheid, Gemeente Waterschap, Gemeenten). Er worden geen specifieke maatregelen voor de Politie vermeld.

In dit addendum worden alle maatregelen genoemd die specifiek zijn voor de Politie, onderverdeeld in de rubriceringen 'Politie Intern', 'Politie Confidentieel' en 'Politie Geheim'.

Voor de rubricering 'Politie Zeer Geheim' geldt dat dit geheel op basis van risico analyses geschiedt.

Het addendum is aanvullend op de teksten en normen uit deel 1 en 2 van de BIO. Hierbij zijn de controls en maatregelen van beveiligingsniveau BBN 2 als basis genomen, eventuele extra te nemen beveiligingsmaatregelen kunnen van toepassing zijn indien uit de BBN-toets blijkt dat beveiligingsniveau BBN 3 van toepassing is.

Het kwartier IB beschrijft hiermee de beveiligingsmaatregelen voor Politie Intern, Confidentieel en Geheim.

De BIO in combinatie met dit document vervangt hiermee de volgende bestaande uitvoeringsregelingen:

- *Uitvoeringsregeling Informatiebeveiliging Dienst ICT Politie Intern v2.0*
- *Uitvoeringsregeling Informatiebeveiliging Dienst ICT Politie Confidentieel v2.0*
- *Uitvoeringsregeling Informatiebeveiliging Dienst ICT Politie Geheim v1.0*

In het kort:

Rubricering	Beveiligingsmaatregelen
Politie Intern	BIO + 'Addendum BIO: Politie-specifieke maatregelen' (voor Politie Intern, aangeduid in de nummering met 'pi').
Politie Confidentieel	BIO + 'Addendum BIO: Politie-specifieke maatregelen' (voor Politie Confidentieel, aangeduid in de nummering met 'pc').
Politie Geheim	BIO + 'Addendum BIO: Politie-specifieke maatregelen' (voor Politie Geheim, aangeduid in de nummering met 'pg').
Politie Zeer Geheim	Op basis van risico analyses.

Uitgangspunten

De volgende uitgangspunten zijn gehanteerd bij het opstellen van de specifieke beveiligingsmaatregelen voor Politie.

Uitgangspunt	Omschrijving
U1	Conform de Rubriceringregeling Politie 2015[1]
U2	Het principe "Alles delen, op basis van need-to-know"
U3	Conform wetgeving
U4	Jericho principe: informatie/data zo dicht mogelijk bij de bron beveiligen
U5	Scheiding van beschikkende, verstrekkende en uitvoerende functies
U6	Alle handelingen zijn onweerlegbaar en worden voor personen en systemen gelogd.
U7	Uitgevoerde controles dienen te worden geregistreerd.
U8	Informatie kan alleen na de-rubricering in een lager gerubriceerde omgeving geplaatst worden.

Tabel 1 Uitgangspunten

Deze acht uitgangspunten zijn de basis uitgangspunten waartegen de risico's worden afgewogen. Indien er een risico optreedt dat niet acceptabel is worden additionele maatregelen genomen.

Toelichting uitgangspunt U2

Zoals eerder genoemd is het principe "alles gesloten, tenzij" losgelaten en is omgezet in "alles delen, op basis van need-to-know"2. Dit "nieuwe" beveiligingsprincipe is in lijn met WPG en het Jericho3 principe. Met dit delen wordt bedoeld dat de politiegegevens gedeeld mogen worden tussen geautoriseerden. Autorisatie is conform WPG artikel 6 lid 3 dat een duidelijk omschreven autorisatie vereist.

Toelichting uitgangspunt U4

Informatie/data wordt zo dicht mogelijk bij de bron beveiligd. Dit houdt in dat bij bijvoorbeeld databases of COTS applicaties de data indien nodig in de database of applicatie versleuteld wordt opgeslagen. Wanneer de informatie over het netwerk wordt getransporteerd, wordt deze versleuteld getransporteerd.

[1] Bron: Rubriceringsregeling Politie 2015 03 12 v1 0.pdf

[2] Bron: goedgekeurde Visie op autoriseren.pdf & 120321 Besluitvorming RKC Autorisatiemodel Politie.pdf

[3] Jericho: het uitgangspunt dat informatie niet beveiligd kan worden door haar veilig af te schermen door het gebruik van firewalls en dmz's, maar dat informatie beveiligd dient te worden op het niveau van de gegevenselementen zelf. (bron: http://nl.wikipedia.org/wiki/Jericho_Forum)

BIO paragraaf 6.1: Interne organisatie

Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.

Politie Intern

6.1.1.pi1	Wet AVG en WPG	

Politie Confidentieel

6.1.1.pc1	Wet AVG en WPG	

Politie Geheim

6.1.1.pg1	Wet AVG en WPG	

BIO paragraaf 6.2: Mobiele apparatuur en telewerken

Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.

Politie Intern

6.2.1.pi1		De mate van bescherming wordt getoetst en geaccordeerd op basis van een risicoanalyse.	

Politie Confidentieel

6.2.1.pc1		De mate van bescherming wordt getoetst en geaccordeerd op basis van een risicoanalyse.	

Politie Geheim

6.2.1.pg1		Politie Geheime informatie wordt niet op draagbare computers ontsloten.	

BIO paragraaf 8.3: Behandelen van media

Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.

Politie Intern

8.3.2.pi1		Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de Dienst ICT ingeleverd. De Dienst ICT zorgt voor een verantwoorde afvoer zodanig dat er geen data op het apparaat aanwezig of toegankelijk is door het fysiek te vernietigen. Het vernietigen wordt door de Dienst ICT geregistreerd, conform de 'Uitvoeringsregeling vernietiging gegevensdragers v1.0', of nieuwere versie daarvan.	
8.3.2.pi2		Hergebruik van apparatuur binnen de organisatie is slechts toegestaan indien alle informatie is verwijderd met een voldoende veilige methode, die bij voorkeur is goedgekeurd door de AIVD. Een veilige methode is bv. NIST 800-88 Purge of DoD 5220.22-M ECE (aanwezig in bv. Blancco) voor apparaten die dit ondersteunen. Apparatuur, waarvan de informatie is verwijderd, mag binnen de organisatie worden hergebruikt mits het wordt ingezet binnen gelijke rubricering 'Politie Intern'.	
8.3.3.pi1		Om Politie interne informatie te beschermen worden maatregelen genomen, zoals: a. versleuteling; b. bescherming door fysieke maatregelen, zoals afgesloten containers; c. gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen; d. persoonlijke aflevering; e. twee-factor authenticatie; f. opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes.	
8.3.3.pi2		Fysieke verzending van vertrouwelijke informatie dient te geschieden met goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.	

Politie Confidentieel

8.3.2.pc1		Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de Dienst ICT ingeleverd. De Dienst ICT zorgt voor een verantwoorde afvoer zodanig dat er geen data op het apparaat aanwezig of toegankelijk is door het fysiek te vernietigen. Het vernietigen wordt door de Dienst ICT geregistreerd, conform de 'Uitvoeringsregeling vernietiging gegevensdragers v1.0, of nieuwere versie daarvan'.	
8.3.2.pc2		Hergebruik van apparatuur die was ingezet voor de rubricering 'Politie Confidentieel' buiten de politie is niet toegestaan. De datadrager wordt onder toezicht fysiek vernietigd, conform de 'Uitvoeringsregeling vernietiging gegevensdragers v1.0', of nieuwere versies daarvan	
8.3.3.pc1		Om Politie Confidentiële informatie te beschermen worden maatregelen genomen, zoals: a. versleuteling (opslag en transport); b. bescherming door fysieke maatregelen, zoals afgesloten containers; c. gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen; d. persoonlijke aflevering; e. twee-factor authenticatie;	

		f. opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes.	
8.3.3.pc2		Fysieke verzending van confidentiële informatie dient te geschieden met door de Dienst ICT goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.	

Politie Geheim

8.3.2.pg1		Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de Dienst ICT ingeleverd. De Dienst ICT zorgt voor een verantwoorde afvoer zodanig dat er geen data op het apparaat aanwezig of toegankelijk is door het fysiek te vernietigen (schredderen) onder toezicht van een daartoe gerechtigd persoon. Het vernietigen wordt door de Dienst ICT geregistreerd, conform de 'Uitvoeringsregeling vernietiging gegevensdragers v1.0, of nieuwere versies daarvan'.	
8.3.2.pg2		Hergebruik van apparatuur die was ingezet voor de rubricering 'Politie Geheim' buiten de politie is niet toegestaan. De datadrager wordt onder toezicht fysiek vernietigd. Het vernietigen wordt door de Dienst ICT geregistreerd, conform de 'Uitvoeringsregeling vernietiging gegevensdragers v1.0, of nieuwere versies daarvan'.	
8.3.3.pg1		Om Politie Geheime informatie te beschermen worden maatregelen genomen, zoals: a. versleuteling (opslag en transport); b. bescherming door fysieke maatregelen, zoals afgesloten containers; c. gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen; d. persoonlijke aflevering; e. twee-factor authenticatie; f. opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes.	
8.3.3.pg2		Fysieke verzending van geheime informatie dient te geschieden met door NBV goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar is en inbreuk detecteerbaar is.	

BIO paragraaf 9.2: Beheer van toegangsrechten van gebruikers

Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.

Politie Intern

9.2.5.pi1		Toegangsrechten van gebruikers worden periodiek, minimaal jaarlijks, geëvalueerd. Het interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau.	

Politie Confidentieel

9.2.5.pc1		Toegangsrechten van gebruikers worden periodiek, minimaal halfjaarlijks, geëvalueerd. Het interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau.	

Politie Geheim

9.2.5.pg1		Toegangsrechten van gebruikers worden periodiek, *minimaal per kwartaal*, geëvalueerd. Het interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau.	

BIO paragraaf 9.4: Toegangsbeveiliging van systeem en toepassing

Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.

Politie Intern

9.4.4.pi1		Er behoren procedures te worden vastgesteld om het gebruik van IT voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort maandelijks te worden beoordeeld.	

Politie Confidentieel

9.4.2.pc1		Toegang tot de Politie Confidentiële omgeving wordt verleend op basis van two-factor authenticatie.	
9.4.4.pc1		Er behoren procedures te worden vastgesteld om het gebruik van IT voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort wekelijks te worden beoordeeld.	

Politie Geheim

9.4.2.pg1		Toegang tot de Politie Geheime omgeving wordt verleend op basis van two-factor authenticatie en in een beveiligde ruimte van geschikt niveau.	
9.4.2.pg2		Na het vijfmaal achtereenvolgens ingeven van een foutief wachtwoord, wordt de toegang geblokkeerd en dient de reset aanvraag via de Teamchef plaats te vinden.	
9.4.2.pg3		Na het 3 maal achtereenvolgens foutief toepassen van de wachtwoord resettool wordt de het account geblokkeerd en kan reset slechts plaatsvinden via de Teamchef na adequate authenticatie (waartoe nog nadere regels worden vastgesteld).	
9.4.2.pg4		Aanvullende beveiligingseisen ten aanzien van privileged (admin of beheer) accounts wachtwoorden; Authenticatie van een privileged account vindt plaats via two-factor authenticatie en in een beveiligde ruimte van geschikt niveau.	
9.4.4.pg1		Er behoren procedures te worden vastgesteld om het gebruik van IT voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort dagelijks te worden beoordeeld.	

BIO paragraaf 10.1: Cryptografische beheersmaatregelen

Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

Politie Intern

10.1.2.pi1		De geldigheidsduur van cryptografische sleutels wordt bepaald aan de hand van de beoogede toepassing met een maximum tot 3 jaar na uitgifte van de sleutel (VBV 41000(B).	

Politie Confidentieel

10.1.2.pc1		De geldigheidsduur van cryptografische sleutels wordt bepaald aan de hand van de beoogde toepassing met een maximum tot één jaar na uitgifte van de sleutel (VBV 41000(B).	

Politie Geheim

10.1.2.pg1		De geldigheidsduur van cryptografische sleutels wordt bepaald aan de hand van de beoogde toepassing met een maximum tot 6 maanden na uitgifte van de sleutel (VBV 41000(B).	

BIO paragraaf 11.1: Beveiligde gebieden

Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen.

Politie Intern

11.1.5.pi1		Er vindt minimaal één keer per jaar een periodieke controle/evaluatie plaats op de autorisaties voor fysieke toegang.	
11.1.5.pi2		Papieren documenten en mobiele gegevensdragers (goedgekeurd door EU, NATO, AIVD of Defensie.) die Politie Interne informatie bevatten worden na gebruik beveiligd opgeslagen.	
11.1.5.pi3		Medewerkers die zelf niet geautoriseerd zijn mogen met een passende screening alleen onder toeziend oog 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 Politie Interne informatie wordt gewerkt.	
11.1.5.pi4		Beveiligde ruimten (zoals een serverruimte of kluis) waarin zich geen personen bevinden zijn afgesloten en worden conform het controleprotocol jaarlijks gecontroleerd.	

Politie Confidentieel

11.1.5.pc1		Er vindt minimaal één keer per jaar een periodieke controle/evaluatie plaats op de autorisaties voor fysieke toegang.	
11.1.5.pc2		Papieren documenten en mobiele gegevensdragers (goedgekeurd door EU, NATO, AIVD of Defensie.) die Politie Confidentiële informatie bevatten worden na gebruik beveiligd opgeslagen.	
11.1.5.pc3		Medewerkers die zelf niet geautoriseerd zijn mogen met een passende screening alleen onder toeziend oog 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 Politie Confidentiële informatie wordt gewerkt.	
11.1.5.pc4		Beveiligde ruimten (zoals een serverruimte of kluis) waarin zich geen personen bevinden zijn afgesloten en worden conform het controleprotocol jaarlijks gecontroleerd.	

Politie Geheim

11.1.4.pg1		Er zijn passende Tempest maatregelen getroffen.	
11.1.5.pg1		Er vindt minimaal één keer per kwartaal een periodieke controle/evaluatie plaats op de autorisaties voor fysieke toegang.	
11.1.5.pg2		Papieren documenten en mobiele gegevensdragers (goedgekeurd door EU, NATO, AIVD of Defensie.) die Politie Geheime informatie bevatten worden na gebruik beveiligd opgeslagen in een kluis waar een beperkt aantal gerechtigde personen toegang tot hebben en de kluis is toegankelijk middels autorisatie. Neem in alle gevallen contact op met de cryptobeheerder voor de vertrekking van middelen.	
11.1.5.pg3		Medewerkers die zelf niet geautoriseerd zijn mogen bij hoge uitzondering en met een passende screening alleen onder toeziend oog 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 Politie Geheime informatie wordt gewerkt.	
11.1.5.pg4		Beveiligde ruimten (zoals een serverruimte of kluis) waarin zich geen personen bevinden zijn afgesloten en worden conform het controleprotocol halfjaarlijks gecontroleerd.	

BIO paragraaf 11.2: Apparatuur

Doelstelling: Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.

Politie Intern

11.2.1.pi1		Niet uitgegeven toegangsmiddelen worden opgeborgen in een afgesloten ruimte waar alleen gerechtigde personen toegang tot hebben en is toegankelijk middels autorisatie.	
11.2.4.pi1		Apparatuur (hardware zonder datadragers) behoort op correcte wijze (conform voorschrift leverancier) te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.	
11.2.9.pi1		In het clear desk-beleid staat minimaal dat de gebruiker geen gerubriceerde informatie op het bureau mag laten liggen. Deze informatie moet altijd worden opgeborgen in een afsluitbare opbergmogelijkheid (kast, locker, bureau of kamer).	
11.2.9.pi2		Bij afdrukken van gevoelige informatie wordt, gebruik gemaakt van de functie “beveiligd afdrukken” (bv. pincode verificatie of via paslezer op de printer).	
11.2.9.pi3		Na 4 uur inactiviteit wordt de sessie uitgelogd. Wil men hier van afwijken dan vindt vooraf een risicoanalyse plaats en worden eventuele risico’s gemitigeerd of geaccepteerd door daarvoor bevoegde personen.	

Politie Confidentieel

11.2.1.pc1		Niet uitgegeven toegangsmiddelen worden opgeborgen in een afgesloten ruimte waar alleen gerechtigde personen toegang tot hebben en is toegankelijk middels autorisatie.	
11.2.4.pc1		Apparatuur (hardware zonder datadragers) behoort op correcte wijze (conform voorschrift leverancier) te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.	
11.2.9.pc1		In het clear desk-beleid staat minimaal dat de gebruiker geen gerubriceerde informatie op het bureau mag laten liggen. Deze informatie moet altijd worden opgeborgen in een afsluitbare opbergmogelijkheid (kast, locker, bureau of kamer).	
11.2.9.pc2		Bij afdrukken van gevoelige informatie wordt, gebruik gemaakt van de functie “beveiligd afdrukken” (bv. pincode verificatie of via paslezer op de printer).	
11.2.9.pc3		Ontgrendeling van het systeem vindt alleen plaats via two-factor authenticatie	
11.2.9.pc4		Na 2 uur inactiviteit wordt de sessie uitgelogd. Wil men hier van afwijken dan vindt vooraf een risicoanalyse plaats en worden eventuele risico’s gemitigeerd of geaccepteerd door daarvoor bevoegde personen.	

Politie Geheim

11.2.1.pg1		Niet uitgegeven toegangsmiddelen worden opgeborgen in een kluis waar een beperkt aantal gerechtigde personen toegang tot hebben en de kluis is toegankelijk middels autorisatie.	
11.2.4.pg1		Apparatuur (hardware zonder datadragers) behoort op correcte wijze (conform voorschrift leverancier) te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.	
11.2.4.pg2		Reparatie en onderhoud van apparatuur vindt altijd op locatie plaats, tenzij het een heimelijke locatie betreft.	
11.2.4.pg3		De toegang voor onderhoud op afstand is niet toegestaan.	
11.2.4.pg4		Voor beveiliging worden componenten gebruikt, conform de lijst met de (op het juiste beveiligingsniveau) goedgekeurde middelen door EU, NATO, AIVD of Defensie.	
11.2.5.pg1		Apparatuur, informatie-(dragers) en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen, anders dan voor het veilig verwijderen van apparatuur zoals beschreven in 11.2.4.	
11.2.7.pg1		Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de Dienst ICT ingeleverd. De Dienst ICT zorgt voor een verantwoorde afvoer zodanig dat er geen data op het apparaat aanwezig of toegankelijk is door het fysiek te vernietigen (schredderen) onder toezicht van een daartoe gerechtigd persoon.	
11.2.7.pg2		Hergebruik van apparatuur die was ingezet voor de rubricering 'Politie Geheim' buiten de politie is niet toegestaan. De datadrager wordt onder toezicht fysiek vernietigd.	
11.2.7.pg3		Het vernietigen gebeurt conform het juiste niveau, vastgelegd in de 'Uitvoeringsregeling vernietiging gegevensdragers v1.0 of nieuwere versies daarvan '.	
11.2.8.pg1		Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd. Binnen Politie Geheim wordt er gebruik gemaakt van een beveiligde ruimte, uitzonderingen geschieden op basis van een risico analyse.	
11.2.9.pg1		In het clear desk-beleid staat minimaal dat de gebruiker geen informatie op het bureau mag laten liggen. Deze informatie moet altijd worden opgeborgen in een kluis.	
11.2.9.pg2		Bij afdrukken van gevoelige informatie wordt, gebruik gemaakt van de functie "beveiligd afdrukken" (bv. pincode verificatie of via paslezer op de printer), Bij Politie Geheim dient printen beperkt te worden tot het strikt noodzakelijke en de communicatie met de printer dient tevens voorzien te zijn van encryptie.	
11.2.9.pg3		Na 2 uur inactiviteit wordt de sessie uitgelogd. Wil men hier van afwijken dan vindt vooraf een risicoanalyse plaats en worden eventuele risico's gemitigeerd of geaccepteerd door daarvoor bevoegde personen.	
11.2.9.pg4		Ontgrendeling van het systeem vindt alleen plaats via two-factor authenticatie en in een beveiligde ruimte van geschikt niveau.	

BIO paragraaf 12.1: Bedieningsprocedures en verantwoordelijkheden

Doelstelling: Correcte en veilige bediening van informatie verwerkende faciliteiten waarborgen.

Politie Intern

12.1.1.pi1		Systeemdocumentatie die als Politie Intern gerubriceerd is, is niet vrij toegankelijk. Wanneer de eigenaar van de systeemdocumentatie er expliciet voor kiest om gerubriceerde systeemdocumentatie buiten het politie domein te brengen, doet hij dat niet zonder risicoafweging (conform de Rubriceringsregeling en de bijbehorende maatregelen) en toestemming van een leidinggevende.	
12.1.4.pi1		Operationele gegevens met de rubricering Politie Intern mogen niet gebruikt worden voor testdoeleinden.	

Politie Confidentieel

12.1.1.pc1		Systeemdocumentatie die als Politie Confidentieel gerubriceerd is, is niet vrij toegankelijk. Wanneer de eigenaar van de systeemdocumentatie er expliciet voor kiest om gerubriceerde systeemdocumentatie buiten het politie domein te brengen, doet hij dat niet zonder risicoafweging (conform de Rubriceringsregeling en de bijbehorende maatregelen) en toestemming van een leidinggevende.	
12.1.4.pc1		Operationele gegevens met de rubricering Politie Confidentieel mogen niet gebruikt worden voor testdoeleinden.	

Politie Geheim

12.1.1.pg1		Systeemdocumentatie die betrekking heeft op maatregelen die gerubriceerd zijn als zijnde Politie Geheim, is niet vrij toegankelijk. Wanneer de eigenaar van de systeemdocumentatie er expliciet voor kiest om gerubriceerde systeemdocumentatie buiten het politie domein te brengen, doet hij dat niet zonder risicoafweging (conform de Rubriceringsregeling en de bijbehorende maatregelen) en toestemming van een leidinggevende.	
12.1.2.pg1		De wijzigingen dienen in een afgeschermde registratie worden opgenomen, die slechts voor een beperkt aantal, daartoe gerechtigde, personen inzichtelijk/toegankelijk is.	
12.1.3.pg1		Binnen Politie Geheim zijn er geen koppelpunten met externe of onvertrouwde zones. Hierdoor zijn er impliciet maatregelen getroffen om DDOS (Denial of Service attacks) of andere Cyberaanvallen te voorkomen. Het gaat hier om aanvallen die erop gericht zijn de verwerkingscapaciteit zodanig te laten vollopen, dat onbereikbaarheid of uitval van computers het gevolg is.	
12.1.4.pg1		Operationele gegevens met de rubricering Politie Geheim mogen niet gebruikt worden voor testdoeleinden.	

BIO paragraaf 12.2: Bescherming tegen malware

Doelstelling: Waarborgen dat informatie en informatie verwerkende faciliteiten beschermd zijn tegen malware.

Politie Intern

12.2.1.pi1		In verschillende schakels van een keten binnen de infrastructuur van een organisatie wordt bij voorkeur de antivirus programmatuur van verschillende leveranciers toegepast.	
12.2.1.pi2		Intrusion detection maatregelen moeten op verschillende lagen van de infrastructuur plaats vinden, bij voorkeur gebruikmakend van verschillende leveranciers.	
12.2.1.pi3		Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt realtime en geautomatiseerd plaats	

Politie Confidentieel

12.2.1.pc1		In verschillende schakels van een keten binnen de infrastructuur van een organisatie wordt verplicht de antivirus programmatuur van verschillende leveranciers toegepast.	
12.2.1.pc2		Intrusion detection maatregelen moeten op verschillende lagen van de infrastructuur plaats vinden, bij voorkeur gebruikmakend van verschillende leveranciers.	
12.2.1.pc3		Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt realtime en automatisch plaats.	

Politie Geheim

12.2.1.pg1		In verschillende schakels van een keten binnen de infrastructuur van een organisatie wordt verplicht de antivirus programmatuur van verschillende leveranciers toegepast.	
12.2.1.pg2		Intrusion detection maatregelen moeten op verschillende lagen van de infrastructuur plaats vinden, bij voorkeur gebruikmakend van verschillende leveranciers.	
12.2.1.pg3		Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt realtime en gecontroleerd plaats en de update is niet ouder dan 24 uur.	

BIO paragraaf 12.3: Back-up

Doelstelling: Beschermen tegen het verlies van gegevens.

Politie Intern

12.3.1.pi1		Van back-upactiviteiten en de verblijfplaats van de media wordt een registratie bijgehouden in een registratie die middels autorisatie toegankelijk is, met een kopie op een andere locatie. De andere locatie is zodanig gekozen dat een incident/calamiteit op de oorspronkelijke locatie niet leidt tot schade aan of toegang tot de kopie van die registratie.	
12.3.1.pi2		Back-ups worden voorzien van encryptie bewaard op een locatie die zodanig is gekozen dat een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-up, waarbij de locatie voldoet aan de eisen voor Politie Intern.	

Politie Confidentieel

12.3.1.pc1		Van back-upactiviteiten en de verblijfplaats van de media wordt een registratie bijgehouden in een registratie die middels autorisatie toegankelijk is, met een kopie op een andere locatie. De andere locatie is zodanig gekozen dat een incident/calamiteit op de oorspronkelijke locatie niet leidt tot schade aan of toegang tot de kopie van die registratie.	
12.3.1.pc2		Back-ups worden voorzien van encryptie bewaard op een locatie die zodanig is gekozen dat een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-up, waarbij de locatie voldoet aan de eisen voor Politie Confidentieel.	

Politie Geheim

12.3.1.pg1		Van back-upactiviteiten en de verblijfplaats van de media wordt een registratie bijgehouden in een afgeschermde registratie die door een beperkt aantal, daartoe gerechtigde, personen inzichtelijk/toegankelijk is, met een kopie op een andere locatie. De andere locatie is zodanig gekozen dat een incident/calamiteit op de oorspronkelijke locatie niet leidt tot schade aan of toegang tot de kopie van die registratie.	
12.3.1.pg2		Back-ups worden off-site en voorzien van encryptie bewaard op een locatie die zodanig is gekozen dat een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-up, waarbij de locatie voldoet aan de eisen voor Politie Geheim.	

BIO paragraaf 12.4: Verslaglegging en monitoren

Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.

Politie Geheim

12.4.2.pg1		Het (automatisch) overschrijven of verwijderen van logbestanden is niet toegestaan, de capaciteit om logbestanden op te slaan dient groot genoeg te zijn.	
12.4.2.pg2		Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is sprake van functiescheiding.	

BIO paragraaf 12.6: Beheer van technische kwetsbaarheden

Doelstelling: Benutting van technische kwetsbaarheden voorkomen.

Politie Intern

12.6.1.pi1		Het SOC van de Nationale Politie zal periodiek (minimaal eens per kwartaal) op een deel van de interne infrastructuur van de Politie een kwetsbaarheden scan uitvoeren.	
12.6.1.pi2		Eventueel gevonden kwetsbaarheden door het SOC, zullen door het SOC worden voorzien van een schriftelijke analyse waarin minimaal is vastgelegd wat de ernst is van de kwetsbaarheid. Hierin worden dezelfde impact categorieën gehanteerd als voor de overige kwetsbaarheden.	
12.6.1.pi3		Termijnen en verantwoordelijkheden voor het implementeren van mitigerende maatregelen, voortkomend uit de scan van het SOC, wijzigen niet ten opzichte van extern gesignaleerde kwetsbaarheden, zoals bijvoorbeeld door het NCSC.	
12.6.1.pi4		Er is een proces ingericht voor het beheer van technische kwetsbaarheden; dit omvat minimaal jaarlijkse penetratietests, risicoanalyses van kwetsbaarheden, patching en noodmaatregelen.	
12.6.1.pi5		Indien een patch beschikbaar is, dient deze gecontroleerd te worden doorgevoerd. Zijn er risico's verbonden met de installatie van de patch dan dienen de risico's te worden vergeleken met de risico's van de kwetsbaarheid.	
12.6.1.pi6		Voor werkstations worden de patches, updates, hot-fixes gecontroleerd doorgevoerd (binnen 4 weken). Ook het patchen van niet kritische maar wel riskante systeemonderdelen (denk aan het besturingssysteem, Java, Adobe, Flash en andere actieve componenten) worden gecontroleerd doorgevoerd, hiervan vertrouwen we het testproces van de leverancier.	
12.6.1.pi7		Voor servers wordt er een onderscheid gemaakt tussen: • Zero-day zaken. Dit zijn zaken met een zeer hoge impact en waarbij er direct actief misbruik wordt gemaakt van de kwetsbaarheid: patchen binnen één dag na beschikbare patch (dit zal ook altijd een NCSC High/High zijn); • Kritische securitypatches (High/High van NCSC) patchen binnen 3 dagen na de triage, waarbij de triage binnen één dag wordt uitgevoerd; • Overige patches worden ingepland bij de eerst volgende onderhoudsronde, echter zeker binnen 4 weken na het uitbrengen van de patches door de leverancier. Daarnaast geldt ook voor servers dat alle patches worden uitgevoerd, aangezien latere patches (ook op producten van andere leveranciers) uit kunnen gaan van de aanname dat alle patches zijn aangebracht.	

12.6.1.pc1		Het SOC van de Nationale Politie zal periodiek (minimaal eens per kwartaal) op een deel van de interne infrastructuur van de Politie een kwetsbaarheden scan uitvoeren.	
12.6.1.pc2		Eventueel gevonden kwetsbaarheden door het SOC, zullen door het SOC worden voorzien van een schriftelijke analyse waarin minimaal is vastgelegd wat de ernst is van de kwetsbaarheid. Hierin worden dezelfde impact categorieën gehanteerd als voor de overige kwetsbaarheden.	
12.6.1.pc3		Termijnen en verantwoordelijkheden voor het implementeren van mitigerende maatregelen, voortkomend uit de scan van het SOC, wijzigen niet ten opzichte van extern gesignaleerde kwetsbaarheden, zoals bijvoorbeeld door het NCSC.	
12.6.1.pc4		Er is een proces ingericht voor het beheer van technische kwetsbaarheden; dit omvat minimaal jaarlijkse penetratietests, risicoanalyses van kwetsbaarheden, patching en noodmaatregelen.	
12.6.1.pc5		Indien een patch beschikbaar is, dient deze gecontroleerd te worden doorgevoerd. Zijn er risico's verbonden met de installatie van de patch dan dienen de risico's te worden vergeleken met de risico's van de kwetsbaarheid.	
12.6.1.pc6		Voor werkstations worden de patches, updates, hot-fixes gecontroleerd doorgevoerd (binnen 4 weken). Ook het patchen van niet kritische maar wel riskante systeemonderdelen (denk aan het besturingssysteem, Java, Adobe, Flash en andere actieve componenten) worden gecontroleerd doorgevoerd, hiervan vertrouwen we het testproces van de leverancier.	
12.6.1.pc7		Voor servers wordt er een onderscheid gemaakt tussen: • Zero-day zaken. Dit zijn zaken met een zeer hoge impact en waarbij er direct actief misbruik wordt gemaakt van de kwetsbaarheid: patchen binnen één dag na beschikbare patch (dit zal ook altijd een NCSC High/High zijn); • Kritische securitypatches (High/High van NCSC) patchen binnen 3 dagen na de triage, waarbij de triage binnen één dag wordt uitgevoerd; • Overige patches worden ingepland bij de eerst volgende onderhoudsronde, echter zeker binnen 4 weken na het uitbrengen van de patches door de leverancier. Daarnaast geldt ook voor servers dat alle patches worden uitgevoerd, aangezien latere patches (ook op producten van andere leveranciers) uit kunnen gaan van de aanname dat alle patches zijn aangebracht.	

12.6.1.pg1		Het SOC van de Nationale Politie zal periodiek (minimaal eens per kwartaal) op een deel van de interne infrastructuur van de Politie een kwetsbaarheden scan uitvoeren.	
12.6.1.pg2		Eventueel gevonden kwetsbaarheden door het SOC, zullen door het SOC worden voorzien van een schriftelijke analyse waarin minimaal is vastgelegd wat de ernst is van de kwetsbaarheid. Hierin worden dezelfde impact categorieën gehanteerd als voor de overige kwetsbaarheden.	
12.6.1.pg3		Termijnen en verantwoordelijkheden voor het implementeren van mitigerende maatregelen, voortkomend uit de scan van het SOC, wijzigen niet ten opzichte van extern gesignaleerde kwetsbaarheden, zoals bijvoorbeeld door het NCSC.	
12.6.1.pg4		Er is een proces ingericht voor het beheer van patches; dit omvat minimaal halfjaarlijkse penetratietests, risicoanalyses van kwetsbaarheden en patching.	
12.6.1.pg5		Indien een patch beschikbaar is, dient deze gecontroleerd te worden doorgevoerd. Zijn er risico's verbonden met de installatie van de patch dan dienen de risico's te worden vergeleken met de risico's van de kwetsbaarheid.	
12.6.1.pg6		Voor werkstations worden de patches, updates, hot-fixes gecontroleerd doorgevoerd (binnen 4 weken). Ook het patchen van niet kritische maar wel riskante systeemonderdelen (denk aan het besturingssysteem, Java, Adobe, Flash en andere actieve componenten) worden gecontroleerd doorgevoerd, hiervan vertrouwen we het testproces van de leverancier.	
12.6.1.pg7		Voor servers wordt er een onderscheid gemaakt tussen: • Zero-day zaken. Dit zijn zaken met een zeer hoge impact en waarbij er direct actief misbruik wordt gemaakt van de kwetsbaarheid: patchen binnen één dag na beschikbare patch (dit zal ook altijd een NCSC High/High zijn); • Kritische securitypatches (High/High van NCSC) patchen binnen 3 dagen na de triage, waarbij de triage binnen één dag wordt uitgevoerd; • Overige patches worden ingepland bij de eerst volgende onderhoudsronde, echter zeker binnen 4 weken na het uitbrengen van de patches door de leverancier. Daarnaast geldt ook voor servers dat alle patches worden uitgevoerd, aangezien latere patches (ook op producten van andere leveranciers) uit kunnen gaan van de aanname dat alle patches zijn aangebracht.	

BIO paragraaf 13.1: Beheer van netwerkbeveiliging

Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatie verwerkende faciliteiten waarborgen.

Politie Intern

13.1.1.pi1		Alleen geïdentificeerde en geauthentiseerde apparatuur kan worden aangesloten op een vertrouwde zone.	
13.1.1.pi2		Eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) wordt alleen aangesloten op een onvertrouwde zone.	
13.1.2.pi1		De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst. Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst dienen te worden afgesloten, hier dient minimaal jaarlijks een controle op te worden uitgevoerd en daarnaast jaarlijks over te worden gerapporteerd.	
13.1.2.pi2		Gebruik altijd de veilige variant van een protocol (zie bijlage A voor een overzicht van veilige protocollen). Gezien de toename van het aantal dreigingen van buitenaf dient hier periodiek controle op uitgevoerd te worden en gerapporteerd te worden.	
13.1.2.pi3		Het controleren van netwerkpoorten wordt ingevoerd op basis van de volgende richtlijnen: Op netwerken waarover Politie intern geclassificeerde informatie wordt gebruikt, wordt geen netwerkpoort control toegepast, tenzij de aangesloten apparatuur in een publieke ruimte is geplaatst of risicoanalyse aangeeft dat het noodzakelijk is in de betreffende omgeving.	
13.1.3.pi1		Er wordt jaarlijks geëvalueerd of de genomen maatregelen behorende bij data met de rubricering 'politie Intern' nog steeds overeenkomt met betreffende zone of dat er passende maatregelen moeten worden genomen.	

Politie Confidentieel

13.1.1.pc1		Alleen geïdentificeerde en geauthentiseerde apparatuur kan worden aangesloten op een vertrouwde zone.	
13.1.1.pc2		Eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) wordt alleen aangesloten op een onvertrouwde zone.	
13.1.2.pc1		De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst. Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst dienen te worden afgesloten, hier dient minimaal halfjaarlijks een controle op te worden uitgevoerd en daarnaast halfjaarlijks over te worden gerapporteerd	
13.1.2.pc2		Gebruik altijd de veilige variant van een protocol (zie bijlage A voor een overzicht van veilige protocollen). Gezien de toename van het aantal dreigingen van buitenaf dient hier periodiek controle op uitgevoerd te worden en gerapporteerd te worden.	
13.1.3.pc1		Er is beleid en er zijn procedures voor beheer op afstand, waarbij minimaal aandacht is voor de volgende aspecten: a. two-factor authenticatie; b. alle handelingen worden gelogd;	

		c. altijd met dataversleuteling.	
13.1.3.pc2		Er wordt halfjaarlijks geëvalueerd of de genomen maatregelen behorende bij data met de rubricering 'politie Confidentieel' nog steeds overeenkomt met betreffende zone of dat er passende maatregelen moeten worden genomen.	

Politie Geheim

13.1.1.pg1		Alleen geïdentificeerde en geauthentiseerde apparatuur kan worden aangesloten op een vertrouwde zone.	
13.1.1.pg2		Eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) wordt alleen aangesloten op een onvertrouwde zone.	
13.1.2.pg1		De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst. Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst dienen te worden afgesloten, hier dient minimaal per kwartaal een controle op te worden uitgevoerd en daarnaast per kwartaal over te worden gerapporteerd.	
13.1.2.pg2		Gebruik altijd de veilige variant van een protocol (zie bijlage A voor een overzicht van veilige protocollen). Gezien de toename van het aantal dreigingen van buitenaf dient hier periodiek controle op uitgevoerd te worden en gerapporteerd te worden.	
13.1.2.pg3		Bij transport van gerubriceerde informatie over onvertrouwde netwerken, zoals het internet, dient altijd geschikte encryptie (AES 256 of beter) gebruik makend van een door de NBV goedgekeurd middel te worden toegepast.	
13.1.2.pg4		Beheer is slechts toegestaan in ruimtes die voldoen aan de eisen voor Politie Geheim.	
13.1.3.pg1		Er wordt per kwartaal geëvalueerd of de genomen maatregelen behorende bij data met de rubricering 'politie Geheim' nog steeds overeenkomt met betreffende zone of dat er passende maatregelen moeten worden genomen.	

BIO paragraaf 13.2: Informatietransport

Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.

Politie Intern

13.2.1.pi1		Het meenemen van Politie Interne informatie buiten gecontroleerd gebied vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is.	
13.2.1.pi2		Medewerkers zijn geïnstrueerd om zodanig om te gaan met (telefoon)gesprekken, e-mail, faxen en ingesproken berichten op antwoordapparaten dat de kans op uitlekken van Politie Interne informatie wordt geminimaliseerd.	
13.2.1.pi3		Medewerkers zijn geïnstrueerd om zodanig om te gaan met mobiele apparatuur en verwijderbare media dat de kans op uitlekken van Politie Interne informatie geminimaliseerd wordt. Hierbij wordt minimaal aandacht besteed aan het risico van adreslijsten en opgeslagen boodschappen in mobiele telefoons.	
13.2.1.pi4		Het printen van Politie Interne documenten vindt uitsluitend plaats via beveiligd printen.	
13.2.1.pi5		Medewerkers zijn geïnstrueerd om beveiligd te printen en in elk geval geen vertrouwelijke documenten bij de printer te laten liggen.	
13.2.1.pi6		Er zijn maatregelen getroffen om het automatisch doorsturen van interne e-mail berichten naar externe e-mail adressen te voorkomen.	
13.2.4.pi1		Er zijn afspraken gemaakt over de beveiliging van de uitwisseling van gegevens en software tussen organisaties waarin de maatregelen om betrouwbaarheid, waaronder traceerbaarheid en onweerlegbaarheid, van gegevens te waarborgen zijn beschreven en getoetst. Een leverancier overlegt periodiek (jaarlijks) een assurance verklaring waarin de volledige scope van de dienstverlening van de politie is benoemd, hierbij moet zowel opzet, bestaan als werking worden getoetst, de verklaring dient te worden afgegeven door een onafhankelijke auditor (RE) in de vorm van een 3000 verklaring met als oordeel “een redelijke mate van zekerheid”. Indien deze verklaring niet kan worden versterkt zal een herstel periode worden afgesproken waarbinnen voldaan moet worden aan de vereisten. Wordt hierna nog niet voldaan aan het gestelde in de verklaring, dan zal de overeenkomst worden beëindigd. Er moet tevens een verwerkersovereenkomst opgesteld worden, conform de WPG.	

Politie Confidentieel

13.2.1.pc1		Het meenemen van Politie Confidentiële informatie buiten gecontroleerd gebied is alleen toegestaan indien er voldoende waarborgen worden genomen om de integriteit en vertrouwelijkheid te kunnen garanderen. De maatregelen die dan worden vereist zijn minimaal gelijkwaardig aan de maatregelen zoals die zijn benoemd in de rest van dit document. De genomen maatregelen moeten door medewerkers van de Nationale Politie of een door de Nationale Politie aangewezen onafhankelijke partij toetsbaar zijn.	
13.2.1.pc2		Medewerkers zijn geïnstrueerd om zodanig om te gaan met (telefoon)gesprekken, e-mail, faxen en ingesproken berichten op antwoordapparaten dat de kans op uitlekken van Politie Confidentiële informatie wordt geminimaliseerd.	

13.2.1.pc3		Medewerkers zijn geïnstrueerd om mobiele apparatuur en verwijderbare media met Politie Confidentiële data niet buiten gecontroleerd gebied te brengen.	
13.2.1.pc4		Het printen van Politie Confidentiële documenten vindt uitsluitend plaats via beveiligd printen in een beveiligde omgeving.	
13.2.1.pc5		Er zijn maatregelen getroffen om het automatisch doorsturen van interne e-mail berichten naar externe e-mail adressen te voorkomen.	
13.2.4.pc1		Er zijn afspraken gemaakt over de beveiliging van de uitwisseling van gegevens en software tussen organisaties waarin de maatregelen om betrouwbaarheid, waaronder traceerbaarheid en onweerlegbaarheid, van gegevens te waarborgen zijn beschreven en getoetst. Een leverancier overlegt periodiek (jaarlijks) een assurance verklaring waarin de volledige scope van de dienstverlening van de politie is benoemd, hierbij moet zowel opzet, bestaan als werking worden getoetst, de verklaring dient te worden afgegeven door een onafhankelijke auditor (RE) in de vorm van een 3000 verklaring met als oordeel “een redelijke mate van zekerheid”. Indien deze verklaring niet kan worden versterkt zal een herstel periode worden afgesproken waarbinnen voldaan moet worden aan de vereisten. Wordt hierna nog niet voldaan aan het gestelde in de verklaring, dan zal de overeenkomst worden beëindigd. Er moet tevens een verwerkersovereenkomst opgesteld worden, conform de WPG.	

Politie Geheim

13.2.1.pg1		Het meenemen van Politie Geheime informatie buiten gecontroleerd gebied is niet toegestaan, uitzonderingen slechts per gebeurtenis met passende middelen, waarbij er toestemming wordt verleend door de data eigenaar.	
13.2.1.pg2		Medewerkers zijn geïnstrueerd om zodanig om te gaan met (telefoon)gesprekken, e-mail, faxen en ingesproken berichten op antwoordapparaten dat de kans op uitlekken van Politie Geheime informatie wordt geminimaliseerd.	
13.2.1.pg3		Het printen van Politie Geheime documenten vindt uitsluitend plaats via beveiligd printen in afgesloten ruimten door geautoriseerde personen.	
13.2.1.pg4		Vanuit Politie Geheim vindt er geen e-mail verkeer plaats naar lager gerubriceerde omgevingen.	
13.2.4.pg1		Er zijn afspraken gemaakt over de beveiliging van de uitwisseling van gegevens en software tussen organisaties waarin de maatregelen om betrouwbaarheid, waaronder traceerbaarheid en onweerlegbaarheid, van gegevens te waarborgen zijn beschreven en getoetst. Een leverancier overlegt periodiek (jaarlijks) een assurance verklaring waarin de volledige scope van de dienstverlening van de politie is benoemd, hierbij moet zowel opzet, bestaan als werking worden getoetst, de verklaring dient te worden afgegeven door een onafhankelijke auditor (RE) in de vorm van een 3000 verklaring met als oordeel “een redelijke mate van zekerheid”. Indien deze verklaring niet kan worden versterkt zal een herstel periode worden afgesproken waarbinnen voldaan moet worden aan de vereisten. Wordt hierna nog niet voldaan aan het gestelde in de verklaring, dan zal de overeenkomst worden beëindigd. Er moet tevens een verwerkersovereenkomst opgesteld worden, conform de WPG.	

BIO paragraaf 14.2: Beveiliging in ontwikkelings- en ondersteunende processen

Doelstelling: Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.

Politie Intern

14.2.7.pi1		Het eigenaarschap van gegevens en programmatuur en de verantwoordelijkheid voor de gegevensbescherming, auteursrechten, licenties van programmatuur zijn vastgelegd. Er is een ESCROW regeling voor maatwerkprogrammatuur én licenties zijn te meten.	

Politie Confidentieel

14.2.7.pc1		Het eigenaarschap van gegevens en programmatuur en de verantwoordelijkheid voor de gegevensbescherming, auteursrechten, licenties van programmatuur zijn vastgelegd. Er is een ESCROW regeling voor maatwerkprogrammatuur én licenties zijn te meten.	

Politie Geheim

14.2.7.pg1		Het eigenaarschap van gegevens en programmatuur en de verantwoordelijkheid voor de gegevensbescherming, auteursrechten, licenties van programmatuur zijn vastgelegd. Er is een ESCROW regeling voor maatwerkprogrammatuur én licenties zijn te meten.	

BIO paragraaf 15.1: Informatiebeveiliging in leveranciers-relaties

Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.

Politie Intern

15.1.2.pi1		Uitbesteding is mogelijk, maar dan alleen ná een risicoanalyse en zoals vastgelegd in de Visie op Sourcing ICT-Voorzieningen.	

Politie Confidentieel

15.1.2.pc1		Uitbesteding is mogelijk, maar dan alleen ná een risicoanalyse en zoals vastgelegd in de Visie op Sourcing ICT-Voorzieningen.	
15.1.2.pc2		De in dienstverleningscontracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld met audits of rapportages en gebeurt halfjaarlijks.	

Politie Geheim

15.1.2.pg1		De dienstverlening van systemen met Politie Geheime informatie wordt niet door een derde partij geëxploiteerd.	

Bijlage A: Lijst met veilige en onveilige protocollen

(Onveilige) variant	Verbeterde (veiligere) variant / Versie(s) / Standaard poort
HTTP / / 80	HTTPS / / 443 (gebruikt *TLS) in combinatie met HSTS
FTP / / 20	SFTP / / 22 (gebruikt SSH 0.4.3)
IMAP / 143	IMAP over *TLS / 993
TELNET / / 23	SSH / vanaf 0.4.3 / 22
RLOGIN / / 513	SSH / vanaf 0.4.3 / 22
RSH / / 514	SSH / vanaf 0.4.3 / 22
REXEC / / 512	SSH / vanaf 0.4.3 / 22
SNMP v1, v2 / / 161	SNMPv3 / V3 / 161
SMTP open relay / / 25	Politie Berichten Dienst (voorkeur), SMTP relay alleen intern en vanaf vooraf gedefinieerde IP adressen / / 587 als alternatieve poort
Simple Binds, LDAP / 3268, 389	LDAP over *TLS (LDAPS) / 389
POP3 / 110	POP3S, POP3 over *TLS / 995
NFSv3 / / 111, 2049	NFSv4 / V4 / 111, 2049
SMBv1 / 445	SMBv3 waar mogelijk, anders minimaal SMBv2, Bij SMBv2 alleen via IPSec tunnel, WEBDAV over *TLS / 445
DNS	DNSSEC
Onversleutelde database connecties tussen machines, in het bijzonder Oracle connecties (Oracle Net Services protocol)	De database connecties dienen geüpgrade te worden naar veilige varianten die door de leverancier worden aanbevolen. In geval van Oracle dient minstens gebruik te worden gemaakt van symmetrische Oracle versleuteling. Indien mogelijk heeft *TLS 1.3 versleuteling de voorkeur.
IPV4	IPV4 én IPV6 (Dualstack)

Overige verplichte standaarden zijn te vinden in de lijst open standaarden van het forum standaardisatie:
https://www.forumstandaardisatie.nl/open-standaarden

* Recentere versies van TLS zijn veiliger dan oudere versies.
De oudste drie versies van TLS (SSL 1.0, SSL 2.0 en SSL 3.0) zijn niet veilig in het gebruik.
De beste bescherming wordt geboden door de meest recente versie van TLS: TLS 1.3.

Versie	Status
TLS 1.3	**Goed**
TLS 1.2	
TLS 1.1	**Uit te faseren**
SSL 3.0	
SSL 2.0	**Onvoldoende**
SSL 1.0	

Bron: NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security v2, d.d. 23-04-2019