Samen aanjagen van vernieuwing

BIS

Baseline Informatiebeveiliging SURF

Auteur(s) : CISO-team

Versie : 1.2
Datum : April 2023
Kenmerk : Baseline Informatiebeveiliging SURF (BIS)

Inhoudsopgave

1 Informatiebeveiliging SURF

1.1 Inleiding en scope

Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatie-systemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit en het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.

De Baseline Informatiebeveiliging SURF (hierna BIS) is een kader met maatregelen voor de beveiliging van de informatie(systemen). Het doel van de BIS is een minimaal beveiligingsniveau te bepalen waar heel SURF aan moet voldoen. Dit zorgt in de basis voor een betrouwbare en professionele dienstverlening en informatievoorziening.

De BIS is van toepassing op de gehele SURF-organisatie. De BIS omvat alle organisatorische en technische maatregelen waar zowel de organisatie in zijn geheel als alle diensten en systemen waar informatie wordt verwerkt, aan moeten voldoen.

1.2 Informatiebeveiligingskaders en uitgangspunten

De BIS vormt een integraal onderdeel van het informatieveiligheidsbeleid van SURF. Bij tegenstrijdigheden met andere documenten in de baseline prevaleert de BIS.

Als basis voor de BIS gelden de volgende normen, kaders en documenten:

- Baseline Informatiebeveiliging Overheid (BIO)
- Informatieveiligheidsbeleid SURF
- ISO 27001 en ISO 27002
- Algemene Verordening Gegevensverwerking
- SURF Juridisch Normenkader (Cloud)Services
- Overige wet- en regelgeving, zoals de AVG

Er is rekening gehouden met het privacybeleid van SURF en bijbehorende procedures en maatregelen. In de BIS ligt de focus op de benodigde securitymaatregelen om verwerkingen van persoonsgegevens volgens AVG adequaat te beveiligen, inclusief het verwerken van bijzondere persoonsgegevens.

Samengevat geldt voor de BIS het volgende:

- Het lijnmanagement is verantwoordelijk voor informatieveiligheid en de beveiliging van informatie(systemen).
- Het lijnmanagement stelt de classificatie op informatie in haar systemen vast voor de aspecten betrouwbaarheid, integriteit en vertrouwelijkheid (zie hoofdstuk 3, Classificatie).
- De classificatie is bepalend voor de beveiligingseisen waaraan het systeem moet voldoen (volgens het principe ‘pas toe of leg uit’).
- Op basis van de classificatie implementeert het lijnmanagement de maatregelen en draagt deze uit
- Informatiebeveiliging is een cyclisch proces volgens de PDCA-cyclus (Plan-Do-Check-Act).

1.3 Evaluatie en bijstelling

Door de ontwikkelingen van de techniek kunnen de maatregelensets voor informatiebeveiliging snel verouderen. De BIS is daarom zoveel mogelijk op een abstractieniveau geschreven zodat dit soort ontwikkelingen zo weinig mogelijk impact hebben op de inhoud: de BIS beschrijft het wat en niet het hoe. Procedures en richtlijnen voor operationele implementatie zijn dus niet verwerkt in de BIS.

Desondanks kan het voorkomen dat wijzigingen moeten worden doorgevoerd, bijvoorbeeld door wijzigingen in onderliggende wet- en regelgeving, nieuwe of vernieuwde beleidsrichtlijnen, ISO-norm of nieuwe dreigingen en kwetsbaarheden, etc. Dit document wordt daarom regelmatig, minimaal jaarlijks, in zijn geheel geëvalueerd en zo nodig geactualiseerd. Om de praktische toepasbaarheid te vergroten, wordt hierbij ook gecontroleerd of er eventueel wijzigingen/aan-vullingen in de maatregelen en de (operationele) procedures en richtlijnen noodzakelijk of gewenst zijn.

2 De BIS-maatregelen

2.1 ISO 27001-controls als basis

De ISO 27002-standaard kan gezien worden als een specificatie van de ISO 27001-standaard. De ISO 27002-standaard (2018) helpt als een praktische richtlijn om informatiebeveiligings-maatregelen te bepalen voor beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening. Deze ISO-standaard bestaat uit 114 controls (beveiligingsdoelstellingen).

De lijst met beheersmaatregelen volgt deze standaard en hoort bij dit document. In de bijlage is een overzicht van de BIS-maatregelenlijst opgenomen. Vanuit praktisch oogpunt is de lijst ook via intranet beschikbaar gesteld.

2.2 Rollen en verantwoordelijkheid

De Raad van Bestuur van SURF is eindverantwoordelijk voor de integrale beveiliging en de inrichting en werking van de beveiligingsorganisatie. In die hoedanigheid is de Raad van Bestuur van SURF eindverantwoordelijk voor de implementatie van alle beveiligingskaders in de organisatie, dus ook voor een juiste toepassing van de BIS.

Het SURF-informatieveiligheidsbeleid regelt dat het lijnmanagement verantwoordelijk is voor de vaststelling dat de getroffen maatregelen aantoonbaar overeenstemmen met de beveiligingseisen en dat ze worden nageleefd.

De dienstverantwoordelijke of de eventueel toegewezen proceseigenaar is verantwoordelijk voor het nemen van beslissingen over de classificatie. Dat bepaalt het vereiste niveau van informatiebeveiliging voor diensten en verwerkingen van informatie. Daarbij wordt rekening gehouden met de classificatie van de te verwerken gegevens door te bepalen voor welke informatie de dienst geschikt moet zijn (zie hoofdstuk 3).

In de BIS is voor diensten een indeling gemaakt op twee rollen qua verantwoordelijkheid voor implementatie van beveiligingsmaatregelen. Bij iedere control is aangegeven wie voor de implementatie van de beveiligingsmaatregel moet zorgen. In sommige gevallen is dat de diensteigenaar, in andere gevallen zorgt SURF centraal voor de implementatie van de beveiligingsmaatregel.

3 Classificatie

3.1 Informatie- en geschiktheidsclassificatie

Door gegevens te classificeren, wordt duidelijk welk beveiligingsniveau vereist is voor beschikbaarheid en integriteit & vertrouwelijkheid (B en IV). De classificatie is bij SURF onderverdeeld in twee onderdelen:

1. Informatieclassificatie - interne gegevens van SURF krijgen een classificatie die duidelijk maakt over welke soort informatie het gaat.
   Bijvoorbeeld 'financiële informatie' of 'personeelsinformatie'.
2. Geschiktheidsclassificatie - SURF-diensten krijgen een aanduiding waaruit blijkt voor welke soort informatie de dienst geschikt is.
   Bijvoorbeeld: SURF-dienst NAAM is geschikt voor gegevens met een classificatie Basis (B)/Hoog (IV).

Instellingen zijn zelf verantwoordelijk om te toetsen of hun eigen gegevensclassificatie en bijbehorende controlemaatregelen vergelijkbaar zijn met de geschiktheidsclassificatie van SURF.

Voor SURF intern geldt dat gegevens uitsluitend in informatiesystemen met de juiste geschiktheidsclassificatie mogen worden verwerkt.

3.2 Classificatiemodel

De classificatie bepaalt welke beheersmaatregelen moeten worden getroffen. We kiezen voor een eenvoudig model waarvan de toepasbaarheid groot is. De beveiligingsmaatregelen voor integriteit en vertrouwelijkheid zijn vergelijkbaar, beide aspecten zijn daarom samengevoegd. Er zijn vier aanduidingen voor het risiconiveau in combinatie tussen Beschikbaarheid en Integriteit & Vertrouwelijkheid mogelijk:

Basis|basis, basis|hoog, hoog|basis, hoog|hoog

Beschikbaarheid (B)	**Integriteit & vertrouwelijkheid (IV)**
BASIS Algeheel verlies of niet beschikbaar zijn gedurende langer dan **1 werkdag** brengt merkbare schade toe aan de belangen van gebruiker en organisatie.	BASIS Het bedrijfsproces staat enkele tot **weinig integriteits-fouten** toe. Informatie toegankelijk voor beperkte tot grote groep gebruikers. Informatie is **openbaar tot vertrouwelijk** en kan persoonsgegevens bevatten.
HOOG Algeheel verlies of niet beschikbaar zijn gedurende langer dan **2 uur** brengt aanzienlijke schade toe aan de belangen van gebruiker en organisatie.	HOOG Het bedrijfsproces staat **geen integriteitsfouten** toe. Informatie alleen toegankelijk voor specifieke personen. De informatie is **zeer vertrouwelijk of sensitief** en kan gevoelige of bijzondere persoonsgegevens bevatten. Het onbedoeld openbaar

Beschikbaarheid (B)	Integriteit & vertrouwelijkheid (IV)
	worden buiten deze groep brengt grote schade toe aan de belangen van gebruiker en organisatie.

3.3 Pas toe of leg uit

De verantwoordelijke voor een dienst of verwerking zorgt voor een registratie van de BIS-maatregelen waaraan niet of nog niet geheel kan worden voldaan, waarom (nog) niet kan worden voldaan, inclusief een inclusief toelichting op de daaruit voortvloeiende risico's. Dit is de verantwoording (ook wel 'explain') volgens het 'pas toe of leg uit'-principe. Zulke risico's moeten formeel worden geaccepteerd (tenzij de geschatte impact laag is). In de risicoacceptatie-matrix in het informatieveiligheidsbeleid is vastgelegd wie – afhankelijk van de geschatte impact – formeel risico's mag accepteren als maatregelen niet in lijn met de BIS worden geïmple-menteerd.

Er geldt een hardheidsbepaling: als een control voor een specifiek geval niet van toepassing kan zijn, is de control niet van toepassing. Dit geldt bijvoorbeeld voor een control die betrekking heeft op een externe koppeling, terwijl het betreffende informatiesysteem geen externe koppeling heeft. De risicoafweging die hieraan ten grondslag ligt ('pas toe of leg uit') moet worden vastgelegd.

Voor de meeste controls is een nadere uitwerking van de maatregelen opgenomen. Deze maatregelen dekken niet altijd de gehele beveiligingsdoelstellingen van de control af. Ook hier een hardheidsbepaling: als een maatregel voor een specifiek geval niet van toepassing kan zijn, vervalt de verplichting. De risicoafweging die hieraan ten grondslag ligt ('pas toe of leg uit') moet worden vastgelegd.

Bij gestapelde diensten binnen SURF kunnen explains een verschil in bescherming tot gevolg hebben. Hierdoor ontstaat een risico voor de verwerkte (en gedeelde) informatie. Voor een dienst die gebruikmaakt van andere SURF-diensten bepaalt de laagste geschiktheidsclassificatie van de subdienst in de keten de maximale geschiktheidsclassificatie (de zwakste schakel bepaalt de maximale sterkte). Diensten waarvoor explains zijn geregistreerd, moeten daarom onderling afstemming zoeken. Het doel van die afstemming is om samen passende maatregelen of tijdelijke maatregelen te treffen die het risico mitigeren of verkleinen zolang de explains niet volgens de BIS geïmplementeerd zijn.

4 Begripsbepalingen

AVG	Algemene verordening gegevensbescherming van 27 april 2016
Comply or explain	het principe van ‘pas toe of leg uit’ zoals bedoeld in het informatieveiligheidsbeleid van SURF
Control	een beheersmaatregel zoals bedoeld in de ISO 27001/ISO 27002
Informatiesysteem	een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur en de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie
ISO 27002	de ISO 27002 ‘Code voor informatiebeveiliging’ geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie
Procedures	concrete stapsgewijze aanwijzingen hoe bepaalde taken of acties uitgevoerd moeten worden, deze hebben een verplicht karakter
Richtlijnen	aanbevelingen in het kader van de bedrijfsvoering die geen verplichtend karakter hebben en niet essentieel zijn voor de werking van een stelsel; een richtlijn geeft een voorbeeld van hoe bepaalde normen, standaarden, technieken of maatregelen te implementeren of te hanteren zijn en kan meer specifiek zijn toegesneden op een team of op een bepaald aandachtsgebied
Standaard	standaardmaatregelen die verplicht zijn om uit te voeren

5 Baseline Informatiebeveiliging SURF - 2023

BIS - Hoofdstukoverzicht

Hieronder zie je het overzicht van de BIS-controls en -maatregelen (startend met 5 volgens de ISO-nummering). De complete lijst vind je in het Information Security Management System (ISMS) van SURF.

5. Informatieveiligheidsbeleid
5.1 Aansturing door de directie van de informatiebeveiliging

6. Organiseren van informatiebeveiliging
6.1 Interne Organisatie
6.2 Mobiele apparatuur en telewerken

7. Veilig personeel
7.1 Voorafgaand aan het dienstverband
7.2 Tijdens het dienstverband
7.3 Beëindiging en wijziging van dienstverband

8. Beheer van bedrijfsmiddelen
8.1 Verantwoordelijkheid voor bedrijfsmiddelen
8.2 Informatieclassificatie
8.3 Behandelen van media

9. Toegangsbeveiliging
9.1 Bedrijfseisen voor toegangsbeveiliging
9.2 Beheer van toegangsrechten van gebruikers
9.3 Verantwoordelijkheden van gebruikers
9.4 Toegangsbeveiliging van systeem en toepassing

10. Cryptografie
10.1 Cryptografische beheersmaatregelen

11. Fysieke beveiliging en beveiliging van de omgeving
11.1 Beveiligde gebieden
11.2 Apparatuur

12. Beveiliging Bedrijfsvoering
12.1 Bedieningsprocedures en verantwoordelijkheden
12.2 Bescherming tegen malware
12.3 Back-up en restore
12.4 Verslaglegging en monitoren
12.5 Beheersing van operationele software
12.6 Beheer van technische kwetsbaarheden
12.7 Overwegingen betreffende audits van informatiesystemen

13. Communicatiebeveiliging
13.1 Beheer van netwerkbeveiliging
13.2 Informatietransport

14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen
14.1 Beveiligingseisen voor informatiesystemen
14.2 Beveiliging in ontwikkelings- en ondersteunende processen
14.3 Testgegevens

15. Leveranciersrelaties
15.1 Informatiebeveiliging in leveranciersrelaties
15.2 Beheer van dienstverlening van leveranciers

16. Beheer van informatiebeveiligingsincidenten
16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen

17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
17.1 Informatiebeveiligingscontinuïteit
17.2 Redundante componenten

18. Naleving
18.1 Naleving van wettelijke en contractuele eisen
18.2 Informatiebeveiligingsbeoordelingen

BIS – Lijst met beheersmaatregelen

Blauw zijn de ISO-controls die we bij SURF als hoofd-beheersmaatregel gebruiken
Groen zijn de uitwerkingen van de maatregelen op niveau 'basis'
Oranje zijn de uitwerkingen van de maatregelen op niveau 'hoog'

V1.2 - 13-04-2023

Hoofdstuk 5 – Informatiebeveiligingsbeleid

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Beleidsregels voor informatiebeveiliging	5.1.1		Beleidsregels voor informatiebeveiliging – Voor informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door het bestuur, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	BIV-Basis
Beleidsregels voor informatiebeveiliging		5.1.1.1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat ten minste de volgende punten: a. de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; b. de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden; c. de toewijzing van de verantwoordelijkheden voor ketens van Informatiesystemen aan lijnmanagers; d. de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn; e. de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd; f. de bevordering van het beveiligingsbewustzijn.	BIV-Basis
Beleidsregels voor informatiebeveiliging		5.1.1.2	Per verwerking, waar nodig, aanvullend beleid voor specifieke gegevens op niveau hoog.	IV-Hoog
Beleidsregels voor informatiebeveiliging	5.1.2		Beoordeling van het informatiebeveiligingsbeleid – Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	BIV-Basis
Beleidsregels voor informatiebeveiliging		5.1.2.1	Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of bij belangrijke wijzigingen als gevolg van reorganisatie of verandering in de verantwoordelijkheidsverdeling, beoordeeld en zo nodig bijgesteld.	BIV-Basis
Beleidsregels voor informatiebeveiliging		5.1.2.2	Aanvullend beleid wordt minimaal een keer per jaar, of bij belangrijke wijzigingen als gevolg van reorganisatie of verandering in de verantwoordelijkheidsverdeling, beoordeeld en zo nodig bijgesteld.	IV-Hoog

Hoofdstuk 6 – Organiseren van informatiebeveiliging

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Interne Organisatie	6.1.1		Rollen en verantwoordelijkheden bij informatiebeveiliging – Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Interne Organisatie		6.1.1.1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging.	BIV-Basis
Interne Organisatie		6.1.1.2	De rol en verantwoordelijkheden van de Corporate Information Security Officer (CISO) zijn vastgelegd in een CISO-functieprofiel.	BIV-Basis
Interne Organisatie		6.1.1.3	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	BIV-Basis
Interne Organisatie	6.1.2		Scheiding van taken – Conflicterende taken en verantwoordelijkheden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	BIV-Basis
Interne Organisatie		6.1.2.1	Bij kritische processen wordt bij de toekenning van verantwoordelijkheden ten aanzien van eindverantwoordelijkheid, eigenaarschap en uitvoering gelet op strikte functiescheiding.	BIV-Basis
Interne Organisatie		6.1.2.2	Er is een autorisatieproces voor toekenning van bevoegdheden geformuleerd inclusief registratie van toegekende bevoegdheden, zodat er aanvullende controle is of de aangevraagde bevoegdheden passen bij de rol die de medewerker vervult in de organisatie.	BIV-Basis
Interne Organisatie		6.1.2.3	Functiescheiding wordt strikt toegepast bij wijzigingen aan security-devices.	BIV-Basis
Interne Organisatie		6.1.2.4	Voor verkrijging van toegang tot systemen en toekennen van privileges wordt sterk gelet op welke privileges bij welke rollen worden betrokken, waarbij in de kritische processen het vierogenprincipe geldt, zodat verschillende personen betrokken zijn bij de uitvoering van kritische werkzaamheden.	IV-Hoog
Interne Organisatie		6.1.2.5	Bij functiescheiding wordt ook gekeken naar betrokkenheid bij specifieke verwerkingen in combinatie met eventuele conflicterende werkzaamheden. Deze worden waar vereist, vanuit het specifieke beleid, strikt toegepast.	IV-Hoog
Interne Organisatie	6.1.3		Contact met overheidsinstanties – Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	BIV-Basis
Interne Organisatie		6.1.3.1	Er is door de organisatie uitgewerkt wie met welke (overheids) instanties en toezichthouders contact heeft voor informatiebeveiligingsaangelegenheden (vergunningen/incidenten/ calamiteiten).	BIV-Basis
Interne Organisatie		6.1.3.2	Het contactoverzicht wordt jaarlijks geactualiseerd.	IV-Hoog
Interne Organisatie	6.1.4		Contact met speciale belangengroepen – Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	BIV-Basis
Interne Organisatie		6.1.4.1	Er is door de organisatie uitgewerkt wie met welke belangengroepen contact heeft.	BIV-Basis
Interne Organisatie	6.1.5		Informatiebeveiliging in projectbeheer – Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.	BIV-Basis
Interne Organisatie		6.1.5.1	Security moet in projecten zijn gewaarborgd door het principe 'Security by Design'.	BIV-Basis
Mobiele apparatuur en telewerken	6.2.1		Beleid voor mobiele apparatuur – Om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren, moeten beleid en ondersteunende beveiligingsmaatregelen worden vastgesteld.	BIV-Basis
Mobiele apparatuur en telewerken		6.2.1.1	Mobiele apparatuur (zoals een laptop, tablet en smartphone) is zo ingericht dat: a. de toegang tot de device is beschermd met een toegangsbeveiligingsmechanisme, en b. de gegevens op de ingebouwde opslag-devices zijn beschermd door middel van versleuteling.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Mobiele apparatuur en telewerken		6.2.1.2	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: a. in bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde; b. het device maakt onderdeel uit van patchmanagement en hardening; c. het device wordt waar mogelijk beheerd en beveiligd via een MDM Mobile Device Management (MDM)-oplossing; d. bedrijfsgegevens op mobile device moeten op afstand gewist kunnen worden via de MDM-oplossing. e. gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt; f. periodiek wordt getoetst of de punten in lid b, c en d worden nageleefd.	BIV-Basis
Mobiele apparatuur en telewerken	6.2.2		Werken op afstand – Voor de beveiliging van informatie die van buiten SURF-locaties wordt benaderd, verwerkt of opgeslagen, moeten beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd	BIV-Basis

Hoofdstuk 7 – Veilig personeel

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Voorafgaand aan het dienstverband	7.1.1		Screening – Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	BIV-Basis
Voorafgaand aan het dienstverband		7.1.1.1	Bij de aanstelling van nieuw personeel worden identiteitspapieren, diploma's en certificaten geverifieerd.	BIV-Basis
Voorafgaand aan het dienstverband		7.1.1.2	Als voor de functie een Verklaring Omtrent het Gedrag (VOG) vereist is, moet de medewerker deze bij indiensttreding overleggen.	BIV-Basis
Voorafgaand aan het dienstverband		7.1.1.3	Voor specifieke projecten en gevoelige dataverwerkingen op risiconiveau hoog wordt overwogen of een zwaardere VOG of andere screeningsmaatregelen nodig zijn. Dit wordt in het aanvullende beleid vastgelegd.	IV-Hoog
Voorafgaand aan het dienstverband	7.1.2		Arbeidsvoorwaarden – De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.	BIV-Basis
Voorafgaand aan het dienstverband		7.1.2.1	Het arbeidsvoorwaardenreglement wordt aan elke nieuwe medewerker verstrekt als onderdeel van de getekende arbeidsovereenkomst.	BIV-Basis
Voorafgaand aan het dienstverband		7.1.2.2	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.	BIV-Basis
Tijdens het dienstverband	7.2.1		Bestuursverantwoordelijkheden – Het bestuur moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	BIV-Basis
Tijdens het dienstverband		7.2.1.1	Er is aansluiting bij een klokkenluidersregeling, zodat iedereen in staat is om anoniem en veilig beveiligingsissues te melden.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Tijdens het dienstverband	7.2.2		Bewustzijn, opleiding en training over informatiebeveiliging – Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	BIV-Basis
Tijdens het dienstverband		7.2.2.1	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.	BIV-Basis
Tijdens het dienstverband		7.2.2.2	Alle medewerkers en contracten worden via awareness-trainingen, presentaties en/of campagnes bijgeschoold.	BIV-Basis
Tijdens het dienstverband		7.2.2.3	Alle medewerkers en contractanten die gebruikmaken van de Informatie-systemen- en diensten hebben binnen twee maanden na indiensttreding een introductie 'informatiebeveiliging' gevolgd.	BIV-Basis
Tijdens het dienstverband		7.2.2.4	Het lijnmanagement benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij haar medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen	BIV-Basis
Tijdens het dienstverband		7.2.2.5	De medewerkers die betrokken zijn bij verwerkingen van niveau hoog worden door de leidinggevende expliciet en gedetailleerd geïnformeerd over de hogere niveau van eisen met betrekking tot de verwerkingen van risiconiveau hoog en hun verantwoordelijkheden daarin.	IV-Hoog
Tijdens het dienstverband	7.2.3		Disciplinaire procedure – Er moet een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	BIV-Basis
Tijdens het dienstverband		7.2.3.1	Het arbeidsvoorwaardenpakket bevat disciplinaire maatregelen die onder andere verband houden met en toegepast kunnen worden in geval van overtredingen van de security-beleidsnormen en -maatregelen.	BIV-Basis
Tijdens het dienstverband		7.2.3.2	In relevante documenten wordt verwezen naar de disciplinaire maatregelen zodat medewerkers op de hoogte zijn van het bestaan van deze maatregelen en zodat deze toegepast kunnen worden bij overtredingen.	BIV-Basis
Tijdens het dienstverband		7.2.3.3	Bij specifieke projecten en gevoelige dataverwerkingen op classificatie hoog (voor vertrouwelijkheid en integriteit) wordt een explicietere koppeling gemaakt tussen de rol die de medewerker vervult ten aanzien van deze verwerkingen en de disciplinaire maatregelen. Er moet meegedeeld worden dat de drempel om over te gaan tot toepassing van disciplinaire maatregelen lager ligt vanwege de aard van de verwerkingen en de gevoeligheid van verwerkte gegevens	IV-Hoog
Beëindiging en wijziging van dienstverband	7.3.1		Beëindiging of wijziging van verantwoordelijkheden van het dienstverband – Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en moeten ten uitvoer worden gebracht.	BIV-Basis
Beëindiging en wijziging van dienstverband		7.3.1.1	Voor beëindiging en wijziging van dienstverband moeten procedures zijn opgesteld waarin beschreven staat hoe verantwoordelijken en rechten worden overgedragen. De procedure moet ten minste de volgende aspecten bevatten: a. overdracht van sleutels, pasjes en dergelijk; b. overdracht van rollen en rechten; c. overdracht van gegevens; d. verwijderen van bedrijfsgegevens van niet door SURF beheerde ICT-middelen; e. overdracht van SURF beheerde ICT-middelen. De procedures moeten minimaal jaarlijks worden gecontroleerd.	BIV-Basis

Hoofdstuk 8 – Beheer van bedrijfsmiddelen

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Verantwoordelijkheid voor bedrijfsmiddelen	8.1.1		Inventariseren van bedrijfsmiddelen – Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd en er moet een inventaris van deze bedrijfsmiddelen worden opgesteld en onderhouden.	BIV-Basis
Verantwoordelijkheid voor bedrijfsmiddelen		8.1.1.1	De bedrijfsmiddelen moeten worden bijgehouden via een Asset Management-proces.	BIV-Basis
Verantwoordelijkheid voor bedrijfsmiddelen		8.1.1.2	In het Asset Management-systeem wordt duidelijk genoteerd welke systemen tot classificatie hoog (voor vertrouwelijkheid en integriteit) moeten.	IV-Hoog
Verantwoordelijkheid voor bedrijfsmiddelen	8.1.2		Eigendom van bedrijfsmiddelen – Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, moeten een eigenaar hebben.	BIV-Basis
Verantwoordelijkheid voor bedrijfsmiddelen		8.1.2.1	De eigenaar is verantwoordelijk voor de lifecycle van de asset, ongeacht waar deze fysiek wordt uitgevoerd (inclusief cloud). Minimaal de volgende aspecten zijn hiervan onderdeel: installeren, beheren, up-to-date houden en beveiliging van de asset, uitfaseren van de asset.	BIV-Basis
Verantwoordelijkheid voor bedrijfsmiddelen	8.1.3		Aanvaardbaar gebruik van bedrijfsmiddelen – Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	BIV-Basis
Verantwoordelijkheid voor bedrijfsmiddelen		8.1.3.1	Aanvaardbaar gebruik van de bedrijfsmiddelen dient te zijn vastgesteld en eenvoudig toegankelijk te zijn.	BIV-Basis
Verantwoordelijkheid voor bedrijfsmiddelen		8.1.3.2	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.	BIV-Basis
Verantwoordelijkheid voor bedrijfsmiddelen		8.1.3.3	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels.	BIV-Basis
Verantwoordelijkheid voor bedrijfsmiddelen	8.1.4		Teruggeven van bedrijfsmiddelen – Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben, teruggeven bij beëindiging van hun dienstverband, contract of overeenkomst.	BIV-Basis
Informatieclassificatie	8.2.1		Classificatie van informatie – Informatie moet orden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	BIV-Basis
Informatieclassificatie		8.2.1.1	De informatie in alle Informatie-systemen is via een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.	BIV-Basis
Informatieclassificatie	8.2.2		Informatie labelen – Om informatie te labelen moet er een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Informatieclassificatie	8.2.3		Behandelen van bedrijfsmiddelen – Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	BIV-Basis
Behandelen van media	8.3.1		Beheer van verwijderbare media – Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	BIV-Basis
Behandelen van media		8.3.1.1	Alle verwijderbare media die in voorraad aanwezig is, moeten op een locatie worden bewaard die alleen toegankelijk is voor bevoegden.	BIV-Basis
Behandelen van media		8.3.1.2	Verwijderbare media worden niet gebruikt voor extern transport van informatie.	BIV-Basis
Behandelen van media		8.3.1.3	Voor printen wordt gebruikgemaakt van printers met authenticatie.	BIV-Basis
Behandelen van media		8.3.1.4	Voor het vernietigen van prints zijn er papiervernietigers of beveiligde papiercontainers.	BIV-Basis
Behandelen van media	8.3.2		Verwijderen van media – Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	BIV-Basis
Behandelen van media		8.3.2.1	Om alle data op het medium te wissen, wordt de data onherstelbaar verwijderd. Dat gebeurt bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is.	BIV-Basis
Behandelen van media		8.3.2.2	Er is een certificaat van vernietiging verplicht als een externe partij het wissen van datadragers en/of data verzorgt.	BIV-Basis
Behandelen van media		8.3.2.3	Media die vertrouwelijke informatie bevatten, zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden. Verwijdering vindt plaats op een veilige manier, bijvoorbeeld door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van de gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie (referentie ISO 27002, implementatierichtlijn 8.3.2.a).	IV-Hoog
Behandelen van media	8.3.3		Het gebruik van koeriers of transporteurs voor vertrouwelijk of hoger geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.	BIV-Basis
Behandelen van media		8.3.3.1	Er is beleid voor fysiek transport van media vastgesteld.	IV-Hoog
Behandelen van media		8.3.3.2	Het gebruik van koeriers of transporteurs voor vertrouwelijk of hoger geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.	IV-Hoog

Hoofdstuk 9 - Toegangsbeveiliging

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Bedrijfseisen voor toegangsbeveiliging	9.1.1		Beleid voor toegangsbeveiliging – Er moet een beleid voor toegangsbeveiliging worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging	9.1.2		Toegang tot netwerken en netwerkdiensten – Gebruikers moeten alleen toegang te krijgen tot het	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
			netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	
Bedrijfseisen voor toegangsbeveiliging		9.1.2.1	De toegang tot netwerk en netwerkdiensten vindt plaats op basis van gedefinieerde security categorieën.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging		9.1.2.2	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging		9.1.2.3	Gebruikers met eigen of niet-geauthenticeerde apparatuur (Bring Your Own Device, BYOD) krijgen alleen toegang tot een onvertrouwde zone.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging	9.2.1		Registratie en afmelden van gebruikers – Er moet een formele registratie- en afmeldingsprocedure orden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging		9.2.1.1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging		9.2.1.2	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging	9.2.2		Gebruikers toegang verlenen – Er moet een formele gebruikerstoegangsverleningsprocedure worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging		9.2.2.1	Er is uitsluitend toegang verleend tot Informatie-systemen na autorisatie door een bevoegde functionaris.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging		9.2.2.2	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging		9.2.2.3	Er is een actueel mandaatregister waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten dan wel functieprofielen.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging		9.2.2.4	Eerder uitgegeven accounts en bijbehorende unieke identifiers worden niet hergebruikt..	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging	9.2.3		Beheren van speciale toegangsrechten – Het toewijzen en gebruik van speciale toegangsrechten moeten worden beperkt en beheerst.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging		9.2.3.1	De toewijzing en het gebruik van speciale bevoegdheden worden tot een minimum beperkt.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging		9.2.3.2	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	IV-Hoog
Bedrijfseisen voor toegangsbeveiliging	9.2.4		Beheer van geheime authenticatie-informatie van gebruikers – Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging	9.2.5		Beoordeling van toegangsrechten van gebruikers – Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging		9.2.5.1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging		9.2.5.2	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.	BIV-Basis
Bedrijfseisen voor toegangsbeveiliging		9.2.5.3	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	IV-Hoog

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Bedrijfseisen voor toegangsbeveiliging	9.2.6		Toegangsrechten intrekken of aanpassen – De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.	BIV-Basis
Verantwoordelijkheden van gebruikers	9.3.1		Geheime authenticatie-informatie gebruiken – Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	BIV-Basis
Verantwoordelijkheden van gebruikers		9.3.1.1	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing	9.4.1		Beperking toegang tot informatie – Toegang tot informatie en systeemfuncties van toepassingen moet worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing		9.4.1.1	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie waarborgen.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing		9.4.1.2	Gebruikers kunnen alleen die informatie inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak. Daarbij worden als uitgangspunt de principes 'Least Privilege' en 'Need-to-Know' gehanteerd.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing	9.4.2		Beveiligde inlogprocedures – Als het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing		9.4.2.1	Voor toegang tot alle systemen en applicaties (ongeacht waar deze zich bevinden) is minimaal multifactorauthenticatie nodig.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing		9.4.2.2	Toegang voor het beheer van systemen en applicaties wordt uitsluitend vanaf een interne vertrouwde zone toegestaan.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing		9.4.2.3	Er wordt vooraf een risicoafweging gemaakt voordat aan externe leveranciers toegang tot het netwerk wordt verleend. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing	9.4.3		Systeem voor wachtwoordbeheer – Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing		9.4.3.1	Wachtwoorden moeten voldoen aan het wachtwoordenbeleid van SURF. Het aantal inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing		9.4.3.2	Wachtwoorden worden volgens de vastgelegde richtlijnen vernieuwd.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing		9.4.3.3	Het wachtwoordbeleid wordt geautomatiseerd afgedwongen.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Toegangsbeveiliging van systeem en toepassing		9.4.3.4	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van 24 uur en moeten bij het eerste gebruik worden gewijzigd.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing		9.4.3.5	Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing	9.4.4		Speciale systeemhulpmiddelen gebruiken – Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moeten worden beperkt en nauwkeurig worden gecontroleerd.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing		9.4.4.1	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing		9.4.4.2	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek	BIV-Basis
Toegangsbeveiliging van systeem en toepassing	9.4.5		Toegangsbeveiliging op programmabroncode – Toegang tot de programmabroncode moet worden beperkt.	BIV-Basis
Toegangsbeveiliging van systeem en toepassing		9.4.5.1	Als er open source wordt gebruikt, kan (een deel van) de programmabroncode worden gedeeld als dit nodig is om het programma te verbeteren of te onderhouden.	BIV-Basis

Hoofdstuk 10 – Cryptografie

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Cryptografische beheersmaatregelen	10.1.1		Beleid inzake het gebruik van cryptografische beheersmaatregelen – Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	BIV-Basis
Cryptografische beheersmaatregelen		10.1.1.1	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: a. wanneer cryptografie ingezet wordt; b. wie verantwoordelijk is voor de implementatie; c. wie verantwoordelijk is voor het sleutelbeheer; d. welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het forum standaardisatie worden toegepast; e. de wijze waarop het beschermingsniveau vastgesteld wordt; f. voor communicatie tussen organisaties wordt het beleid onderling vastgesteld.	BIV-Basis
Cryptografische beheersmaatregelen		10.1.1.2	Cryptografische toepassingen voldoen aan passende standaarden.	BIV-Basis
Cryptografische beheersmaatregelen	10.1.2		Sleutelbeheer – Voor het gebruik, de bescherming en de levensduur van cryptografische sleutels moet voor de gehele levenscyclus beleid worden ontwikkeld en geïmplementeerd.	BIV-Basis
Cryptografische beheersmaatregelen		10.1.2.1	De standaard ISO 11770 wordt gehanteerd voor het beheer van cryptografische sleutels.	BIV-Basis

Hoofdstuk 11 – Fysieke beveiliging en beveiliging van de omgeving

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Fysieke beveiliging en beveiliging van de omgeving	11.1.1		Fysieke beveiligingszone – Er moeten beveiligingszones worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	BIV-Basis
Fysieke beveiliging en beveiliging van de omgeving		11.1.1.1	Er wordt gebruikgemaakt van standaarden voor het inrichten van beveiligde zones.	BIV-Basis
Fysieke beveiliging en beveiliging van de omgeving	11.1.2		Fysieke toegangsbeveiliging – Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	BIV-Basis
Fysieke beveiliging en beveiliging van de omgeving		11.1.2.1	Er zijn toegangsregels vastgelegd. De toegang tot ruimtes waarin systemen en/of informatie zijn opgeslagen, zijn beveiligd met een identificatie-, authenticatie-, en autorisatiesysteem en er vindt logging van toegang plaats. Identiteit moet vooraf vastgesteld worden	BIV-Basis
Fysieke beveiliging en beveiliging van de omgeving	11.1.3		Kantoren, ruimten en faciliteiten beveiligen – Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	BIV-Basis
Fysieke beveiliging en beveiliging van de omgeving		11.1.3.1	Sleutelbeheer is ingericht op basis van een sleutelplan.	BIV-Basis
Fysieke beveiliging en beveiliging van de omgeving	11.1.4		Beschermen tegen bedreigingen van buitenaf – Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	BIV-Basis
Fysieke beveiliging en beveiliging van de omgeving		11.1.4.1	Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.	BIV-Basis
Fysieke beveiliging en beveiliging van de omgeving		11.1.4.2	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.	BIV-Basis
Fysieke beveiliging en beveiliging van de omgeving	11.1.5		Werken in beveiligde gebieden – Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	BIV-Basis
Fysieke beveiliging en beveiliging van de omgeving		11.1.5.1	In beveiligde gebieden moet iedereen een zichtbare identificatie dragen (inclusief gasten).	BIV-Basis
Fysieke beveiliging en beveiliging van de omgeving	11.1.6		Laad- en loslocatie – Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	BIV-Basis
Apparatuur	11.2.1		Plaatsing en bescherming van apparatuur – Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf en de kans op onbevoegde toegang worden verkleind.	BIV-Basis
Apparatuur	11.2.2		Nutsvoorzieningen – Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Apparatuur	11.2.3		Beveiliging van bekabeling – Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	BIV-Basis
Apparatuur	11.2.4		Onderhoud van apparatuur – Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	BIV-Basis
Apparatuur		11.2.4.1	Onderhoudscontract met leverancier voor support tijdens kantooruren en respons binnen 4 uur kantoortijden.	BIV-Basis
Apparatuur		11.2.4.2	Onderhoudscontract met leverancier voor support 24 uur x 7 dagen en respons binnen 2 uur. Afspraken over aanwezigheid vervangende componenten op locatie moet worden overwogen.	B-Hoog
Apparatuur	11.2.5		Verwijdering van bedrijfsmiddelen – Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	BIV-Basis
Apparatuur	11.2.6		Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein – Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd. Daarbij moet rekening worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	BIV-Basis
Apparatuur	11.2.7		Veilig verwijderen of hergebruiken van apparatuur – Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	BIV-Basis
Apparatuur	11.2.8		Onbeheerde gebruikersapparatuur – Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	BIV-Basis
Apparatuur	11.2.9		'Clear desk'- en 'clear screen'-beleid – Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	BIV-Basis
Apparatuur		11.2.9.1	Een onbeheerde werkplek in een ongecontroleerde omgeving is altijd vergrendeld.	BIV-Basis
Apparatuur		11.2.9.2	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screenlock na een inactiviteit van maximaal 5 minuten.	BIV-Basis
Apparatuur		11.2.9.3	Sessies op remote desktops worden op het remote platform vergrendeld na 15 minuten. Het overnemen van sessies op remote desktops op een ander client apparaat is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd.	BIV-Basis
Apparatuur		11.2.9.4	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het token de toegangsbeveiligingslock automatisch geactiveerd.	BIV-Basis
Apparatuur		11.2.9.5	Whiteboards, flipovers en dergelijk in algemene ruimten (vergaderzalen en flexruimten) moeten na gebruik worden geschoond.	BIV-Basis

Hoofdstuk 12 – Beveiliging Bedrijfsvoering

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Bedieningsprocedures en verantwoordelijkheden	12.1.1		Gedocumenteerde bedieningsprocedures – Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	BIV-Basis
Bedieningsprocedures en verantwoordelijkheden	12.1.2		Wijzigingsbeheer – Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.	BIV-Basis
Bedieningsprocedures en verantwoordelijkheden		12.1.2.1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: a. het administreren van wijzigingen; b. risicoafweging van mogelijke gevolgen van de wijzigingen; c. goedkeuringsprocedure voor wijzigingen.	BIV-Basis
Bedieningsprocedures en verantwoordelijkheden	12.1.3		Capaciteitsbeheer – Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	BIV-Basis
Bedieningsprocedures en verantwoordelijkheden		12.1.3.1	Met betrekking tot externe koppelingen zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief kunnen beïnvloeden (bijvoorbeeld DDoS-aanvallen) te signaleren en hierop te reageren.	BIV-Basis
Bedieningsprocedures en verantwoordelijkheden		12.1.3.2	De IT-resources mogen structureel niet meer dan 90% in gebruik zijn, denk hierbij aan netwerk-, disk-ruimte- en CPU-capaciteit. Een trendmatige toename van incidentele overschrijdingen moet 24 uur x 7 dagen worden gemonitord en eventueel wordt actie ondernomen.	B-Hoog
Bedieningsprocedures en verantwoordelijkheden	12.1.4		Scheiding van ontwikkel-, test- en productieomgevingen – Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	BIV-Basis
Bedieningsprocedures en verantwoordelijkheden		12.1.4.1	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	BIV-Basis
Bedieningsprocedures en verantwoordelijkheden		12.1.4.2	Wijzigingen op de productieomgeving worden altijd getest voordat ze in productie worden gebracht. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	BIV-Basis
Bescherming tegen malware	12.2.1		Beheersmaatregelen tegen malware – Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, en in combinatie daarmee moet voor een passende awareness van gebruikers worden gezorgd.	BIV-Basis
Bescherming tegen malware		12.2.1.1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	BIV-Basis
Bescherming tegen malware		12.2.1.2	Gebruikers zijn voorgelicht over de risico's van surfgedrag en het klikken op onbekende links.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Bescherming tegen malware		12.2.1.3	Software en bijbehorende herstelsoftware die malware opspoort, zijn geïnstalleerd en worden regelmatig geüpdatet.	BIV-Basis
Bescherming tegen malware		12.2.1.4	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan moet omvatten: a. alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen; b. bijlagen en downloads vóór gebruik.	BIV-Basis
Bescherming tegen malware		12.2.1.5	De malwarescan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.	BIV-Basis
Back-up	12.3.1		Back-up van informatie – Regelmatig moeten back-ups informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	BIV-Basis
Back-up		12.3.1.1	Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld	BIV-Basis
Back-up		12.3.1.2	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	BIV-Basis
Back-up		12.3.1.3	Ter voorkoming van beschadiging tijdens een calamiteit moet minimaal één back-up-kopie fysiek op een remotelocatie opgeslagen worden. De minimale afstand van de remotelocatie tot het datacenter (hoofdlocatie) bedraagt 5 km.	BIV-Basis
Back-up		12.3.1.4	De restoreprocedure wordt minimaal jaarlijks getest of na een grote wijziging om de betrouwbaarheid te waarborgen als ze in noodgevallen uitgevoerd moet worden.	BIV-Basis
Back-up		12.3.1.5	Het maximaal toegestane dataverlies is 1 uur.	B-Hoog
Verslaglegging en monitoren	12.4.1		Gebeurtenissen registreren – Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	BIV-Basis
Verslaglegging en monitoren		12.4.1.1	Een logregel bevat minimaal de gebeurtenis: a. de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; b. het gebruikte apparaat; c. het resultaat van de handeling (bijvoorbeeld: lezen, schrijven, modificeren en verwijderen); d. de datum en het tijdstip van de gebeurtenis.	BIV-Basis
Verslaglegging en monitoren		12.4.1.2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	BIV-Basis
Verslaglegging en monitoren		12.4.1.3	Alle authenticatielogs worden doorgestuurd naar de centrale loggingserver	BIV-Basis
Verslaglegging en monitoren		12.4.1.4	De informatieverwerkende omgeving wordt gemonitord op basis van een risico-inschatting, mede aan de hand van en de aard van de te beschermen gegevens en Informatie-systemen, zodat aanvallen kunnen worden gedetecteerd.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Verslaglegging en monitoren		12.4.1.5	Netwerkflow-informatie wordt gesampled en naar een centrale datacollector gestuurd.	BIV-Basis
Verslaglegging en monitoren		12.4.1.6	Logging is aangezet voor alle verwerkingen van de gegevens door het systeem of applicaties. Dit betreft alle soorten verwerkingen: lezen, schrijven, modificeren en verwijderen.	BIV-Basis
Verslaglegging en monitoren		12.4.1.7	Een geautomatiseerd monitoringsysteem beoordeelt de logfiles en produceert alarmen in geval van onregelmatigheden of situaties die op een potentieel risico wijzen.	IV-Hoog
Verslaglegging en monitoren	12.4.2		Beschermen van informatie in logbestanden – Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	BIV-Basis
Verslaglegging en monitoren		12.4.2.1	Er is een overzicht van logbestanden. De logbestanden worden gegenereerd met vermelding van opslaglocatie.	BIV-Basis
Verslaglegging en monitoren		12.4.2.2	Voor de loganalyse moeten logbestanden voor een periode van minimaal 6 maanden worden bewaard. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	BIV-Basis
Verslaglegging en monitoren		12.4.2.3	Logfiles worden beschermd tegen wijziging of vernietiging. Toegang tot de logs wordt gelogd.	BIV-Basis
Verslaglegging en monitoren		12.4.2.4	Er is een (onafhankelijke) interne auditprocedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	IV-Hoog
Verslaglegging en monitoren		12.4.2.5	Oneigenlijk wijzigen, verwijderen van loggegevens of poging daartoe, wordt zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten.	IV-Hoog
Verslaglegging en monitoren	12.4.3		Logbestanden van beheerders en operators – Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.	BIV-Basis
Verslaglegging en monitoren		12.4.3.1	Alle acties van de systemadmins worden gelogd.	IV-Hoog
Verslaglegging en monitoren	12.4.4		Kloksynchronisatie – De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.	BIV-Basis
Verslaglegging en monitoren		12.4.4.1	De machine bevat de juiste tijd, tijdzone (lokale tijdzone) en datum.	BIV-Basis
Verslaglegging en monitoren		12.4.4.2	De systeemklok en de tijdsynchronisatie via de SURF NTP-servers (Network Time Protocol) zijn ingesteld.	BIV-Basis
Beheersing van operationele software	12.5.1		Software installeren op operationele systemen – Om het op operationele systemen installeren van software te beheersen, moeten procedures worden geïmplementeerd.	BIV-Basis
Beheer van technische kwetsbaarheden	12.6.1		Beheer van technische kwetsbaarheden – Informatie over technische kwetsbaarheden van Informatie-systemen die worden gebruikt, moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten passende maatregelen worden genomen om het risico dat ermee samenhangt aan te pakken.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Beheer van technische kwetsbaarheden		12.6.1.1	Voor elk aan het SURF-netwerk aangesloten systeem en de daarop geïnstalleerde software moet patchmanagement zijn ingericht, ongeacht alle andere gerealiseerde security- en beheermaatregelen.	BIV-Basis
Beheer van technische kwetsbaarheden		12.6.1.2	De afdeling waar het beheer van het systeem onder valt moet voor een adequaat patchschema zorgen.	BIV-Basis
Beheer van technische kwetsbaarheden		12.6.1.3	Iedere patch wordt beoordeeld op impact en consequenties. Aan de hand van deze beoordeling wordt er een prioriteit aan gekoppeld. Afhankelijk van de prioriteit en impact wordt de installatie van de patch gepland. Dat kan resulteren in een onmiddellijke uitrol van de patch, een uitrol tijdens de eerstvolgende maintenance-window of een uitrol op een datum ergens in de toekomst.	BIV-Basis
Beheer van technische kwetsbaarheden		12.6.1.4	Security-patches moeten met voorrang worden behandeld. Dat betekent dat er een onmiddellijke beoordeling van impact en prioriteit moet worden gemaakt.	BIV-Basis
Beheer van technische kwetsbaarheden		12.6.1.5	Als een patch met een hoge prioriteit niet snel kan worden uitgerold, bijvoorbeeld op technische gronden, dan moeten daarvoor een adequate work-around en/of maatregelen worden ingevoerd om het systeem of de applicatie te beschermen tegen kwetsbaarheden.	BIV-Basis
Beheer van technische kwetsbaarheden		12.6.1.6	In het kader van systeem hardening, dienen overbodige componenten, services en software op de servers en netwerkelementen worden uitgeschakeld om het risico op technische kwetsbaarheden en succesvolle aanvallen te minimaliseren. Met andere woorden op het systeem draaien uitsluitende de noodzakelijk onderdelen.	BIV-Basis
Beheer van technische kwetsbaarheden	12.6.2		Beperkingen voor het installeren van software – Voor het door gebruikers installeren van software moeten regels worden vastgesteld en worden geïmplementeerd.	BIV-Basis
Beheer van technische kwetsbaarheden		12.6.2.1	Gebruikers kunnen op hun werkomgeving software installeren. De werkplekken worden gemonitord op geïnstalleerde software en verdacht gedrag.	BIV-Basis
Overwegingen betreffende audits van Informatie-systemen	12.7.1		Beheersmaatregelen betreffende audits van Informatie-systemen – Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	BIV-Basis

Hoofdstuk 13 - Communicatiebeveiliging

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Beheer van netwerkbeveiliging	13.1.2		Beveiliging van netwerkdiensten – Eisen voor beveiligingsmechanismen, dienstverleningsniveaus en beheer voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	BIV-Basis
Beheer van netwerkbeveiliging		13.1.2.1	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt tegen en geanalyseerd op kwaadaardige elementen met detectievoorzieningen,	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
			zoals het Nationaal Detectie Netwerk, die worden ingezet op basis van een risicoinschatting, mede aan de hand van de aard van de te beschermen gegevens en Informatie-systemen.	
Beheer van netwerkbeveiliging		13.1.2.2	Aansluiting op bedrijfsnetwerken (inclusief wireless) is alleen mogelijk na authenticatie.	BIV-Basis
Beheer van netwerkbeveiliging		13.1.2.3	Voor externe toegang tot interne netwerken wordt gebruikt gemaakt van een VPN server voorzien van Multi Factor Authenticatie.	BIV-Basis
Beheer van netwerkbeveiliging		13.1.2.4	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied, wordt gebruikgemaakt van encryptie middelen.	BIV-Basis
Beheer van netwerkbeveiliging		13.1.2.5	Nieuwe dreigingen die zijn gedetecteerd door de detectie-oplossing als genoemd in 13.1.2.1 worden, rekening houdend met de geldende juridische kaders, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing) gemeld en behandeld door interne SURF CERT/SOC.	BIV-Basis
Beheer van netwerkbeveiliging		13.1.2.6	Netwerkverkeer wordt zowel inkomend als uitgaand gefilterd. Filtering wordt ingezet aan de hand van de aard van de te beschermen gegevens en Informatie-systemen en mede op basis van een risico-inschatting.	BIV-Basis
Beheer van netwerkbeveiliging	13.1.3		Beveiligingsmechanismen, dienstverleningsniveaus en beheereisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	BIV-Basis
Beheer van netwerkbeveiliging		13.1.3.1	Ieder VLAN heeft een gedefinieerd security-beveiligingsniveau.	BIV-Basis
Beheer van netwerkbeveiliging		13.1.3.1	De beveiliging van de IT-systemen vindt plaats op basis van gedefinieerde security-beveiligingsniveaus volgens een gestructureerde VLAN-indeling.	BIV-Basis
Informatietransport	13.2.1		Beleid en procedures voor informatietransport – Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	BIV-Basis
Informatietransport	13.2.2		Overeenkomsten over informatietransport – Overeenkomsten moeten betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	BIV-Basis
Informatietransport	13.2.3		Elektronische berichten – Informatie die is opgenomen in elektronische berichten moet passend zijn beschermd.	BIV-Basis
Informatietransport		13.2.3.1	Voor de beveiliging van elektronische berichten gelden de vastgestelde standaarden tegen malware, phishing, afluisteren en modificatie zoals SPF, DKIM, DMARC en encryptie.	BIV-Basis
Informatietransport		13.2.3.2	E-mailberichten worden geautomatiseerd gescand op aanwezigheid van spamberichten en virussen en andere kwaadaardige software.	BIV-Basis
Informatietransport		13.2.3.3	Data in transit moet altijd versleuteld zijn. Maak gebruik van SURFcertificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn o.a. digitale documenten waar gebruikers rechten aan kunnen ontlenen.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Informatietransport		13.2.3.4	In het Gebruiksreglement ICT-middelen (ook wel de Acceptable Use Policy) is beschreven hoe de medewerkers om moeten gaan met ICT-middelen (internet, laptops, e-mail, etc.).	BIV-Basis
Informatietransport	13.2.4		Vertrouwelijkheids- of geheimhoudingsovereenkomst – Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.	BIV-Basis

Hoofdstuk 14 – Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Beveiligingseisen voor Informatie-systemen	14.1.1		Analyse en specificatie van informatiebeveiligingseisen – De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe Informatie-systemen of voor uitbreidingen van bestaande Informatie-systemen.	BIV-Basis
Beveiligingseisen voor Informatie-systemen		14.1.1.1	Bij nieuwe Informatie-systemen en bij wijzigingen op bestaande Informatie-systemen moet een expliciete risicoafweging worden uitgevoerd voor het vaststellen van de beveiligingseisen, uitgaande van de baseline van SURF.	BIV-Basis
Beveiligingseisen voor Informatie-systemen	14.1.2		Toepassingen op openbare netwerken beveiligen – Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	BIV-Basis
Beveiligingseisen voor Informatie-systemen		14.1.2.1	Zie maatregel 13.2.3.3 (Maak gebruik van SURFcertificaten)	BIV-Basis
Beveiligingseisen voor Informatie-systemen	14.1.3		Transacties van toepassingen beschermen – Informatie die deel uitmaakt van transacties van toepassingen moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	BIV-Basis
Beveiligingseisen voor Informatie-systemen		14.1.3.1	Zie maatregel 13.2.3.3 (Maak gebruik van SURFcertificaten)	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen	14.2.1		Beleid voor beveiligd ontwikkelen – Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen		14.2.1.1	Security by Design is het uitgangspunt voor de ontwikkeling van software en systemen.	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen		14.2.1.2	Het testen en ontwikkelen van software en systemen wordt uitgevoerd op basis van het OTAP-principe.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Beveiliging in ontwikkelings- en ondersteunende processen	14.2.2		Procedures voor wijzigingsbeheer met betrekking tot systemen – Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen		14.2.2.1	Voor het wijzigingsbeheer wordt een algemeen geaccepteerd framework zoals FitSM of ITIL gebruikt.	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen	14.2.3		Technische beoordeling van toepassingen na wijzigingen besturingsplatform – Als besturingsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen	14.2.4		Beperkingen op wijzigingen aan softwarepakketten – Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen	14.2.5		Principes voor engineering van beveiligde systemen – Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van Informatie-systemen.	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen		14.2.5.1	Zie control 14.2.1.1 (Security by Design)	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen	14.2.6		Beveiligde ontwikkelomgeving – Organisaties moeten beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen		14.2.6.1	Zie control 14.2.1.2 (OTAP)	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen	14.2.7		Uitbestede softwareontwikkeling – Uitbestede systeemontwikkeling behoort onder supervisie te staan van en worden gemonitord door de organisatie.	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen		14.2.7.1	Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd.	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen	14.2.8		Testen van systeembeveiliging – Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Beveiliging in ontwikkelings- en ondersteunende processen	14.2.9		Systeemacceptatietests – Voor nieuwe Informatie-systemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen		14.2.9.1	Een systeem of applicatie wordt aan een van tevoren gedefinieerde acceptatietest onderworpen.	BIV-Basis
Beveiliging in ontwikkelings- en ondersteunende processen		14.2.9.2	Voor acceptatietesten van systemen worden gestructureerde testmethodieken zoals bijvoorbeeld TMap gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	BIV-Basis
Testgegevens	14.3.1		Bescherming van testgegevens – Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	BIV-Basis
Testgegevens		14.3.1.1	Productiedata mogen niet als testgegevens worden gebruikt. Voor de testomgeving gelden dezelfde maatregelen als in de productieomgeving.	BIV-Basis
Testgegevens		14.3.1.2	Als het onvermijdelijk is dat productiedata in een testomgeving worden gebruikt, moeten deze worden geanonimiseerd of gepseudonimiseerd.	BIV-Basis

Hoofdstuk 15 – Leveranciersrelaties

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Informatiebeveiliging in leveranciersrelaties	15.1.1		Informatiebeveiligingsbeleid voor leveranciersrelaties – Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.	BIV-Basis
Informatiebeveiliging in leveranciersrelaties		15.1.1.1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen voor informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd.	BIV-Basis
Informatiebeveiliging in leveranciersrelaties		15.1.1.2	De beheersmaatregelen voor leverancierstoegang tot bedrijfsinformatie worden op basis van een expliciete risicoafweging vastgesteld.	BIV-Basis
Informatiebeveiliging in leveranciersrelaties		15.1.1.3	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.	BIV-Basis
Informatiebeveiliging in leveranciersrelaties	15.1.2		Opnemen van beveiligingsaspecten in leveranciersovereenkomsten – Alle relevante informatiebeveiligingseisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	BIV-Basis
Informatiebeveiliging in leveranciersrelaties		15.1.2.1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.	BIV-Basis
Informatiebeveiliging in leveranciersrelaties		15.1.2.2	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Informatiebeveiliging in leveranciersrelaties		15.1.2.3	In inkoopcontracten wordt expliciet de mogelijkheid van een externe audit opgenomen waarmee de betrouwbaarheid van de geleverde dienst kan worden getoetst. Een audit is niet nodig als de contractant d.m.v. certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.	BIV-Basis
Informatiebeveiliging in leveranciersrelaties		15.1.2.4	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaard voorwaarden voor inkoop gehanteerd.	BIV-Basis
Informatiebeveiliging in leveranciersrelaties		15.1.2.5	Voordat een contract wordt afgesloten, wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exitstrategie.	BIV-Basis
Informatiebeveiliging in leveranciersrelaties		15.1.2.6	In inkoopcontracten wordt expliciet de mogelijkheid van een externe audit opgenomen waarmee de betrouwbaarheid van de geleverde dienst kan worden getoetst. Een audit is niet nodig als de contractant via certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.	IV-Hoog
Informatiebeveiliging in leveranciersrelaties	15.1.3		Toeleveringsketen van informatie- en communicatietechnologie – Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	BIV-Basis
Informatiebeveiliging in leveranciersrelaties		15.1.3.1	Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers.	BIV-Basis
Beheer van dienstverlening van leveranciers	15.2.1		Monitoring en beoordeling van dienstverlening van leveranciers – Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	BIV-Basis
Beheer van dienstverlening van leveranciers		15.2.1.1	Minimaal 1 keer per jaar wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.	BIV-Basis
Beheer van dienstverlening van leveranciers	15.2.2		Beheer van veranderingen in dienstverlening van leveranciers – Veranderingen in de dienstverlening van leveranciers met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, moeten worden, beheerd, rekening houdend met betrokken systemen en processen, herbeoordeling van risico's en met hoe kritiek bedrijfsinformatie is.	BIV-Basis

Hoofdstuk 16 – Beheer van informatiebeveiligingsincidenten

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Beheer van informatiebeveiligings-incidenten en - verbeteringen	16.1.1		Verantwoordelijkheden en procedures – Er moeten bestuursverantwoordelijkheden en -procedures worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Beheer van informatiebeveiligings-incidenten en - verbeteringen	16.1.2		Rapportage van informatiebeveiligingsgebeurtenissen – Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	BIV-Basis
Beheer van informatiebeveiligingsincidenten en - verbeteringen		16.1.2.1	Alle security-incidenten worden gemeld bij SURF-IRT.	BIV-Basis
Beheer van informatiebeveiligings-incidenten en - verbeteringen		16.1.2.2	Het SURF-IRT-team geeft opvolging aan security-incidenten volgens de daarvoor geldende incidentprocedure en zorgt voor de nodige escalaties.	BIV-Basis
Beheer van informatiebeveiligings-incidenten en - verbeteringen		16.1.2.3	Alle medewerkers en contractanten hebben aantoonbaar kennisgenomen van de security incidenten procedure.	BIV-Basis
Beheer van informatiebeveiligings-incidenten en - verbeteringen		16.1.2.4	Incidenten worden zo snel als mogelijk, maar in ieder geval binnen 24 uur na bekendwording, gemeld bij het SURF-IRT (SIRT).	BIV-Basis
Beheer van informatiebeveiligings-incidenten en - verbeteringen		16.1.2.5	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.	BIV-Basis
Beheer van informatiebeveiligingsincidenten en - verbeteringen		16.1.2.6	De opvolging van incidenten wordt periodiek gerapporteerd aan de verantwoordelijke.	BIV-Basis
Beheer van informatiebeveiligings-incidenten en - verbeteringen		16.1.2.7	Informatie afkomstig uit de procedure voor coordinated vulnerability disclosure (voorheen 'responsible disclosure', is onderdeel van de incidentrapportage.	BIV-Basis
Beheer van informatiebeveiligings-incidenten en - verbeteringen	16.1.3		Rapportage van zwakke plekken in de informatiebeveiliging – Van medewerkers en contractanten die gebruikmaken van de Informatie-systemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	BIV-Basis
Beheer van informatiebeveiligingsincidenten en - verbeteringen		16.1.3.1	Er is een procedure voor coordinated vulnerability disclosure gepubliceerd en ingericht (voor heen 'responsible disclosure').	BIV-Basis
Beheer van informatiebeveiligings-incidenten en - verbeteringen	16.1.4		Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen – Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld, waarbij wordt geoordeeld of ze moeten worden geclassificeerd als informatiebeveiligingsincidenten.	BIV-Basis
Beheer van informatiebeveiligings-incidenten en - verbeteringen		16.1.4.1	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende systemen, moeten zo snel mogelijk (binnen 24 uur) worden gemeld aan SURF-IRT (SIRT). SIRT maakt vervolgens samen met de verantwoordelijke	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
			afdeling een impactanalyse van het incident en definieert nodige herstelmaatregelen.	
Beheer van informatiebeveiligings-incidenten en - verbeteringen	16.1.5		Respons op informatiebeveiligingsincidenten – Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	BIV-Basis
Beheer van informatiebeveiliging-sincidenten en - verbeteringen	16.1.6		Lering uit informatiebeveiligingsincidenten – Kennis die is verkregen door het analyseren en oplossen van informatiebeveiligingsincidenten, moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	BIV-Basis
Beheer van informatiebeveiligings-incidenten en - verbeteringen		16.1.6.1	Beveiligingsincidenten worden geanalyseerd met als doel te leren en het voorkomen van toekomstige beveiligingsincidenten.	BIV-Basis
Beheer van informatiebeveiligings-incidenten en - verbeteringen		16.1.6.2	De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.	BIV-Basis
Beheer van informatiebeveiligings-incidenten en - verbeteringen	16.1.7		Verzamelen van bewijsmateriaal – De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	BIV-Basis

Hoofdstuk 17 – Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Informatiebeveiligings-continuïteit	17.1		Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer zijn geïmplementeerd.	BIV-Basis
Informatiebeveiligings-continuïteit	17.1.1		Informatiebeveiligingscontinuïteitsplannen – De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	BIV-Basis
Informatiebeveiligings-continuïteit		17.1.1	Er moet een crisisplan aanwezig te zijn, deze moet onderdeel te zijn van de continuïteitsplannen voor informatiebeveiliging.	BIV-Basis
Informatiebeveiligings-continuïteit	17.1.2		Informatiebeveiligingscontinuïteit implementeren – De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	BIV-Basis
Informatiebeveiligings-continuïteit	17.1.3		Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren – De organisatie moet de voor informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	BIV-Basis
Informatiebeveiligings-continuïteit		17.1.3.1	Continuïteitsplannen van bedrijfskritische systemen worden jaarlijks getest op geldigheid en bruikbaarheid. Continuïteitsplannen van overige systemen worden tweejaarlijks getest op geldigheid en bruikbaarheid.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Informatiebeveiligings-continuïteit		17.1.3.2	Door het uitvoeren van een expliciete risicoafweging worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd.	BIV-Basis
Informatiebeveiligings-continuïteit		17.1.3.3	De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten minimaal binnen een week hersteld.	BIV-Basis
Informatiebeveiligings-continuïteit		17.1.3.4	Het crisisplan worden jaarlijks getest op geldigheid, actualiteit en bruikbaarheid.	BIV-Basis
Redundante componenten	17.2.1		Beschikbaarheid van informatieverwerkende faciliteiten – Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	BIV-Basis
Redundante componenten		17.2.1.1	De maximale hersteltijd na een incident, calamiteit of uitval informatieverwerkende faciliteit is 4 uur.	B-Hoog

Hoofdstuk 18 - Naleving

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Naleving van wettelijke en contractuele eisen	18.1.1		Vaststellen van toepasselijke wetgeving en contractuele eisen – Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.	BIV-Basis
Naleving van wettelijke en contractuele eisen	18.1.2		Intellectuele-eigendomsrechten – Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen, moeten passende procedures worden geïmplementeerd.	BIV-Basis
Naleving van wettelijke en contractuele eisen	18.1.3		Beschermen van registraties – Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	BIV-Basis
Naleving van wettelijke en contractuele eisen		18.1.3.1	Per soort informatie is inzichtelijk gemaakt wat de bewaartermijn is.	BIV-Basis
Naleving van wettelijke en contractuele eisen	18.1.4		Privacy en bescherming van persoonsgegevens – Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	BIV-Basis
Naleving van wettelijke en contractuele eisen		18.1.4.1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris voor Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.	BIV-Basis
Naleving van wettelijke en contractuele eisen		18.1.4.2	Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	BIV-Basis
Naleving van wettelijke en contractuele eisen	18.1.5		Voorschriften voor het gebruik van cryptografische beheersmaatregelen – Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	BIV-Basis
Naleving van wettelijke en contractuele eisen		18.1.5.1	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij internationale standaarden.	BIV-Basis

Sub-hoofdstuk	ISO	ID	Control/maatregel	Classificatie
Informatiebeveiligingsbeoordelingen	18.2.1		Onafhankelijke beoordeling van informatiebeveiliging – De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijvoorbeeld beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	BIV-Basis
Informatiebeveiligingsbeoordelingen		18.2.1.1	Er is een information security information system (ISMS) waarmee de gehele PDCA-cyclus (plan-do-check-act) aantoonbaar op gestructureerde wijze wordt afgedekt.	BIV-Basis
Informatiebeveiligingsbeoordelingen		18.2.1.2	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	BIV-Basis
Informatiebeveiligingsbeoordelingen	18.2.2		Naleving van beveiligingsbeleid en -normen – Het bestuur moet regelmatig de naleving van de informatieverwerking en – procedures binnen haar verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	BIV-Basis
Informatiebeveiligingsbeoordelingen		18.2.2.1	In de P&C-cyclus wordt gerapporteerd over informatiebeveiliging. Diensteigenaar aan proceseigenaar, proceseigenaar aan bestuur.	BIV-Basis
Informatiebeveiligingsbeoordelingen	18.2.3		Beoordeling van technische naleving – Informatie-systemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	BIV-Basis
Informatiebeveiligingsbeoordelingen		18.2.3.1	Informatie-systemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of pentesten.	IV-Hoog