Samen aanjagen van vernieuwing

BIS

Baseline Informatiebeveiliging SURF

Versie: 1.1
Datum: 21 juni 2022
Kenmerk: Baseline informatiebeveilging SURF

Wijzigingshistorie:

VERSIE	DATUM	OPMERKINGEN
0.1	00-00-2020	Opzet eerste versie, als bron gebruikt BIR
0.2	00-00-2020	Review en aanpassingen op basis van SURFsara beleid
0.3	00-00-2020	Review en aanpassingen door Security kernteam
0.4	12-2-2021	Tweede review van de maatregelen
0.5	22-3-2021	Maatregelen vastgesteld
0.9	01-06-2021	Redactionele wijzigingen
0.91	10-08-2021	Redactionele wijzigingen
0.92	19-10-2021	Review van smaakmakers verwerkt
1.1	**21-06-2022**	**Aanpassingen nalv security bijeenkomsten**

Inhoudsopgave

1. Informatiebeveiliging SURF

1.1 Inleiding

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

De Baseline Informatiebeveiliging SURF(BIS), beoogt de beveiliging van informatie(systemen) bij alle bedrijfsonderdelen van SURF te bevorderen, zodat deze bedrijfsonderdelen erop kunnen vertrouwen dat gegevens die SURF verwerkt, in lijn met wet- en regelgeving, passend beveiligd zijn.

1.2 Scope

De BIS is van toepassing op de gehele SURF-organisatie.

De BIS vormt een integraal onderdeel van het informatiebeveiligingsbeleid. De BIS omvat alle organisatorische en technische maatregelen waar zowel de organisatie in zijn geheel als alle diensten en systemen waar informatie op wordt verwerkt aan moeten voldoen. Waar mogelijk strijdigheid is tussen een ander toepasselijk beleidsdocument in de baseline dan prevaleert de baseline.

Er is rekening gehouden met de eisen die de Algemene Verordening Gegevensbescherming (AVG) stelt, het uitgangspunt is om compliant te zijn met de AVG. Specifieke eisen uit de AVG zijn echter niet opgenomen in de baseline. De BIS beperkt zich alleen tot securitymaatregelen die nodig zijn om een verwerking van persoonsgegevens volgens AVG adequaat te beveiligen. Er is speciale aandacht besteed aan de eisen voor het verwerken van bijzondere persoonsgegevens. Specifieke AVG-onderwerpen en maatregelen behoren echter tot het domein van privacy en dienen in het privacy beleid en de bijbehorende procedures en maatregelen te worden behandeld.

1.3 Informatiebeveiligingskaders en uitgangspunten

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

- Informatieveiligheidsbeleid SURF
- Acceptable Use Policy SURF
- NEN/ISO 27001
- NEN/ISO 27002
- SURF Juridisch Normenkader (Cloud)Services
- Baseline Informatiebeveiliging Overheid (BIO)

- Algemene Verordening Gegevensverwerking (AVG)

Voor de BIS geldt op basis van deze documenten kort samengevat het volgende:

- Een ruime definitie voor een informatiesysteem, namelijk “een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie”;
- Het lijnmanagement is verantwoordelijk voor de beveiliging van informatie(systemen);
- Informatiebeveiliging is een cyclisch proces is, volgens de Plan-Do-Check-Act cyclus;
- De Raad van Bestuur van SURF is eindverantwoordelijk voor deze beveiliging en voor de inrichting en werking van de beveiligingsorganisatie;
- Het lijnmanagement stelt de betrouwbaarheidseisen voor zijn informatiesystemen vast;
- Op basis van de betrouwbaarheidseisen kiest, implementeert en draagt het lijnmanagement de maatregelen uit.

De BIS is allereerst een gemeenschappelijk normenkader voor de beveiliging van de informatie(systemen) van SURF. Daarnaast concretiseert de BIS een aantal normen tot verplichte maatregelen:

- op grond van SURF beleid
- op grond van wet- en regelgeving;
- vanwege de gemeenschappelijk veiligheid van informatieketens;
- omdat deze fundamenteel zijn voor een betrouwbare en professionele dienstverlening en informatievoorziening.

1.4 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. Deze standaard is een “best practice” om informatiebeveiligingsrisico’s aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening. De standaard kan gezien worden als een nadere specificatie van de ISO 27001 standaard. De ISO 27002 kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en als effectieve methode voor het bereiken van deze veiligheid.

De ISO bestaat uit 114 controls; de term ‘control’ wordt in de ISO vertaald als een beheersmaatregel. De BIS volgt de opbouw van de ISO 27002 en haar controls. De controls zijn in de BIS letterlijk overgenomen. Dit vergemakkelijkt de afstemming zowel intern in de organisatie als waar nodig met externe partners.

1.5 Evaluatie en bijstelling

Door de ontwikkelingen van de techniek kunnen de maatregelensets voor informatiebeveiliging snel verouderen. De BIS is daarom zoveel als mogelijk op een abstractieniveau geschreven waarbij dergelijke wijzigingen en ontwikkelingen een zo klein mogelijke impact hebben op de maatregelen. De BIS beschrijft het wat en niet het hoe. Desondanks kunnen wijzigingen noodzakelijk zijn bij bijvoorbeeld aanpassingen van onderliggende wet- en regelgeving, nieuwe of juist verouderde beleidsrichtlijnen of nieuwe dreigingen en kwetsbaarheden.

Dit document zal daarom regelmatig, minimaal jaarlijks, in zijn geheel worden geëvalueerd en zo nodig geactualiseerd. Daarnaast wordt specifiek bezien of er wijzigingen en aanvullingen in de maatregelen en de (operationele) richtlijnen noodzakelijk of gewenst zijn om hiermee de praktische toepasbaarheid te vergroten.

2. Opzet van de BIS

2.1 Opzet basis beveiligingsniveau's

De BIS onderscheidt twee basis beveiligingsniveaus (BBN). Hiermee wordt de keuze voor de set van maatregelen hanteerbaar, efficiënt en proportioneel aan de te beschermen informatie in combinatie met relevante dreigingen. Voor BBN1 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie "Openbaar, laag-/middenniveau, basis persoonsgegevens", volgens het principe van een betrouwbare dienstverlening. BBN2[1] is van toepassing op gerubriceerde informatie "(Strikt)Vertrouwelijk, vitaal of bijzondere persoonsgegevens, oftewel hoog niveau" waarbij hogere mate bescherming en weerstand tegen zowel basis als complexe en geavanceerde bedreigingen nodig is.

De keuze voor een BBN wordt gemaakt door de dienstverantwoordelijke/ proceseigenaar en is gebaseerd op de aard van de te verwerken gegevens en de belangen die ermee gepaard gaan.

Beschikbaarheidseisen spelen geen rol bij de bepaling van de BBN-niveau. De eisen daarvoor dienen binnen de context van de dienst en de bijbehorende SLA's te worden beoordeeld en de benodigde specifieke maatregelen daarvoor in dezelfde context getroffen.

2.2 Controls

Na de BBN-toets doorloopt het lijnmanagement alle toepasselijke controls uit de BIS. Op basis van een beoordeling van de omstandigheden en risicoafweging in de specifieke context waarbinnen de control moet worden geïmplementeerd wordt bepaald hoe moet worden voldaan aan de gestelde beveiligingsdoelstellingen van de controls. Voor het voldoen aan deze doelstellingen kunnen SURF-implementatierichtlijnen en implementatierichtlijnen uit de ISO 27002 worden gebruikt.

Er geldt een hardheidsbepaling: in het geval 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 (explain) dient vastgelegd te worden.

[1] De BBN-toets is geen volwaardige vervanger van een uitgebreide risicoanalysemethodiek. De BBN-toets zorgt er alleen voor dat eenvoudig het juiste BBN geselecteerd kan worden en dat bepaald kan worden in hoeverre extra eisen noodzakelijk zijn.

2.3 Implementatierichtlijnen

De implementatierichtlijnen zijn niet in de BIS opgenomen, hiervoor wordt primair verwezen naar de SURF implementatierichtlijnen (zie paragraaf 2.4) en secundair naar die van de ISO 27002.

De BIS-maatregelen dekken niet altijd de gehele beveiligingsdoelstellingen van de control af. Net als bij de controls, geldt hier een hardheidsbepaling: in het geval een maatregel voor een specifiek geval niet van toepassing kan zijn, vervalt de verplichting. In dit geval moet aangegeven worden wat de risicoafweging is die hieraan ten grondslag ligt (explain).

2.4 Operationalisering in standaarden, procedures, richtlijnen (of aanbevelingen, handreikingen en best practices)

Om de praktische toepasbaarheid van de BIS te verhogen, wordt de BIS geoperationaliseerd in de SURF implementatierichtlijnen, uitgewerkt in standaarden, procedures en richtlijnen[2].

2.5 Rollen

De BIS onderscheidt drie (hoofd)rollen: het Bestuur, de Proceseigenaar en de Dienstverantwoordelijke. Deze rollen zijn hieronder beschreven vanuit het perspectief van informatiebeveiliging. Er zijn uiteraard meer rollen betrokken bij informatiebeveiliging, zoals toezichthouder en medewerker, maar het gaat hier om de verantwoordelijke voor de uitvoering van de control.

Bestuur	Als eindverantwoordelijke voor het beveiligingsbeleid in de organisatie is de Raad van Bestuur verantwoordelijk voor strategische vraagstukken ten aanzien van informatiebeveiliging. In de praktijk is één bestuurslid verantwoordelijk voor informatiebeveiliging en wordt daarbij ondersteund door de (C)ISO.

[2] Definities volgens het SURF Informatiebeveiligingsbeleid: Standaarden zijn standaard maatregelen die verplicht zijn om uit te voeren. Procedures zijn concrete stapsgewijze aanwijzingen hoe bepaalde taken of acties uitgevoerd moeten worden, deze hebben een verplicht karakter. Richtlijnen zijn aanbevelingen in het kader van de bedrijfsvoering die niet een verplichtend karakter hebben en niet essentieel zijn voor de werking van een stelsel. Een richtlijn geeft dus een voorbeeld hoe bepaalde normen, standaarden, technieken of maatregelen te implementeren of te hanteren zijn. Een richtlijn kan meer specifiek zijn toegesneden op een team of op een bepaald aandachtsgebied.

Proceseigenaar	Een Proceseigenaar is iemand die verantwoordelijk is voor een van de primaire of ondersteunende processen, al dan niet gebruikmakend van meerdere systemen. Vaak is de proceseigenaar van een primair proces (bijvoorbeeld human resources, finance, informatiebeveiliging) ook formeel intern verantwoordelijk voor de gegevens die in dat proces en de daarvan afgeleide processen worden verwerkt (informatie- of broneigenaar)
Dienstverantwoordelijke	Als dienstverantwoordelijke wordt bedoeld de lijnmanager of product manager die verantwoordelijk is voor een product of dienst en de bijbehorende informatiesystemen.

In de BIS is bij iedere control aangegeven wie de verantwoordelijke is. De BIS verplicht wel daarmee om de controls en BIS-maatregelen die bij de rollen staan intern toe te delen en hierbij rekening te houden met voldoende functiescheiding.
Bij een aantal controls is zowel de Dienstverantwoordelijke als de Proceseigenaar opgenomen. Uitgangspunt daarbij is dat de dienstverantwoordelijke de eindverantwoordelijke is.
De algemene organisatie van de informatiebeveiliging, waaronder verantwoordelijkheden, taken en bevoegdheden is terug te vinden in het informatiebeveiligingsbeleid.

3. Basisbeveiligingsniveaus

Zoals in paragraaf 2.1 beschreven, onderscheidt de BIS twee basisbeveiligingsniveaus (BBN's). Ieder BBN bestaat uit een aantal controls, een aantal verplichte maatregelen en een verantwoordings- en toezichtregime. Niveau 2 bouwt voort op niveau 1. Daarbij vult BBN2 de controls van BBN1 aan of vervangt deze door zwaardere maatregelen.

3.1 BBN1

Voor informatiesystemen binnen SURF vormt BBN1 het uitgangspunt. BBN1 is van toepassing indien informatie wordt verwerkt op niveau laag of midden volgens de risicoklassen uit het SURF Juridisch Normenkader. Daarbij kan gedacht worden aan het verwerken van basis persoonsgegevens of onderzoeksgegevens die bij een mogelijk incident niet zullen leiden tot verlies van intellectuele rechten en gevoelige kennis en kunde.

BBN1 is het minimum niveau en geldt voor alle systemen, tenzij op basis van de gemaakte risico analyse en data classificatie blijkt dat er zwaardere maatregelen nodig zijn.

Controls en maatregelen komen voort uit:

- wet- en regelgeving;
- algemeen geldende beveiligingsprincipes (fundamentele controls en maatregelen) zoals genoemd in het SURF informatiebeveilingsbeleid.

3.2 BBN2

BBN2 richt zich op de bescherming van vertrouwelijke, gevoelige informatie waarbij weerstand geboden moet worden tegen allerlei vormen van dreigingen, zowel interne als externe dreigingen. Daarbij kan gedacht worden aan het verwerken van bijzondere persoonsgegevens of onderzoeksgegevens waarbij gevoelige kennis en kunde een rol spelen of de intellectuele rechten van groot belang zijn.
BBN2 is van toepassing indien verlies van informatie een grote impact heeft voor de belangen van de eigenaar van de informatie en de daarmee gepaard gaande belangen van SURF waarvan niet uit te leggen is als deze informatie niet gerubriceerd is en beschermd wordt op het niveau van BBN1;

4. Verantwoording over de BIS

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.

4.1 Verantwoordelijkheid afhankelijk van basisbeveiligingsniveau

De ISO 27001 en het SURF-informatiebeveiligingsbeleid bepalen dat het lijnmanagement vaststelt dat de getroffen maatregelen aantoonbaar overeenstemmen met de beveiligingseisen en dat deze maatregelen worden nageleefd.

Voor diensten en verwerkingen van informatie op BBN1 en BBN2 niveau is de dienstverantwoordelijke of indien toegewezen de proceseigenaar verantwoordelijk voor het nemen van beslissingen.

Voor BBN1 en BBN2 geldt dat de dienstverantwoordelijke of de proceseigenaar het beveiligingsplan[3] van het informatiesysteem voor ingebruikname (bij voorkeur in ontwerp/ ontwikkelfase) voorlegt aan de ISO voor advies.

Voor BBN2 geldt dat vooraf toestemming verleend moet worden door de Raad van Bestuur voor het verwerken van gevoelige en bijzondere informatie. Voor het verlenen van toestemming is mandatering mogelijk.

4.2 Explains op BIS-maatregelen

De verantwoordelijke voor een dienst of verwerking dient te beschikken over een registratie van BIS-maatregelen waaraan niet of nog niet geheel kan worden voldaan. Dit zijn explains volgens het ‘comply or explain’[4] principe. Daarbij worden de daaruit voortvloeiende risico’s tevens aangegeven.

Explains ten aanzien van BIS-maatregelen kunnen bij het samenwerken in ketens zorgen voor een verschil in bescherming tussen partijen waardoor een risico ontstaat voor de verwerkte (en gedeelde) informatie. Diensten met explains, moeten dit afstemmen met hun samenwerkings- of ketenpartners zodat ze samen passende maatregelen of tijdelijke maatregelen treffen die het risico mitigeren of verkleinen zolang de explains niet conform de BIS geïmplementeerd zijn.

---

[3] Dit kan ook een securityplan zijn.

[4] In het SURF informatiebeveiligingsbeleid wordt dit het “pas toe of leg uit” principe genoemd.

4.3 Kader BIS

Ieder informatiesysteem wordt ingedeeld in een Basis Beveiligingsniveau (BBN) categorie: BBN1 of BBN2. Het BBN bepaalt welke controls vervolgens verplicht moeten worden doorlopen en geïmplementeerd. Per control worden bepaald welke maatregelen in aanvulling op de verplichte BIS-maatregelen nodig zijn. Voor meer toelichting op de opzet van de BIS en de BBN's wordt verwezen naar deel 1, de achtergrondinformatie van de BIS.

In het document zijn de controls dan als volgt opgebouwd:

Controlnummer overeenkomstig met ISO 27002	BBN (1, 2)	Controltekst (SURF of ISO 27002)	**Verantwoordelijke(n)** Bestuur Proceseigenaar Dienstverantwoordelijke
Maatregel nummer	BBN(1 of 2)	Maatregel tekst	
		Beleid (Policy \ Richtlijn) (optioneel)	

Om het verschil tussen de ISO 27002 controls en de SURF-maatregelen te duiden, zijn verschillende kleurmarkeringen gebruikt:

- Blauw zijn de SURF of ISO 27002 controls.
- Groen zijn BIS-maatregelen op BBN 1 niveau.
- Oranje zijn de BIS-maatregelen op BBN 2 niveau.

Waar passend wordt verwezen naar interne SURF (beleids-)documenten om invulling te geven aan de maatregelen. Deze documenten kunnen zowel verplichte onderdelen (standaarden en procedures) als implementatierichtlijnen bevatten die niet verplicht zijn. Deze verwijzingen naar de documenten hebben geen nummer en zijn als een document titel weergegeven.

In de kolom 'Verantwoordelijke(n)' staat aangegeven wie voor de uitvoering van de control verantwoordelijk is: Raad van Bestuur (eindverantwoordelijke voor de bedrijfsvoering van de organisatie), Proceseigenaar en/of Dienstverantwoordelijke.

BBN Toets

Bij het doorlopen van deze toets is BBN1 het uitgangspunt voor alle informatiesystemen.

Stap 1: Is BBN1 voldoende?
BBN1 is het standaard minimum niveau bij informatiesysteem. Het kan echter zijn dat BBN1 niet voldoende is. BBN1 is onvoldoende indien:

- informatie verwerkt wordt die onder het niveau hoog valt volgens risicoklassen van het SURF Juridische Normenkader;

of
- informatie verwerkt wordt die geclassificeerd is als vertrouwelijkheidsniveau hoog.

In elk van deze gevallen is BBN2 van toepassing.

Stap 2: Is BBN2 te zwaar?

Bij BBN2 informatiesystemen kan het ongewenst of onbedoeld openbaren van informatie leiden tot BBN2-schade:

- (politieke) schade aan een bestuurder: bestuurder moet verantwoording afleggen aan de (gekozen) controlerende organen, bijvoorbeeld n.a.v. verantwoordingsvragen;

of
- financiële gevolgen: niet meer op te vangen binnen de begroting van de SURF of SURF geen accountantsverklaring afgegeven;

of
- bindende aanwijzing van de AP in verband met schending van de privacy;

of
- waarschijnlijk leidt tot een hoog risico voor de rechten en vrijheden van betrokkenen

of
- verlies van vertrouwen (door doelgroep); stoppen of mijden van gebruik van diensten door onderzoekers en studenten;

of
- directe imagoschade, bijvoorbeeld door negatieve publiciteit.

Zijn dergelijke schades niet aan de orde, dan is BBN1 van toepassing.

Controls en SURF-maatregelen

Voor de herkenbaarheid is gekozen om de nummering van de hoofdstukken en de controls in lijn te houden met de nummering uit de ISO 27002.

5. Informatiebeveiligingsbeleid

Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

5.1 Aansturing door de directie van de informatiebeveiliging

5.1.1	1	**Beleidsregels voor informatiebeveiliging** Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Bestuur
5.1.1.1	1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste 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.	
		Zie: SURF Informatiebeveiligingsbeleid	

5.1.2	1	**Beoordeling van het informatiebeveiligingsbeleid** Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Bestuur
5.1.2.1	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.	

6. Organiseren va Informatie beveiliging

6.1 Interne Organisatie

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

6.1.1	**1**	**Rollen en verantwoordelijkheden bij informatiebeveiliging** Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Bestuur
6.1.1.1	1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging.	
6.1.1.2	1	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	
6.1.1.3	1	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	
		Zie: SURF SO-functieprofiel	
6.1.2	**1**	**Scheiding van taken** Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Dienstverantwoordelijke Proceseigenaar
6.1.2.1	1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	
6.1.3	**1**	**Contact met overheidsinstanties** Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.	Bestuur Dienstverantwoordelijke Proceseigenaar
6.1.3.1	1	Er is door de organisatie vastgelegd wie met welke (overheids-) instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/ calamiteiten).	
6.1.3.2	2	Het contactoverzicht wordt jaarlijks geactualiseerd.	
6.1.4	**1**	**Contact met speciale belangengroepen** Er behoren passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties te worden onderhouden.	Bestuur Dienstverantwoordelijke Proceseigenaar
6.1.5	**1**	**Informatiebeveiliging in projectbeheer** Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	Dienstverantwoordelijke Proceseigenaar
6.1.5.1	1	Security dient in projecten gewaarborgd te worden door het "security by design" principe.	

6.2 Mobiele apparatuur en telewerken

Doelstelling: Het waarborgen van de veiligheid van telewerken5 en het gebruik van mobiele apparatuur.

6.2.1	1	**Beleid voor mobiele apparatuur** Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	Dienstverantwoordelijke Proceseigenaar
6.2.1.1	1	Mobiele apparatuur (zoals een laptop, tablet en smartphone) is zo ingericht dat de toegang tot de device is beschermd door middel van een toegangsbeveiligingsmechanisme en dat de gegevens op de ingebouwde opslag-devices zijn beschermd door middel van versleuteling.	
6.2.1.2	1	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), d) en e) worden nageleefd.	

6.2.2	2	**Telewerken** Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.	Dienstverantwoordelijke Proceseigenaar
		Zie: handreiking Telewerken	

[5] Telewerken: arbeid die op afstand van de werk- of opdrachtgever wordt uitgevoerd met behulp van informatie- en communicatietechnologie (ICT). SURF maakt geen onderscheid van telewerken en op kantoorwerken. Dit is vastgelegd in de SURF werkplekbeleid.

7. Veilig personeel

7.1 Voorafgaand aan het dienstverband

Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen.

7.1.1	1	**Screening** Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.	Bestuur Proceseigenaar
7.1.1.1	1	Bij aanstelling nieuw personeel vindt verificatie plaats van identiteitspapieren, diploma's en certificaten.	
7.1.1.2	1	Indien de functie een Verklaring Omtrent het Gedrag (VOG) vereist moet de medewerker deze bij indiensttreding overleggen.	

7.1.2	1	**Arbeidsvoorwaarden** De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	Bestuur Proceseigenaar
7.1.2.1	1	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.	

7.2 Tijdens het dienstverband

Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.

7.2.1	1	**Bestuursverantwoordelijkheden** Het bestuur behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	Bestuur
7.2.2	1	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging.** Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	Bestuur Proceseigenaar
7.2.2.1	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	

7.2.2.2	1	Alle medewerkers en contracten worden door middel van awareness trainingen, presentaties en/of campagnes bijgeschoold.	
7.2.2.3	1	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen- en diensten hebben binnen twee maanden na indiensttreding een introductie informatiebeveiliging gevolgd.	
7.2.2.4	1	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	

7.2.3	**1**	**Disciplinaire procedure** Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Bestuur Proceseigenaar
		Zie: SURF Acceptable Use Policy	

7.3 Beëindiging en wijziging van dienstverband

Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.

7.3.1	**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 behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht.	Bestuur Proceseigenaar
7.3.3.1	1	Voor beëindigen en wijziging van dienstverband moeten procedures te zijn opgesteld waarin beschreven staat hoe verantwoordelijken en rechten worden overgedragen. De procedure dient ten minste de volgende aspecten te 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 IT middelen; e. overdracht van SURF beheerde IT middelen. De procedures dienen minimaal jaarlijks gecontroleerd te worden.	

8. Beheer van bedrijfsmiddelen

8.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren

8.1.1	**1**	**Inventariseren van bedrijfsmiddelen** Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.	Dienstverantwoordelijke Proceseigenaar
8.1.1.1	1	Er dient een Asset Management proces te zijn waarbij bedrijfsmiddelen geïnventariseerd en bijgehouden worden. Het vastgesteld beveiligingsniveau is opgenomen in het Asset Management.	
8.1.2	**1**	**Eigendom van bedrijfsmiddelen** Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.	Dienstverantwoordelijke Proceseigenaar
8.1.2.1	1	De eigenaar is verantwoordelijk voor de lifecycle van de asset, ongeacht waar deze fysiek uitgevoerd worden (incl. cloud). De volgende aspecten zijn minimaal onderdeel hiervan: installeren, beheren, up-to-date houden en beveiliging van de asset, uitfaseren van de asset.	
8.1.3	**1**	**Aanvaardbaar gebruik van bedrijfsmiddelen** Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Dienstverantwoordelijke Proceseigenaar
8.1.3.1	1	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.	
8.1.3.2	1	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels.	
8.1.4	**1**	**Teruggeven van bedrijfsmiddelen** Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven.	Bestuur Procesverantwoordelijke

8.2 Informatieclassificatie

Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.

8.2.1	1	**Classificatie van informatie** Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Proceseigenaar Dienstverantwoordelijke
		Zie: Beleid Gegevensclassificatie	
8.2.1.1	1	De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.	
8.2.2	1	**Informatie labelen** Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Procesverantwoordelijke
8.2.3	1	**Behandelen van bedrijfsmiddelen** Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Procesverantwoordelijke

8.3 Behandelen van media

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

8.3.1	1	**Beheer van verwijderbare media** Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Proceseigenaar Dienstverantwoordelijke
8.3.1.1	1	Er is een verwijderinstructie waarin is opgenomen dat van herbruikbare media die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd (Referentie ISO27002 – implementatierichtlijn 8.3.2.a).	
8.3.1.2	2	De wijze waarop vertrouwelijk of hoger geclassificeerde informatie is opgeslagen, voldoet aan de eisen van het Nationaal Bureau voor Verbindingsbeveiliging (NBV/AIVD).	
		Handreiking: NBV brochure BSPA | Publicatie | AIVD	
8.3.2	1	**Verwijderen van media** Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Proceseigenaar Dienstverantwoordelijke
		Zie: Procedure veilig verwijderen of hergebruiken van IT middelen. Zie: SURF E-waste beleid	

8.3.2.1	1	Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, 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.	
8.3.2.2	1	Indien data dragers en/of data door een externe partij wordt uitgevoerd is een certificaat van vernietiging verplicht.	
8.3.2.3	2	Media die vertrouwelijke informatie bevatten zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden. Verwijdering vindt plaats op een veilige manier, bijv. 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 ISO27002 – implementatierichtlijn 8.3.2.a)	

8.3.3	**1**	**Media fysiek overdragen** Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Bestuur Proceseigenaar Dienstverantwoordelijke
8.3.3.1	2	Er is beleid voor het fysiek transport van media vastgesteld.	
		Zie: Handreiking omgaan met verwijderbare media	
8.3.3.2	2	Het gebruik van koeriers of transporteurs voor vertrouwelijk of hoger geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.	

9. Toegangsbeveiliging

9.1 Bedrijfseisen voor toegangsbeveiliging

Doelstelling: Toegang tot informatie en informatieverwerkende faciliteiten beperken.

9.1.1	1	**Beleid voor toegangsbeveiliging** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Bestuur

9.1.2	1	**Toegang tot netwerken en netwerkdiensten** Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Proceseigenaar Dienstverantwoordelijke
		Zie: Logische toegangsbeveiliging	
9.1.2.1	1	De toegang tot netwerk en netwerkdiensten vindt plaats op basis van gedefinieerde security categorieën.	
9.1.2.2	1	Alleen geauthentiseerde apparatuur kan toegang krijgen tot een vertrouwde zone.	
9.1.2.3	1	Gebruikers met eigen of ongeauthentiseerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een niet vertrouwde/daarvoor bedoelde zone.	

9.2 Beheer van toegangsrechten van gebruikers

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

9.2.1	1	**Registratie en afmelden van gebruikers** Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Proceseigenaar Dienstverantwoordelijke
		Zie: Logische toegangsbeveiliging	
9.2.1.1	1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	
9.2.1.2	1	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	

9.2.2	1	**Gebruikers toegang verlenen** Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Proceseigenaar Dienstverantwoordelijke
9.2.2.1	1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	
9.2.2.2	1	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	

9.2.2.3	1	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	
9.2.2.4	1	Eerder uitgegeven accounts en bijbehorende unieke identifiers worden niet hergebruikt.	
9.2.3	**1**	**Beheren van speciale toegangsrechten** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	Proceseigenaar Dienstverantwoordelijke
9.2.3.1	1	De toewijzing en het gebruik van speciale bevoegdheden worden tot een minimum beperkt.	
9.2.3.2	2	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	
9.2.4	**1**	**Beheer van geheime authenticatie-informatie van gebruikers** Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	Proceseigenaar Dienstverantwoordelijke
9.2.5	**1**	**Beoordeling van toegangsrechten van gebruikers** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Proceseigenaar Dienstverantwoordelijke
9.2.5.1	1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.	
9.2.5.2	1	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident	
9.2.5.3	2	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	
9.2.6	**1**	**Toegangsrechten intrekken of aanpassen** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	Proceseigenaar Dienstverantwoordelijke

9.3 Verantwoordelijkheden van gebruikers

Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.

9.3.1	**1**	**Geheime authenticatie-informatie gebruiken** Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	Bestuur Dienstverantwoordelijke
9.3.1.1	1	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.	

9.4 Toegangsbeveiliging van systeem en toepassing

Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.

9.4.1	**1**	**Beperking toegang tot informatie** Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	Dienstverantwoordelijke Proceseigenaar
9.4.1.1	1	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie waarborgen.	
9.4.1.2	1	Gebruikers kunnen alleen die informatie inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak. Daarbij wordt als uitgangspunt 'Least Privilege' en 'Need to Know' principes gehanteerd.	
9.4.2	**1**	**Beveiligde inlogprocedures** Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	Dienstverantwoordelijke Proceseigenaar
9.4.2.1	1	Voor toegang tot alle systemen en applicaties (ongeacht waar deze zich bevinden) is minimaal Multi Factor Authenticatie nodig.	
9.4.2.2	1	Toegang ten behoeve van het beheer van systemen en applicaties wordt uitsluitend vanaf een interne vertrouwde zone toegestaan.	
9.4.2.3	1	Voor het verlenen van toegang tot het netwerk door externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	
9.4.3	**1**	**Systeem voor wachtwoordbeheer** Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	Dienstverantwoordelijke Proceseigenaar
9.4.3.1	1	Wachtwoorden moeten voldoen aan de SURF wachtwoorden beleid. Het aantal inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.	
9.4.3.2	1	Wachtwoorden worden volgens de vastgelegde richtlijnen vernieuwd (zie ook 9.4.3.1).	
9.4.3.3	1	Het wachtwoordbeleid wordt geautomatiseerd afgedwongen.	
9.4.3.4	1	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van 24 uur en moeten bij het eerste gebruik worden gewijzigd.	
9.4.3.5	1	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.	
		Zie: Veilige wachtwoorden	

9.4.4	**1**	**Speciale systeemhulpmiddelen gebruiken** Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	Dienstverantwoordelijke Proceseigenaar
9.4.4.1	1	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.	
9.4.4.2	1	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	

9.4.5	**1**	**Toegangsbeveiliging op programmabroncode** Toegang tot de programmabroncode behoort te worden beperkt.	Dienstverantwoordelijke Proceseigenaar
9.4.5.1	**1**	De toegang tot de in operatie zijnde programmabroncode van de dienst hoort te worden beperkt.	

10. Cryptografie

10.1 Cryptografische beheersmaatregelen

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

10.1.1	**1**	**Beleid inzake het gebruik van crvptografische beheersmaatregelen** Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	Bestuur
10.1.1.1	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) bij inter-organisatie communicatie wordt het beleid onderling vastgesteld.	
10.1.1.2	1	Cryptografische toepassingen voldoen aan passende standaarden.	
		Zie: Handreiking cryptografie	

10.1.2	**1**	**Sleutelbeheer** Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.	Dienstverantwoordelijke Proceseigenaar
10.1.2.1	1	De standaard ISO-11770 wordt gehanteerd voor het beheer van cryptografische sleutels.	
		Zie: Handreiking cryptografie	

11. Fysieke beveiliging en beveiliging van de omgeving

11.1 Beveiligde gebieden

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

11.1.1	**1**	**Fysieke beveiligingszone** Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	Bestuur
11.1.1.1	1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.	

11.1.2	**1**	**Fysieke toegangsbeveiliging** Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Bestuur
11.1.2.1	1	Er zijn toegangsregels vastgelegd. De toegang tot ruimtes waarin systemen en/of informatie zijn opgeslagen zijn beveiligd d.m.v. een Identificatie Authenticatie en Autorisatie systeem en er vindt logging van toegang plaats. Identiteit dient vooraf vastgesteld te worden	
		Zie: Toegang en veiligheid computervloeren	

11.1.3	**1**	**Kantoren, ruimten en faciliteiten beveiligen** Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	Proceseigenaar Dienstverantwoordelijke
11.1.3.1	1	Sleutelbeheer is ingericht op basis van een sleutelplan.	

11.1.4	**1**	**Beschermen tegen bedreigingen van buitenaf** Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	Proceseigenaar Dienstverantwoordelijke
11.1.4.1	1	Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.	
11.1.4.2	1	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.	

11.1.5	**1**	**Werken in beveiligde gebieden** Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	Proceseigenaar Dienstverantwoordelijke
11.1.5.1	1	In beveiligde gebieden dient iedereen een zichtbare identificatie te dragen (inclusief gasten).	

11.1.6	**1**	**Laad- en loslocatie** Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te	Proceseigenaar Dienstverantwoordelijke

		vermijden.	

11.2 Apparatuur

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

11.2.1	1	**Plaatsing en bescherming van apparatuur** Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	Dienstverantwoordelijke
11.2.2	1	**Nutsvoorzieningen** Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Dienstverantwoordelijke
11.2.3	1	**Beveiliging van bekabeling** Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	Dienstverantwoordelijke
11.2.4	1	**Onderhoud van apparatuur** Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Dienstverantwoordelijke
11.2.5	1	**Verwijdering van bedrijfsmiddelen** Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	Dienstverantwoordelijke
11.2.6	1	**Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein** Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	Dienstverantwoordelijke
11.2.7	1	**Veilig verwijderen of hergebruiken van apparatuur** Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	Dienstverantwoordelijke
		Zie maatregelen van 8.3.2.	
11.2.8	1	**Onbeheerde gebruikersapparatuur** Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Proceseigenaar

11.2.9	**1**	**'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 te worden ingesteld.	Bestuur Proceseigenaar
		Zie: Beleid Clear desk clear screen	
11.2.9.1	1	Een onbeheerde werkplek in een ongecontroleerde omgeving is altijd vergrendeld.	
11.2.9.2	1	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screenlock na een inactiviteit van maximaal 5 minuten.	
11.2.9.3	1	Sessie op remote desktops worden op het remote platform vergrendeld na 15 minuten. Het overnemen van sessie op remote desktops op een ander client apparaat is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd.	
11.2.9.4	1	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van de token de toegangsbeveiligingslock automatisch geactiveerd.	
11.2.9.5	1	Whiteboards, flipovers en dergelijk in algemene ruimten (vergaderzalen en flexruimten) moeten na gebruik worden geschoond.	

12. Beveiliging Bedrijfsvoering

12.1 Bedieningsprocedures en verantwoordelijkheden

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

12.1.1	1	**Gedocumenteerde bedieningsprocedures** Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	Dienstverantwoordelijke Proceseigenaar

12.1.2	1	**Wijzigingsbeheer** Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	Dienstverantwoordelijke Proceseigenaar
12.1.2.1	1	Voor wijzigingen is een procedure voor wijzigingsbeheer ingericht. In de procedure wordt minimaal aandacht besteed aan: (a) het administreren van wijzigingen; (b) risicoafweging van mogelijke gevolgen van dewijzigingen; (c) goedkeuringsprocedure voor wijzigingen.	

12.1.3	1	**Capaciteitsbeheer** Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	Dienstverantwoordelijke
12.1.3.1	1	Met betrekking tot externe koppelingen zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief kunnen beïnvloeden (bijv. DDoS attacks) te signaleren en hierop te reageren.	

12.1.4	1	**Scheiding van ontwikkel-, test- en productieomgevingen** Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Dienstverantwoordelijke Proceseigenaar
12.1.4.1	1	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	
12.1.4.2	1	Wijzigingen op de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	

12.2 Bescherming tegen malware

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

12.2.1	1	**Beheersmaatregelen tegen malware** Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Proceseigenaar Dienstverantwoordelijke
12.2.1.1	1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	

12.2.1.2	1	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.	
12.2.1.3	1	Software en bijbehorende herstelsoftware die malware opspoort zijn geïnstalleerd en worden regelmatig geüpdatet.	
12.2.1.4	1	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te 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.	
12.2.1.5	1	De malware scan wordt op verschillende omgevingen uitgevoerd, bijv. op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie	

12.3 Back-up

Doelstelling: Beschermen tegen het verlies van gegevens.

12.3.1	**1**	**Beheersmaatregelen tegen malware** Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Procesverantwoordelijke Dienstverantwoordelijke
		Zie: Beleid Backup en Restore	
12.3.1.1	1	Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld	
12.3.1.2	1	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	
12.3.1.3	1	Ter voorkoming van beschadiging tijdens een calamiteit dient minimaal één back-up kopie fysiek op een remote locatie opgeslagen te worden. De minimale afstand van de remote locatie tot het datacenter (hoofdlocatie) bedraagt 5 km.	
12.3.1.4	1	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de betrouwbaarheid te waarborgen als ze in noodgevallen uitgevoerd moet worden.	

12.4 Verslaglegging en monitoren

Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.

12.4.1	**1**	**Gebeurtenissen registreren** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Dienstverantwoordelijke Proceseigenaar

12.4.1.1	1	Een logregel bevat minimaal de gebeurtenis: - de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; - het gebruikte apparaat; - het resultaat van de handeling (bijvoorbeeld: Lezen, Schrijven, Modificeren en Verwijderen); - datum en tijdstip van de gebeurtenis.	
12.4.1.2	1	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	
12.4.1.3	1	Alle authenticatielogs worden doorgestuurd naar de centrale logging server	
12.4.1.4	1	De informatie verwerkende omgeving wordt gemonitord op basis van een risico-inschatting, mede aan de hand van en de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	
12.4.1.5	1	Netwerk flow informatie wordt gesampled en naar een centrale data collector gestuurd.	
12.4.1.6	1	Logging is aangezet voor alle verwerkingen van de gegevens door het systeem of applicaties. Dit zal alle soorten verwerkingen betreffen: Lezen, Schrijven, Modificeren en Verwijderen.	
12.4.1.7	2	Een geautomatiseerd monitoring systeem beoordeelt de log files en produceert alarmen in geval van onregelmatigheden of situaties die op een potentieel risico wijzen.	
12.4.2	**1**	**Beschermen van informatie in logbestanden** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Dienstverantwoordelijke Proceseigenaar
12.4.2.1	1	Er is een overzicht van logbestanden die worden gegenereerd met vermelding van opslaglocatie.	
12.4.2.2	1	Ten behoeve van de loganalyse moeten logbestanden voor een periode van minimaal 6 maanden bewaard worden. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	
12.4.2.3	1	Log files worden beschermd tegen wijziging of vernietiging. Toegang tot de logs wordt gelogd.	
12.4.2.4	2	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	
12.4.2.5	2	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.	
12.4.3	**1**	**Logbestanden van beheerders en operators** Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	Dienstverantwoordelijke Proceseigenaar
12.4.3.1	2	Alle acties van de system admins worden gelogd.	
12.4.4	**1**	**Kloksynchronisatie** De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	Dienstverantwoordelijke
		Zie: Richtlijn voor instellen van de systeemklok	

12.4.4.1	1	De machine bevat de juiste tijd, tijdzone (locale tijdzone) en datum.	
12.4.4.2	1	De systeemklok en de tijd-synchronisatie via de SURF NTP (Network Time Protocol) servers zijn ingesteld.	

12.5 Beheersing van operationele software

Doelstelling: De integriteit van operationele systemen waarborgen.

12.5.1	1	**Software installeren op operationele systemen** Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	Dienstverantwoordelijke

12.6 Beheer van technische kwetsbaarheden

Doelstelling: Benutting van technische kwetsbaarheden voorkomen.

12.6.1	1	**Beheer van technische kwetsbaarheden** Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.	Dienstverantwoordelijke
		Zie: Handreiking penetratietesten	
12.6.1.1	1	Voor elk aan het SURF-netwerk aangesloten systeem en de daarop geïnstalleerde software dient ongeacht alle andere gerealiseerde security- en beheermaatregelen patch management ingericht te zijn.	
12.6.1.2	1	De afdeling waar het beheer van het systeem onder valt moet voor een adequate patch schema zorgen.	
12.6.1.3	1	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.	
12.6.1.4	1	Security patches moeten met voorrang worden behandeld. Dat betekent dat er een onmiddellijke beoordeling van impact en prioriteit moet worden gemaakt.	
12.6.1.5	1	Als een patch met een hoge prioriteit niet snel uitgerold kan worden, bijvoorbeeld op technische gronden, dan moet daarvoor een adequate work-around of maatregelen worden ingevoerd om het systeem of de applicatie te beschermen tegen kwetsbaarheden.	
12.6.1.6	1	In het kader van systeem hardening, dienen overbodige componenten, services en software op de servers en netwerkelementen te worden uitgeschakeld om het risico op technische kwetsbaarheden en succesvolle aanvallen te minimaliseren. Met andere woorden op het systeem draaien uitsluitende de noodzakelijk onderdelen.	

12.7 Overwegingen betreffende audits van informatiesystemen

Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.

12.7.1	1	**Beheersmaatregelen betreffende audits van informatiesystemen** Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	Dienstverantwoordelijke Proceseigenaar

13. Communicatiebeveiliging

13.1 Beheer van netwerkbeveiliging

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

13.1.1	1	**Beheersmaatregelen voor netwerken** Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Dienstverantwoordelijke
13.1.2	1	**Beveiliging van netwerkdiensten** Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Dienstverantwoordelijke
13.1.2.1	1	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt tegen en geanalyseerd op kwaadaardige elementen middels detectie-voorzieningen zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	
		Handreiking voor implementatie van detectie-oplossingen: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/handreiking-voor-implementatie-van-detectie-oplossingen/Handreiking-voor-implementatie-van-detectie-oplossingen.pdf	
13.1.2.2	1	Aansluiting op bedrijfsnetwerken (inclusief wireless) is alleen mogelijk na authenticatie.	
13.1.2.3	1	Voor externe toegang tot interne netwerken wordt gebruikt gemaakt van een VPN server voorzien van Multi Factor Authenticatie.	
13.1.2.4	1	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied, wordt gebruik gemaakt van encryptie middelen.	
13.1.2.5	1	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.	
13.1.2.6	1	Netwerkverkeer wordt zowel inkomend als uitgaand gefilterd. Filtering wordt ingezet aan de hand van de aard van de te beschermen gegevens en informatiesystemen en mede op basis van een risico-inschatting.	
		Zie: Handreiking wijzigen van configuratie van veiligheid devices	
13.1.3	1	**Beveiliging van netwerkdiensten** Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Dienstverantwoordelijke

		Zie: Handreiking beveiligingsniveaus en gestructureerde VLAN indeling	
13.1.3.1	1	Ieder VLAN heeft een gedefinieerd security beveiligingsniveau.	
13.1.3.2	1	De beveiliging van de IT-systemen vindt plaats op basis van gedefinieerde security beveiligingsniveaus conform een gestructureerde VLAN indeling.	

13.2 Informatietransport

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

13.2.1	**1**	**Beleid en procedures voor informatietransport** Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	Bestuur Proceseigenaar Dienstverantwoordelijke
13.2.2	**1**	**Overeenkomsten over informatietransport** Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Dienstverantwoordelijke Proceseigenaar
13.2.3	**1**	**Elektronische berichten** Gevoelige en vertrouwelijke informatie die is opgenomen in elektronische berichten behoordpassend te zijn beschermd.	Dienstverantwoordelijke
13.2.3.1	1	Voor de beveiliging van elektronische berichten gelden de vastgestelde standaarden tegen malware, phishing, afluisteren en modificatie zoals SPF, DKIM, DMARC en encryptie.	
13.2.3.2	1	E-mail berichten worden geautomatiseerd gescand op aanwezigheid van spamberichten en virussen en andere kwaadaardige software.	
13.2.3.3	1	Data in transit dient altijd versleuteld te zijn. Maak gebruik van certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn o.a. digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenen.	
13.2.3.4	1	In de Acceptable Use Policy is beschreven hoe de medewerkers om moeten gaan met internet en email gebruik.	
13.2.4	**1**	**Vertrouwelijkheids- of geheimhoudingsovereenkomst** Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	Bestuur Proceseigenaar Dienstverantwoordelijke

14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen

14.1 Beveiligingseisen voor informatiesystemen

Doelstelling: Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.

14.1.1	1	**Analyse en specificatie van informatiebeveiligingseisen** De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaandeinformatiesystemen.	Dienstverantwoordelijke Proceseigenaar
14.1.1.1	1	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de SURF baseline.	
14.1.2	1	**Toepassingen op openbare netwerken beveiligen** Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	Dienstverantwoordelijke
14.1.2.1	1	Zie maatregel 13.2.3.3 (Maak gebruik van SURFcertificaten)	
14.1.3	1	**Transacties van toepassingen beschermen** Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	Dienstverantwoordelijke
14.1.3.1	1	Zie maatregel 13.2.2.3 (Maak gebruik van SURFcertificaten)	

14.2 Beveiliging in ontwikkelings- en ondersteunende processen

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

14.2.1	1	**Beleid voor beveiligd ontwikkelen** Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.	Bestuur Dienstverantwoordelijke Proceseigenaar
14.2.1.1	1	Security by design is de uitgangspunt voor de ontwikkeling van software en systemen.	
14.2.1.2	1	Het testen en ontwikkelen van software en systemen wordt uitgevoerd op basis van het OTAP principe.	
		Zie: Handreiking grip op Secure Software Development (SSD).	

14.2.2	**1**	**Procedures voor wijzigingsbeheer met betrekking tot systemen** Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	Dienstverantwoordelijke Proceseigenaar
14.2.2.1	1	Voor het wijzigingsbeheer wordt een algemeen geaccepteerd framework zoals FitSM of ITIL gebruikt.	
		Zie: Handreiking proces wijzigingsbeheer	
14.2.3	**1**	**Technische beoordeling van toepassingen na wijzigingen besturingsplatform** Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	Dienstverantwoordelijke
14.2.4	**1**	**Beperkingen op wijzigingen aan softwarepakketten** Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd.	Dienstverantwoordelijke
14.2.5	**1**	**Principes voor engineering van beveiligde systemen** Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	Dienstverantwoordelijke
14.2.5.1	1	Zie control 14.2.1.1	
14.2.6	**1**	**Beveiligde ontwikkelomgeving** Organisaties behoren 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.	Dienstverantwoordelijke
14.2.6.1	1	Zie control 14.2.1.2	
14.2.7	**1**	**Uitbestede softwareontwikkeling** Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	Proceseigenaar
14.2.7.1	1	Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd.	
14.2.8	**1**	**Testen van systeembeveiliging** Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	Dienstverantwoordelijke
14.2.9	**1**	**Systeemacceptatietests** Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	Dienstverantwoordelijke Proceseigenaar
14.2.9.1	1	Een systeem of applicatie wordt aan een van te voren gedefinieerde acceptatietest onderworpen.	
14.2.9.2	1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken zoals bijvoorbeeld TMap gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	

14.2.9.3	1	Een systeem of applicatie wordt niet geaccepteerd voordat het gewenste niveau van security is bereikt.	
		Zie: Handreiking acceptatiecriteria nieuwe applicaties	

14.3 Testgegevens

Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.

14.3.1	**1**	**Bescherming van testgegevens** Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.	Dienstverantwoordelijke Proceseigenaar
14.3.1.1	1	Productiedata mogen niet als testgegevens gebruikt worden, hiervoor gelden dezelfde maatregelen als in de productieomgeving.	
14.3.1.2	1	Indien het onvermijdelijk is dat productiedata in een testomgeving worden gebruikt moeten deze geanonimiseerd of gepseudonimiseerd te worden.	

15. Leveranciersrelaties

15.1 Informatiebeveiliging in leveranciersrelaties

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

15.1.1	1	**Informatiebeveiligingsbeleid voor leveranciersrelaties** Om risico's te verlagen moeten informatiebeveiligingseisen met de leveranciers worden overeengekomen. Deze moeten overeengekomen en gedocumenteerd worden. De afspraken en overeenkomsten dienen tenminste afspraken te bevatten over de toegang van de leverancier tot de bedrijfsmiddelen.	Bestuur Proceseigenaar
15.1.1.1	1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen t.a.v. informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd.	
15.1.1.2	1	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.	
		Zie: Beleid leveranciersmanagement	
		Zie: Handreiking SURF model verwerkersovereenkomst	

15.1.2	1	**Opnemen van beveiligingsaspecten in leveranciersovereenkomsten** Alle relevante informatiebeveiligingseisen behoren te 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.	Bestuur Proceseigenaar
15.1.2.1	1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.	
15.1.2.2	1	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	
15.1.2.3	1	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.	
15.1.2.4	1	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaard voorwaarden voor inkoop gehanteerd.	
15.1.2.5	1	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 exit-strategie.	
15.1.2.6	2	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.	
		Zie: Beleid leveranciersmanagement	

15.1.3	1	**Toeleveringsketen van informatie- en communicatietechnologie** Overeenkomsten met leveranciers behoren eisen te 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.	Dienstverantwoordelijke Proceseigenaar

15.1.3.1	1	Leveranciers moeten hun keten van toeleveranciers bekend maken en transparant zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers.	

15.2 Beheer van dienstverlening van leveranciers

Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.

15.2.1	1	**Toeleveringsketen van informatie- en communicatietechnologie** Overeenkomsten met leveranciers behoren eisen te 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.	Dienstverantwoordelijke Proceseigenaar
15.2.1.1	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.	
		Zie: Beleid leveranciersmanagement	

15.2.2	1	**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, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Dienstverantwoordelijke Proceseigenaar

16. Beheer van informatiebeveiligingsincidenten

16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen

Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.

16.1.1	1	**Verantwoordelijkheden en procedures** Bestuursverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Bestuur
		Handreiking: Samenhang beheerprocessen en informatiebeveiliging: https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2021/04/201906-Handreiking-Samenhang-Beheerprocessen-en-Informatiebeveiliging-v2.02.docx Handreiking voor implementatie van detectie-oplossingen: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/handreiking-voor-implementatie-van-detectie-oplossingen/Handreiking-voor-implementatie-van-detectie-oplossingen.pdf	
16.1.2	1	**Rapportage van informatiebeveiligingsgebeurtenissen** Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. Diensteigenaar aan proceseigenaar, proceseigenaar aan bestuur.	Bestuur Proceseigenaar Dienstverantwoordelijke
16.1.2.1	1	Alle security incidenten worden gemeld bij CSIRT.	
16.1.2.2	1	Het CSIRT-team geeft opvolging aan security incidenten conform security incidenten procedure en zorgt voor de nodige escalaties.	
16.1.2.3	1	Alle medewerkers en contractanten hebben aantoonbaar kennisgenomen van de security incidenten procedure.	
16.1.2.4	1	Incidenten worden zo snel als mogelijk, maar in ieder geval binnen 24 uur na bekendwording, gemeld bij het CSIRT-team.	
16.1.2.5	1	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.	
16.1.2.6	1	De opvolging van incidenten wordt periodiek gerapporteerd aan de verantwoordelijke.	
16.1.2.7	1	Informatie afkomstig uit de responsible disclosure procedure zijn onderdeel van de incidentrapportage.	
		Zie: Procedure SURF CSIRT charter	
16.1.3	1	**Rapportage van zwakke plekken in de informatiebeveiliging** Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	Dienstverantwoordelijke Proceseigenaar
		Zie maatregel 16.1.2.4	
16.1.3.1	1	Een responsible disclosure procedure is gepubliceerd en ingericht.	
16.1.4	1	**Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen** Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en	Dienstverantwoordelijke Proceseigenaar

		er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	
16.1.4.1	1	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verwerkende systemen, behoren zo snel mogelijk (binnen 24 uur) te worden gemeld aan CSIRT. CSIRT maakt vervolgens samen met de verantwoordelijke afdeling een impact analyse van het incident en definieert nodige herstelmaatregelen.	
16.1.5	**1**	**Respons op informatiebeveiligingsincidenten** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Dienstverantwoordelijke Proceseigenaar
16.1.6	**1**	**Lering uit informatiebeveiligingsincidenten** Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Dienstverantwoordelijke Proceseigenaar
16.1.7	**1**	**Verzamelen van bewijsmateriaal** De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Dienstverantwoordelijke Proceseigenaar
16.1.7.1	**1**	**De bewijslast dient vastgelegd te worden.**	

17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

17.1 Informatiebeveiligingscontinuïteit

Doelstelling: Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.

		Zie: Handreiking bedrijfscontinuïteit	
17.1.1	1	**Informatiebeveiligingscontinuïteit plannen** De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen.	Bestuur
17.1.1.1	1	Er dient een crisisplan aanwezig te zijn, deze dient onderdeel te zijn van de informatiebeveiliging continuïteitsplannen.	
17.1.2	1	**Informatiebeveiligingscontinuïteit implementeren** De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Dienstverantwoordelijke Proceseigenaar
17.1.3	1	**Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren** De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Dienstverantwoordelijke Proceseigenaar
17.1.3.1	1	Continuïteitsplannen van bedrijfskritische systemen worden jaarlijks getest op geldigheid en bruikbaarheid. Continuïteitsplannen van overige systemen worden2-jaarlijks getest op geldigheid en bruikbaarheid.	
17.1.3.2	1	Door het uitvoeren van een expliciete risicoafweging worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd.	
17.1.3.3	1	De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten minimaal binnen een week hersteld.	
17.1.3.4	1	Crisisplan worden jaarlijks getest op geldigheid, actualiteit en bruikbaarheid.	

17.2 Redundante componenten

Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.

17.2.1	1	**Beschikbaarheid van informatieverwerkende faciliteiten** Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Dienstverantwoordelijke

18. Naleving

18.1 Naleving van wettelijke en contractuele eisen

Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.

18.1.1	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 behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	Bestuur Proceseigenaar Dienstverantwoordelijke
18.1.2	1	**Intellectuele-eigendomsrechten** Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen behoren passende procedures te worden geïmplementeerd.	Bestuur Proceseigenaar Dienstverantwoordelijke
18.1.3	1	**Beschermen van registraties** Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Proceseigenaar Dienstverantwoordelijke
18.1.3.1	1	Per soort informatie is inzichtelijk gemaakt wat de bewaartermijn is.	
18.1.4	1	**Privacy en bescherming van persoonsgegevens** Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Bestuur Proceseigenaar Dienstverantwoordelijke
18.1.4.1	1	In overeenstemming met de AVG heeft de organisatie een Privacy Officer/ Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren	
18.1.4.2	1	Organisatie controleert regelmatig de naleving van de privacyregels en informatieverwerking en –procedures aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	
18.1.5	1	**Voorschriften voor het gebruik van cryptografische beheersmaatregelen** Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Bestuur
18.1.5.1	1	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij internationale standaarden.	

18.2 Informatiebeveiligingsbeoordelingen

Doelstelling: Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.

18.2.1	**1**	**Onafhankelijke beoordeling van informatiebeveiliging** De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.	Bestuur Proceseigenaar Dienstverantwoordelijke
18.2.1.1	1	Er is een information security information system (ISMS) waarmee aantoonbaar de gehele plan-do-check-act cyclus op gestructureerde wijze wordt afgedekt.	
18.2.1.2	1	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	

18.2.2	**1**	**Naleving van beveiligingsbeleid en –normen** Het bestuur behoort regelmatig de naleving van de informatieverwerking en - procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Bestuur Proceseigenaar Dienstverantwoordelijke
18.2.2.1	1	In de P&C cyclus wordt gerapporteerd over informatiebeveiliging. Diensteigenaaar aan proceseigenaar, proceseigenaar aan bestuur	

18.2.3	**1**	**Beoordeling van technische naleving** Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Proceseigenaar Dienstverantwoordelijke
18.2.3.1	2	Informatiesystemen worden minimaal twee jaarlijks of bij grote wijziging door een onafhankelijke derde gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of pentesten.	

Addendum BIS

Inleiding Addendum

In de addendum bevat een overzicht van de beleid en SURF implementatierichtlijn documenten die vermeld worden in de BIS met daarbij een verwijzing naar de locatie waar het document te vinden is.

Algemene regels voor de oplevering van een dienst
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Aangifte van security incidenten
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Acceptatiecriteria nieuwe applicaties
URL:

Grip op Secure Software Development (SSD)
URL:

Procedures Data Centers
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Procedure veilig verwijderen of hergebruiken van hardware
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Handreiking bedrijfscontinuïteit
URL: https://intranet.surf.nl/display/IBB/Algemene+informatie+voor+clusters+en+diensten

Handreiking proces wijzigingsbeheer
URL:

Handreiking Cryptografie
URL: https://intranet.surf.nl/display/IBB/Handreiking+cryptografie

Beveiligingsniveaus en gestructureerde VLAN indeling
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Security incidenten en Meldplicht Datalekken
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Telewerken
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Veilige Wachtwoorden
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Veiligheidsrisico's en veiligheidsrichtlijnen smartphones
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Veilig wachtwoordmanagement
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

VLAN security categorieën
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Toegang en veiligheid computervloeren
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Wijzigen van configuratie van veiligheiddevices
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Aansluiten hardware op het SURF netwerk
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Backup en Restore
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Beheer van toegangsrechten van medewerkers
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Beleid clear desk clear screen
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Beleid Patch Management
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Beveiligd Ontwikkelen
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Disaster Recovery
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Beleid Gegevensclassificatie
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Richtlijn voor het instellen van de systeemklok
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Beleid Leveranciersmanagement
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

Omgaan met verwijderbare media
URL: https://intranet.surf.nl/display/IBB/Ondersteunende+Procedures+en+Richtlijnen

SURF Juridisch Normenkader

URL: https://www.surf.nl/surf-juridisch-normenkader-cloudservices

SURF model verwerkersovereenkomst
URL: https://www.surf.nl/surf-juridisch-normenkader-cloudservices

SURF Informatiebeveiligingsbeleid
URL: https://intranet.surf.nl/display/IBB/Beleid+en+Standaarden

SURF SO-functieprofiel
URL:

SURF Acceptable Use Policy
URL:

NBV brochure BSPA | Publicatie | AIVD
URL:

Procedure SURF CSIRT charter
URL:

Handreiking penetratietesten
URL:

SURF E-waste beleid
URL:

SURF werkplekbeleid
URL:

Handreiking proces wijzigingsbeheer
URL:

Logische toegangsbeveiliging
URL: