Samen aanjagen van vernieuwing

BIS

Baseline Informatiebeveiliging SURF

Auteur(s) : CISO-team

Versie : zie colofon
Datum : 1 februari 2024
Kenmerk : Baseline Informatiebeveiliging SURF (BIS)

Colofon

Dit document beschrijft de baseline voor informatiebeveiliging bij SURF, de reeks minimale beveiligingsstandaarden die de basis vormen voor de beveiliging van gegevens bij SURF: de Baseline Informatiebeveiliging SURF, afgekort 'BIS'. De BIS is een standaard die voortvloeit uit het Informatieveiligheidsbeleid SURF.

Documenteigenschappen

Titel	BIS
Onderwerp	Baseline Informatiebeveiliging SURF (BIS)
Document type	Standaard
Classificatie	SURF publiek
Datum	3 september 2024
Eigenaar	Chief Information Security Officer
Status	2.0

Versiebeheer

Versie	Datum	Door	Toelichting wijziging	Vaststelling
1.0	19-10-2021	Alvin Anita, René Ritzen, Rosanne Pouw, Bart Bosman, Sedat Çapkin	Initieel document	CISO
1.2	April 2023	CISO-team	Begripsbepaling, classificatie vernieuwd, BIS-set vernieuwd	CISO
1.3/1.5	Juli 2023/februari 2024	Helma	Tussenversie, concept	-
2.0	03-09-2024	Helma, Sedat, Alvin, Arvid	BIS 2024 op basis van ISO 27001:2022 e.a. major	CISO

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. Voor het bepalen van die beveiligingsmaatregelen hanteert SURF de documentstandaard Baseline Informatiebeveiliging SURF (hierna BIS).

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

- Informatieveiligheidsbeleid SURF
- ISO 27001 en ISO 27002
- SURF Sector Baseline (surf.sec.nl)
- Algemene Verordening Gegevensverwerking
- Overige wet- en regelgeving, zoals NIS2

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.

Reikwijdte

De BIS geeft de beveiligingsmaatregelen (organisatorisch, mensgericht, fysiek en technisch) voor de informatie(systemen) van SURF. De BIS is van toepassing op de hele SURF-organisatie, inclusief de diensten en systemen waar informatie wordt verwerkt. Door deze maatregelen te volgen, kan SURF een betrouwbare en professionele dienstverlening en informatievoorziening bieden.

Voor de begripsbepalingen, zie intranet: verklarende begrippenlijst informatiebeveiliging.

1.2 Rollen en verantwoordelijkheid

De rollen en verantwoordelijkheden volgen het Three Lines-model (3LM) zoals beschreven in het informatieveiligheidsbeleid. De Raad van Bestuur van SURF is eindverantwoordelijk voor de integrale beveiliging. Het lijnmanagement is verantwoordelijk voor het implementeren van passende beveiligingsmaatregelen. De dienstverantwoordelijke of de eventueel toegewezen proceseigenaar is verantwoordelijk voor het nemen van beslissingen over het benodigde beschermingsniveau (de risicoclassificatie).

SURF verzorgt een deel van de implementatie van de beveiligingsmaatregelen centraal, voor de rest verder is dat de diensteigenaar. In de BIS is dit onderscheid aangebracht en is steeds aangegeven wie voor de implementatie van een beveiligingsmaatregel verantwoordelijk is.

1.3 Evaluatie en bijstelling

Door de ontwikkelingen van de techniek kunnen de maatregelensets voor informatiebeveiliging snel verouderen. De BIS is weliswaar zo concreet mogelijk geschreven, maar beschrijft alleen het

wat en niet het hoe. Zo hebben technische ontwikkelingen zo weinig mogelijk impact op de inhoud. Procedures en richtlijnen voor operationele implementatie zijn dus niet verwerkt in de BIS zelf; informatie hierover is terug te vinden op het intranet.

Dit document wordt regelmatig, minimaal jaarlijks, in het geheel geëvalueerd en geactualiseerd als dat nodig is. Het kan voorkomen dat er wijzigingen nodig zijn, bijvoorbeeld door wijzigingen in onderliggende wet- en regelgeving, nieuwe of vernieuwde beleidsrichtlijnen, ISO-norm of nieuwe dreigingen en kwetsbaarheden, etc. Maatregelen die wijzigen, krijgen een opgehoogd versienummer om vergelijking te vergemakkelijken.

Bij de jaarlijkse evaluatie wordt ook gecontroleerd of er wijzigingen/aanvullingen in de maatregelen en de (operationele) procedures en richtlijnen nodig zijn. Dit helpt de praktische toepasbaarheid te vergroten.

2 Werking BIS-maatregelen

2.1 ISO 27001-controls als basis

De controls uit de ISO 27001-standaard bestaan uit 93 beheersmaatregelen (controls) en vormen de basis van de baseline. De ISO 27002-standaard is een specificatie van de ISO 27001-standaard. De ISO 27002-standaard helpt als een praktische richtlijn om informatiebeveiligings-maatregelen te bepalen voor beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening.

De lijst met beheersmaatregelen volgt deze standaard en hoort bij dit document. In de bijlage zijn de controls opgenomen inclusief concrete maatregelen. De BIS wordt gepubliceerd op de website surf.nl zodat leden kunnen zien wat de beveiligingsmaatregelen van SURF precies inhouden. Vanuit praktisch oogpunt is de lijst ook via intranet te downloaden voor eigen gebruik.

2.2 Selectie van maatregelen en hardheidsbepalingen

De risicoanalyse en informatieclassificatie (BIV) bepalen welke BIS-beveiligingsmaatregelen er moeten worden genomen. Zie het document ‘SURF Risicomanagement Informatieveiligheid’ (SRI)

Als bekend is welke classificatie van toepassing is, moeten de relevante maatregelen worden geselecteerd. Afhankelijk van de context zijn sommige maatregelen uit de standaardset niet van toepassing); dit is de hardheidsbepaling: als een control voor een specifiek geval niet van toepassing kan zijn, dan zijn de control en de bijbehorende, nader uitgewerkte maatregelen niet van toepassing. Dit geldt bijvoorbeeld als een control 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, zie 2.3.

2.3 Pas toe of leg uit en acceptatie

De verantwoordelijke voor een dienst of verwerking zorgt voor een registratie van de BIS-maatregelen die niet van toepassing zijn, waaraan nog niet geheel kan worden voldaan en 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 risicoacceptatiematrix 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 geïmplementeerd.

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 sub-dienst in de keten meestal 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.

3 Informatiebeveiligingskaders op basis van classificatie

Voor de BIS geldt:

- Het lijnmanagement is verantwoordelijk voor informatieveiligheid en de beveiliging van informatie(systemen).
- Het lijnmanagement stelt het beschermingsniveau van informatie in haar systemen vast voor de BIV-aspecten betrouwbaarheid, integriteit en vertrouwelijkheid (basis of hoog). Dit heet informatieclassificatie en geschiktheidsclassificatie. Voor de werkwijze van classificatie, zie het document ‘SURF Risicomanagement Informatieveiligheid’.
- 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 bijbehorende maatregelen en draagt deze uit.
- Informatiebeveiliging is een cyclisch verbeterproces volgens de PDCA-methodiek (Plan-Do-Check-Act).

4 BIS - Baseline Informatiebeveiliging SURF - 2024

BIS - Hoofdstukoverzicht
Hieronder zie je het overzicht van de BIS-controls en -maatregelen (in overeenstemming met de ISO-nummering ISO 27001:2022). De complete lijst met controls en maatregelen vind je in hoofdstuk 5 t/m 8.

---

5. Organisatorische beheersmaatregel
5.1 Beleidsregels voor informatiebeveiliging
5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging
5.3 Functiescheiding
5.4 Managementverantwoordelijkheden
5.5 Contact met overheidsinstanties
5.6 Contact met speciale belangengroepen
5.7 Informatie over informatiebeveiligingsdreigingen
5.8 Informatiebeveiliging in projectmanagement
5.9 Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen
5.10 Aanvaard gebruik van informatie en andere gerelateerde bedrijfsmiddelen
5.11 Retourneren van bedrijfsmiddelen
5.12 Classificeren van informatie
5.13 Labelen van informatie
5.14 Overdragen van informatie
5.15 Toegangsbeveiliging
5.16 Identiteitsbeheer
5.17 Beheren van authenticatie informatie
5.18 Toegangsrechten
5.19 Informatiebeveiliging in leveranciersrelaties
5.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten
5.21 Beheren van informatiebeveiliging in de ICT-keten
5.22 Monitoren, beoordelen en het beheren van wijzigingen op van leveranciersdiensten
5.23 Informatiebeveiliging voor het gebruik van clouddiensten
5.24 Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten
5.25 Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen
5.26 Reageren op informatiebeveiligingsincidenten
5.27 Leren van informatiebeveiligingsincidenten
5.28 Verzamelen van bewijsmateriaal
5.29 Informatiebeveiliging tijdens een verstoring
5.30 ICT-gereedheid voor bedrijfscontinuïteit
5.31 Wettelijke, statutaire, regelgevende en contractuele eisen
5.32 Intellectuele eigendomsrechten
5.33 Beschermen van registraties
5.34 Privacy en bescherming van persoonsgegevens
5.35 Onafhankelijke beoordeling van informatiebeveiliging
5.36 Naleving van beleid, regels en normen voor informatiebeveiliging
5.37 Gedocumenteerde bedieningsprocedures

6. Mensgerichte beheersmaatregel
6.1 Screening
6.2 Arbeidsovereenkomst
6.3 Bewustwording, opleiding en training op informatiebeveiliging
6.4 Disciplinaire procedure
6.5 Verantwoordelijkheden na beëindiging of wijziging van het dienstverband
6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten
6.7 Werken op afstand
6.8 Melden van informatiebeveiligingsgebeurtenissen

7. Fysieke beheersmaatregel
7.1 Fysieke beveiligingszones
7.2 Fysieke toegangsbeveiliging
7.3 Beveiligen van kantoren, ruimten en faciliteiten
7.4 Monitoren van de fysieke beveiliging
7.5 Beschermen tegen fysieke en omgevings dreigingen
7.6 Werken in beveiligde gebieden
7.7 'Clear desk' en 'clear screen'
7.8 Plaatsen en beschermen van apparatuur
7.9 Beveiligen van bedrijfsmiddelen buiten het terrein
7.10 Opslagmedia
7.11 Nutsvoorzieningen
7.12 Beveiligen van bekabeling

7.13 Onderhoud van apparatuur
7.14 Veilig verwijderen of hergebruiken van apparatuur

8. Technische beheersmaatregel
8.1 Gebruikersapparatuur
8.2 Speciale toegangsrechten
8.3 Beperking toegang tot informatie
8.4 Toegangsbeveiliging op broncode
8.5 Beveiligde authenticatie
8.6 Capaciteitsbeheer
8.7 Bescherming tegen malware
8.8 Beheer van technische kwetsbaarheden
8.9 Configuratiebeheer
8.10 Wissen van informatie
8.11 Maskeren van gegevens
8.12 Voorkomen van gegevenslekken
8.13 Back-up van informatie
8.14 Redundantie van informatieverwerkende faciliteiten
8.15 Gebeurtenisregistratie
8.16 Monitoren van activiteiten
8.17 Kloksynchronisatie
8.18 Gebruik van speciale systeemhulpmiddelen
8.19 Installeren van software op operationele systemen
8.20 Beveiliging netwerkcomponenten
8.21 Beveiliging van netwerkdiensten
8.22 Netwerksegmentatie
8.23 Toepassen van webfilters
8.24 Gebruik van cryptografie
8.25 Beveiligen tijdens de ontwikkelcyclus
8.26 Toepassingsbeveiligingseisen
8.27 Principes voor de engineering van beveiligde systemen en systeemarchitecturen
8.28 Veilige software ontwikkelen
8.29 Testen van de beveiliging tijdens ontwikkeling en acceptatie
8.30 Uitbestede systeemontwikkeling
8.31 Scheiding van ontwikkel-, test- en productieomgevingen
8.32 Wijzigingsbeheer
8.33 Testgegevens
8.34 Bescherming van informatiesystemen tijdens audit

5 BIS - Organisatorische maatregelen

5. Organisatorisch	BIS-ID	Beheersmaatregel	BIV	Versie
Beleidsregels voor informatiebeveiliging	5.01	SURF heeft door de RvB vastgesteld informatieveiligheidsbeleid gepubliceerd en gecommuniceerd.	BIV-Standaard	2.0
	5.01.1	SURF heeft een baseline met beveiligingsmaatregelen vastgesteld (de BIS, Baseline Informatieveiligheid SURF) als concrete invulling van het informatieveiligheidsbeleid.	BIV-Standaard	
	5.01.2	Diensten formuleren aanvullende voorschriften voor informatiebeveiliging waar dat nodig is.	IV-Hoog	2.0
	5.01.3	SURF controleert het SURF-brede informatieveiligheidsbeleid eens per drie jaar of vaker als dat nodig is.	BIV-Standaard	2.0
	5.01.4	Diensten controleren ten minste eens per jaar of aanvullende voorschriften nog actueel zijn of moeten worden bijgesteld.	IV-Hoog	2.0
Rollen en verantwoordelijkheden bij informatiebeveiliging	5.02	SURF beschrijft generiek de rollen en verantwoordelijkheden voor informatiebeveiliging in het strategisch informatieveiligheidsbeleid.	BIV-Standaard	2.0
	5.02.1	SURF heeft een CISO-functieprofiel opgesteld waarin de rol en verantwoordelijkheden van de CISO zijn vastgelegd en er is een CISO aangesteld volgens dit profiel.	BIV-Standaard	2.0
	5.02.2	Je beschrijft als dienst de rollen en de bijbehorende verantwoordelijkheden voor informatiebeveiliging (op basis van het informatieveiligheidsbeleid). Deze wijs je toe. Bij deze indeling houd je rekening met wat SURF als organisatie nodig heeft.	BIV-Standaard	2.0
Functiescheiding	5.03	De dienst zorgt ervoor dat medewerkers geen combinaties van rollen en bevoegdheden krijgen waarmee ze zonder controle van collega's (belangrijke of kritische) processen, systemen of data kunnen manipuleren of onbedoelde fouten kunnen maken.	BIV-Standaard	2.0
	5.03.1	Risicovolle taken worden op zo'n manier gescheiden dat het risico op fouten, fraude, diefstal, etc. zo klein mogelijk is.	BIV-Standaard	2.0
	5.03.2	De dienst beschrijft bevoegdheden die bij een rol passen. Om te kunnen controleren of aangevraagde bevoegdheden passen bij de rol van een medewerker, wordt het toekennen van de bevoegdheden geregistreerd. De toekenning van die bevoegdheden is beschreven in het autorisatieproces	BIV-Standaard	2.0
	5.03.3	De dienst past strikte scheiding toe tussen beheer- en gebruikstaken specifiek bij apparaten die worden ingezet voor beveiliging, zoals firewalls, camerabeveiliging en alarmsystemen.	BIV-Standaard	2.0
	5.03.4	De dienst past het vierogenprincipe toe bij de uitvoering van kritische werkzaamheden. Dit is specifiek van belang bij het verstrekken van toegang en toekennen van privileges in systemen.	IV-Hoog	2.0
	5.03.5	De dienst past functiescheiding strikt toe als er sprake is van een van taken in combinatie met conflicterende werkzaamheden.	IV-Hoog	2.0
Managementverantwoordelijkheden	5.04	Het bestuur stuurt erop dat alle medewerkers volgens het SURF-beleid (en bijbehorende procedures) met informatiebeveiliging omgaan.	BIV-Standaard	2.0
	5.04.1	Het bestuur van SURF houdt toezicht op de uitvoering van de vereiste beveiligingsmaatregelen (volgens de Baseline Informatiebeveiliging SURF, de 'BIS').	BIV-Standaard	2.0

5. Organisatorisch	BIS-ID	Beheersmaatregel	BIV	Versie
	5.04.2	Ieder team zorgt voor voldoende bemensing (capaciteit) om belangrijke taken en processen uit te voeren ook in periodes van lagere bezetting (zoals vakantie). Hiervoor: a. wordt de capaciteit gemonitord zodat structurele onderbezetting wordt gesignaleerd en aangepakt. b. zijn procedures bekend in geval van ongeplande afwezigheid van teamleden c. zijn personen geïdentificeerd als SPoF (Single Point of Failure) als zij als enige in staat zijn specifieke (belangrijke) taken uit te voeren.	BIV-Standaard	2.0
	5.04.3	De dienst zorgt ervoor dat kwetsbare kennis (van SPoF's, Single Point of Failure) wordt geborgd via kennisoverdracht of via externe expertise.	BIV-Standaard	2.0
	5.04.4	Medewerkers kunnen anoniem melding maken van problemen met informatiebeveiliging. Hiervoor is een klokkenluidersregeling beschikbaar.	BIV-Standaard	2.0
Contact met overheidsinstanties	5.05	SURF heeft en onderhoudt contact met de overheid waar dat nodig is op het gebied van informatieveiligheid.	BIV-Standaard	2.0
	5.05.1	SURF heeft een lijst opgesteld waarin staat met welke overheidsinstanties en toezichthouders contact wordt onderhouden. Deze lijst wordt regelmatig vernieuwd, minimaal jaarlijks.	BIV-Standaard	2.0
	5.05.2	SURF heeft een proces voor de aanmelding bij de bevoegde autoriteit met de juiste informatie. Wijzigingen worden binnen twee weken doorgegeven.	BIV-Standaard	2.0
Contact met speciale belangengroepen	5.06	SURF heeft en onderhoudt contact met stakeholders en experts op het gebied van informatiebeveiliging.	BIV-Standaard	2.0
	5.06.1	SURF heeft een lijst opgesteld waarin staat met welke stakeholders en experts contact wordt onderhouden. Deze lijst wordt regelmatig vernieuwd.	BIV-Standaard	2.0
Informatie en analyses over dreigingen	5.07	SURF verzamelt informatie over dreigingen voor informatiebeveiliging. Die informatie wordt geanalyseerd om de organisatie adequaat te kunnen informeren over dreigingen, om hierop te kunnen inspelen.	BIV-Standaard	2.0
	5.07.1	De dienst voert een risicoanalyse uit, zodat er inzicht is in de risico's (kans * impact) die er zijn op het gebied van informatiebeveiliging en stelt deze analyse periodiek bij.	BIV-Standaard	2.0
Informatiebeveiligin g in projectbeheer	5.08	Bij ieder project of bij nieuwe ontwikkelingen is bewust aandacht voor het implementeren van de juiste beveiligingsmaatregelen.	BIV-Standaard	2.0
	5.08.1	Het projectteam maakt een risicoafweging (risicoanalyse en classificatie) voor het bepalen van de benodigde beveiligingsmaatregelen van de BIS. Je stelt deze risicoanalyse bij in de verschillende projectfases.	BIV-Standaard	2.0
	5.08.2	Het projectteam past 'Security by Design' toe en beschrijft in het projectplan hoe dat wordt ingevuld.	BIV-Standaard	2.0
Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	5.09	De dienst inventariseert: welke informatie zij beheert welke bedrijfsmiddelen zij gebruikt en wie daarvan eigenaar is Dit staat in een inventarislijst die regelmatig wordt vernieuwd.	BIV-Standaard	2.0
	5.09.1	De dienst beheert de eigen bedrijfsmiddelen via een proces voor Asset Management.	BIV-Standaard	2.0

5. Organisatorisch	BIS-ID	Beheersmaatregel	BIV	Versie
	5.09.2	Voor ieder object/asset (inclusief cloud) is lifecycle management ingeregeld met procedures voor in ieder geval: installatie beheer actueel houden beveiliging uitfaseren	BIV-Standaard	2.0
	5.09.3	In de configuratiemanagement-database (CMDB) krijgt ieder systeem dat qua risico 'hoog' scoort op het gebied van integriteit en vertrouwelijkheid een label waaruit dit blijkt.	IV-Hoog	2.0
Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	5.10	SURF heeft een ICT-reglement waarin gedragsregels staan over hoe medewerkers moeten omgaan met de ICT-voorzieningen (internet, laptops, e-mail, etc.) van de organisatie.	BIV-Standaard	2.0
	5.10.1	Het ICT-reglement is voor iedere medewerker toegankelijk.	BIV-Standaard	2.0
	5.10.2	Medewerkers zijn bekend met het bestaan van (de gedragsregels van) het ICT-reglement.	BIV-Standaard	2.0
	5.10.3	Externe medewerkers zijn via het contract akkoord gegaan met de geldende gedragsregels.	BIV-Standaard	2.0
Retourneren van bedrijfsmiddelen	5.11	Door SURF beschikbaar gestelde bedrijfsmiddelen voor het uitvoeren van taken, worden ingeleverd als deze taken stoppen.	BIV-Standaard	2.0
Classificatie van informatie	5.12	SURF heeft een schema voor informatieclassificatie vastgesteld voor de BIV-aspecten (Beschikbaarheid, Integriteit, Vertrouwelijkheid).	BIV-Standaard	2.0
	5.12.1	Diensten bepalen het benodigde beschermingsniveau van hun dienst op basis van het door SURF vastgestelde schema voor informatieclassificatie, zodat de juiste beveiligingsmaatregelen van de BIS kunnen worden geselecteerd.	BIV-Standaard	2.0
	5.12.2	De dienst mag tijdens reguliere kantooruren maximaal 24 uur ongepland onbeschikbaar zijn op jaarbasis.	BIV-Standaard	2.0
	5.12.3	De dienst mag tijdens reguliere kantooruren maximaal circa 4 uur ongepland onbeschikbaar zijn op jaarbasis. Soms is meer uptime nodig (hoog+).	B-Hoog	2.0
Labelen van informatie	5.13	SURF heeft een schema voor het labelen van (de vertrouwelijkheid) van informatie vastgesteld.	BIV-Standaard	2.0
	5.13.1	Diensten labelen hun informatie op basis van het schema met categorieën van vertrouwelijkheid.	BIV-Standaard	2.0
Overdragen van informatie	5.14	SURF heeft vastgesteld onder welke eisen en voorwaarden informatie mag worden overgedragen.	BIV-Standaard	2.0
	5.14.1	Data die onderweg is ('in transit') wordt altijd beveiligd met encryptie. Bij web- en mailverkeer van gevoelige gegevens wordt de dienst SURFcerticaten of SURFfilesender gebruikt.	BIV-Standaard	2.0
	5.14.2	De dienst volgt de eisen en voorwaarden voor overdracht van informatie zoals SURF die heeft vastgesteld.	BIV-Standaard	2.0
Toegangsbeveiliging	5.15	SURF heeft procedures voor fysieke en logische toegangsbeveiliging vastgesteld en geïmplementeerd.	BIV-Standaard	2.0
Identiteitsbeheer	5.16	Iedere dienst beheert de volledige lifecycle van digitale identiteiten.	BIV-Standaard	2.0

5. Organisatorisch	BIS-ID	Beheersmaatregel	BIV	Versie
Authenticatie via organisatorische identiteit	5.16.1	De dienst verifieert eindgebruikers van applicaties die toegang geven tot gegevens via een vertrouwde identity-provider. SURF heeft een duidelijke relatie met personen die toegang krijgen, bijvoorbeeld via contractuele afspraken. Voor alle gebruikers worden bij voorkeur federatieve identiteiten gebruikt voor authenticatie op het systeem.	BIV-Standaard	2.0
	5.16.2	De dienst zorgt voor het beheer van gebruikersidentificatie en heeft daarvoor een formele procedure voor het registreren en afmelden van gebruikers ingericht.	BIV-Standaard	2.0
	5.16.3	Accounts worden zoveel mogelijk individueel toegekend en gebruikt. Als het niet anders kan mag je een groepsaccount gebruiken. Dit moet de diensteigenaar motiveren en vastleggen.	BIV-Standaard	2.0
Beheren van authenticatie-informatie	5.17	Er is een proces geïmplementeerd dat zorgt voor beheer van authenticatie-informatie van gebruikers. Medewerkers die met deze informatie werken, krijgen instructie over hoe ze dit op de juiste manier moeten doen.	BIV-Standaard	2.0
	5.17.1	SURF stelt een tool voor wachtwoordbeheer aan medewerkers beschikbaar.	BIV-Standaard	2.0
	5.17.2	De dienst implementeert het wachtwoordbeleid van SURF, waarbij de regels voor het gebruik zo zijn doorgevoerd dat systemen deze afdwingen.	BIV-Standaard	2.0
	5.17.3	Initiële en geresette wachtwoorden zijn maximaal 24 uur geldig en de gebruiker moet deze bij het eerste gebruik verplicht wijzigen.	BIV-Standaard	2.0
Toegangsrechten	5.18	De dienst gaat op de door SURF voorgeschreven manier met toegangsrechten tot informatie en bedrijfsmiddelen om. Dat geldt voor het verstrekken, wijzigen, verwijderen en beoordelen van die rechten.	BIV-Standaard	2.0
	5.18.1	Personen hebben geen toegang tot informatiesystemen tenzij een daartoe bevoegde medewerker die toegang autoriseert en verleent.	BIV-Standaard	2.0
	5.18.2	De toepassing van functiescheiding en het toekennen van toegangsrechten gebeurt op basis van een risicoafweging.	BIV-Standaard	2.0
	5.18.3	Er is een overzicht c.q. functieprofiel van wie toegangsrechten mag toekennen (het 'mandaatregister').	BIV-Standaard	2.0
	5.18.4	Eerder uitgegeven accounts en bijbehorende unieke identifiers worden niet hergebruikt..	BIV-Standaard	2.0
	5.18.5	Toegangsrechten worden ten minste jaarlijks beoordeeld.	BIV-Standaard	2.0
	5.18.6	Afwijkingen met impact worden behandeld als securityincident inclusief melding, opvolging en documentatie.	BIV-Standaard	2.0
	5.18.7	Toegekende toegangsrechten worden iedere zes maanden gecontroleerd/opnieuw beoordeeld	IV-Hoog	2.0
	5.18.8	SURF verleent apparaten toegang tot het netwerk en -diensten aan de hand van van het benodigde beveiligingsniveau.	BIV-Standaard	2.0
	5.18.9	Apparatuur die SURF beheert (en heeft geauthenticeerd) kan toegang krijgen tot vertrouwde netwerkzones. Apparatuur die SURF niet beheert (bijvoorbeeld Bring Your Own Device, BYOD), krijgt alleen toegang tot een netwerksegment met beperkte (toegangs)rechten.	BIV-Standaard	2.0
Informatiebeveiliging in leveranciersrelaties	5.19	Je zorgt voor adequaat beheer van de informatiebeveiligingsrisico's die er zijn door het gebruik van leveranciers voor bepaalde producten en diensten.	BIV-Standaard	2.0
	5.19.1	De dienst bepaalt hoe de periodieke controle van haar leveranciers wordt uitgevoerd.	BIV-Standaard	2.0

5. Organisatorisch	BIS-ID	Beheersmaatregel	BIV	Versie
Adresseren van informatiebeveiliging in leveranciersovereen komsten	5.20	Met iedere leverancier leg je in het contract de voor de leveranciersrelatie relevante eisen voor informatiebeveiliging vast.	BIV-Standaard	2.0
	5.20.1	Bij inkoopprocessen communiceert de dienst de eisen voor informatiebeveiliging (BIV) aan mogelijke leveranciers,	BIV-Standaard	2.0
	5.20.2	In (inkoop)contracten waar informatie een rol speelt, neem je de beveiligingseisen uit de offerteaanvraag op.	BIV-Standaard	2.0
	5.20.3	In inkoopcontracten zorg je voor prestatieindicatoren en bijbehorende verantwoordingsrapportages waarmee je de afgesproken prestatie van de leverancier kunt controleren.	BIV-Standaard	2.0
	5.20.4	In inkoopcontracten regel je dat je regelmatig een externe audit kunt uitvoeren om de betrouwbaarheid van de geleverde dienst te toetsen.	BIV-Standaard	2.0
	5.20.5	Bij inkoop van ICT houd je je aan de standaardinkoopvoorwaarden om vertrouwelijkheid c.q. geheimhouding te borgen.	BIV-Standaard	2.0
	5.20.6	Voordat je een contract afsluit, heb je op basis van een risicoafweging bepaald of de afhankelijkheid van deze leverancier beheersbaar is. Een vast onderdeel van het contract is een uitgewerkte exitstrategie.	BIV-Standaard	2.0
	5.20.7	Je sluit een verwerkersovereenkomst af met leveranciers die voor SURF persoonsgegevens verwerken.	BIV-Standaard	2.0
	5.20.8	Als leveranciers toegang nodig hebben tot bedrijfsinformatie van SURF, gebeurt dit na een risicoafweging. Over die toegang maak je duidelijke afspraken en je legt die vast.	BIV-Standaard	2.0
Beheren van informatiebeveiliging in de ICT-keten	5.21	Je hebt een proces ingeregeld waarmee je ketenrisico's identificeert zodat je deze risico's in de toeleveringsketen kunt managen.	BIV-Standaard	2.0
	5.21.1	Je beschikt over inzicht in de keten van toeleveranciers van je leverancier. De leverancier is transparant over hoe de afgesproken/vereiste security-eisen zijn doorvertaald naar hun toeleveranciers.	BIV-Standaard	2.0
Monitoren, beoordelen en beheren van wijzigingen van leveranciersdiensten	5.22	Je controleert of de leverancier de afspraken over securitymaatregelen nakomt. Je maakt daarvoor een structurele planning voor monitoring, beoordeling en evaluatie van deze afspraken.	BIV-Standaard	2.0
	5.22.1	Minimaal eens per jaar controleer je de prestatie van je leverancier(s) aan de hand van vooraf vastgestelde prestatieindicatoren volgens het contract.	BIV-Standaard	2.0
Informatiebeveiligin g voor het gebruik van clouddiensten	5.23	De dienst volgt de SURF-brede afspraken voor het inkopen en gebruiken en verlaten van clouddiensten. In deze procedure is een proces opgenomen voor het beheren en beëindigen van de clouddienst. De uitwerking past bij de eisen van SURF op het gebied van informatiebeveiliging.	BIV-Standaard	2.0
Plannen en voorbereiden van het beheer van informatiebeveiliging sincidenten	5.24	SURF heeft een helder proces over de werkwijze rondom securityincidenten vastgesteld en gecommuniceerd, inclusief een duidelijke beschrijving van de rollen en verantwoordelijkheden.	BIV-Standaard	2.0
Beoordelen van en besluiten over informatiebeveiliging sgebeurtenissen	5.25	Het SIRT bepaalt wanneer een issue als securityincident wordt geregistreerd.	BIV-Standaard	2.0
	5.25.1	Een incident dat (mogelijk) leidt tot een inbreuk op de beschikbaarheid, integriteit of vertrouwelijkheid moeten zo snel mogelijk (binnen 24 uur als streven) aan het SIRT worden gemeld.	BIV-Standaard	2.0

5. Organisatorisch	BIS-ID	Beheersmaatregel	BIV	Versie
	5.25.2	Het SIRT rapporteert periodiek aan het CISO-team over de status en opvolging van incidenten.	BIV-Standaard	2.0
	5.25.3	Het SIRT neemt in de incidentrapportage informatie op uit de CVD-procedure.	BIV-Standaard	2.0
	5.25.4	Grote securityincidenten, melden we volgens de vereisten aan de bevoegde autoriteit.	BIV-Standaard	2.0
Reageren op informatiebeveiliging sincidenten.	5.26	Securityincidenten worden opgepakt en afgehandeld volgens de daarvoor afgesproken procedure.	BIV-Standaard	
	5.26.1	Het SIRT volgt securityincidenten op volgens de de incidentprocedure en zorgt voor eventuele escalatie.	BIV-Standaard	2.0
	5.26.2	SURF heeft een integraal crisisplan. De dienst verwijst naar dit plan in continuïteitsplannen voor informatiebeveiliging (voor escalatie).	BIV-Standaard	2.0
	5.26.3	SURF test jaarlijks of het integrale crisisplan nog geldig, actueel en bruikbaar is.	BIV-Standaard	2.0
Leren van informatiebeveiliging sincidenten	5.27	De kennis die ontstaat door het analyseren van securityincidenten, wordt gebruikt om de beveiligingsmaatregelen te verbeteren en herhaling te voorkomen.	BIV-Standaard	2.0
	5.27.1	SURF deelt de analyses van securityincidenten met relevante partners om herhaling te voorkomen.	BIV-Standaard	2.0
Verzamelen van bewijsmateriaal	5.28	SURF heeft procedures vastgesteld en geïmplementeerd voor het omgaan met bewijsmateriaal bij securityincidenten.	BIV-Standaard	2.0
Informatiebeveiligin g tijdens verstoring	5.29	Je hebt een plan waarmee je ervoor kunt zorgen dat er nog steeds sprake is van een passend niveau van informatiebeveiliging tijdens een verstoring.	BIV-Hoog	2.0
ICT-gereedheid voor bedrijfscontinuïteit	5.30	De dienst bepaalt doelstellingen voor bedrijfscontinuïteit (van ICT). Deze zijn nodig om als dienst efffectief te blijven werken als zich een ICT-gerelateerd incident voordoet. Diensten zijn zo voldoende in staat in te spelen op situaties waarin de business-continuïteit en noodherstel centraal staan.	BIV-Standaard	2.0
	5.30.1	De dienst voert een inventarisatie uit om de bedrijfskritische (proces)onderdelen te identificeren.	BIV-Standaard	2.0
	5.30.2	De dienst test periodiek de contintuïteitsplannen van niet bedrijfskritische systemen.	BIV-Standaard	2.0
	5.30.3	De dienst test jaarlijks de contintuïteitsplannen van bedrijfskritische systemen.	B-Hoog	2.0
Wettelijke, statutaire, regelgevende en contractuele vereisten	5.31	De dienst zorgt voor documentatie over relevante eisen vanuit o.a. wet- en regelgeving, contracten en statuten en houdt dit actueel.	BIV-Standaard	2.0
	5.31.1	De dienst beschrijft welke aanpak wordt gevolgd om aan de relevante eisen vanuit wet- en regelgeving te voldoen.	BIV-Standaard	2.0
Intellectuele eigendomsrechten	5.32	Je houdt rekening met intellectuele eigendomsrechten en beschermt deze.	BIV-Standaard	2.0
Beschermen van registraties	5.33	Je beschermt belangrijke informatie over wettelijke verplichtingen en zakelijke transacties ('registraties') tegen verlies, vernietiging, vervalsing, onbevoegde toegang, openbaarmaking, etc.	BIV-Standaard	2.0
	5.33.1	De dienst maakt per informatiesoort inzichtelijk welke bewaartermijn geldt.	BIV-Standaard	2.0
Privacy en bescherming van persoonsgegevens	5.34	SURF zorgt voor adequate bescherming van privacy en persoonsgegevens in overeenstemming met wet- en regelgeving.	BIV-Standaard	2.0

5. Organisatorisch	BIS-ID	Beheersmaatregel	BIV	Versie
	5.34.1	SURF heeft een Functionaris voor Gegevensbescherming (FG) aangesteld. De FG heeft voldoende mandaat om de functie adequaat uit te voeren.	BIV-Standaard	2.0
	5.34.2	SURF controleert regelmatig of de eisen en afspraken over privacy en gegevensbescherming worden nageleefd.	BIV-Standaard	2.0
	5.34.3	De dienst zorgt ervoor dat ze weet welke invulling SURF geeft aan eisen voor de verwerking van persoonsgegevens en past deze toe.	BIV-Standaard	2.0
Onafhankelijke beoordeling van informatiebeveiliging	5.35	SURFs aanpak rondom beheer en implementatie van informatieveiligheid wordt volgens planning of bij belangrijke wijzigingen beoordeeld via interne en externe audits.	BIV-Standaard	2.0
	5.35.1	SURF stelt jaarlijks een auditplan vast waarin de keuzes staan over welke soort en op welke manier audits worden uitgevoerd.	BIV-Standaard	2.0
Naleving van beleid, regels en normen voor informatiebeveiliging	5.36	SURF controleert regelmatig of het informatiebeveiligingsbeleid en onderwerpspecifieke afspraken en normen worden nageleefd.	BIV-Standaard	2.0
	5.36.1	De CISO rapporteert periodiek over informatiebeveiliging aan bestuur en management.	BIV-Standaard	2.0
	5.36.2	Jaarlijks controleer je de naleving van de technische eisen aan beveiliging, bijvoorbeeld met een securitytest, pentest of geautomatiseerde kwetsbaarheidsscans.	BIV-Standaard	2.0
Gedocumenteerde bedieningsprocedures	5.37	Er zijn werkinstructies beschikbaar voor het werken met configuraties en informatieverwerkende faciliteiten (systeem, infratructuur) voor taken die moeilijk zijn of niet vaak worden uitgevoerd.	BIV-Standaard	2.0
Bedrijfsprocedures voor veilig gebruik van IT-services	5.37.1	Gebruikers kunnen via een handleiding stap voor stap zien hoe zij een systeem veilig kunnen gebruiken. De instructie is helder en concreet en de gebruiker kan gemakkelijk zien of het om voorschriften gaat of om een handreiking/best practice.	BIV-Standaard	2.0

6 BIS - Mensgerichte maatregelen

6. Mensgericht	BIS-ID	Beheersmaatregel	BIV	Versie
Screening	6.01	Voordat een nieuwe medewerker in dienst treedt, controleert SURF de achtergrond van deze persoon. De controle gebeurt in lijn met geldende wet- en regelgeving en wordt op gezette tijden herhaald. De zwaarte van de controle past bij de eisen van SURF en de bij de functie of opdracht behorende risico's.	BIV-Basis	2.0
	6.01.1	HR controleert de identiteit, relevante diploma's en certificaten van een nieuwe medewerker bij aanstelling.	BIV-Basis	2.0
	6.01.2	SURF vraagt de medewerker een geldige, toepasselijke Verklaring Omtrent Gedrag (VOG) te tonen bij indiensttreding en registreert de controle.	BIV-Basis	2.0
	6.01.3	Als in nieuwe situaties iemand wordt ingezet voor gevoelige dataverwerkingen met een hoog risico, wordt gecontroleerd of een zwaardere VOG of andere screeningsmaatregelen nodig zijn.	IV-Hoog	2.0
Arbeidsovereenkomst	6.02	In het arbeidscontract staat vermeld welke verantwoordelijkheden er voor informatiebeveiliging voor medewerker en organisatie gelden. Medewerkers worden hier specifiek op gewezen, ook bij een functiewisseling.	BIV-Basis	2.0
	6.02.1	Medewerkers krijgen uitgelegd waar ze de voor hen geldende afspraken en instructies voor informatiebeveiliging kunnen vinden. De toegang tot deze informatie is eenvoudig.	BIV-Basis	2.0
	6.02.2	SURF verstrekt nieuwe medewerkers het arbeidsvoorwaardenreglement als onderdeel van de getekende arbeidsovereenkomst.	BIV-Basis	2.0

6. Mensgericht	BIS-ID	Beheersmaatregel	BIV	Versie
Bewustwording van, opleiding en training in informatiebeveiliging	6.03	SURF zorgt ervoor dat medewerkers op het gebied van informatiebeveiliging een passende, voor hun functie relevant(e): bewustwordingsniveau opleiding en training regelmatige updates over beleid en beleidsregels/procedures van de organisatie hebben of krijgen.	BIV-Basis	2.0
	6.03.1	Medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en eventuele speciale eisen voor specifieke omgevingen.	BIV-Basis	2.0
	6.03.2	Medewerkers krijgen bijscholing over informatiebeveiliging van SURF, bijvoorbeeld awareness-activiteiten, trainingen, presentaties en campagnes.	BIV-Basis	2.0
	6.03.3	Medewerkers krijgen als onderdeel van de onboarding een introductie 'informatiebeveiliging'. Dit gebeurt uiterlijk binnen drie maanden na indiensttreding.	BIV-Basis	2.0
	6.03.4	Voor veilig werken op de werkplek zijn minimaal de volgende aspecten geïmplementeerd: a. in bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde; b. voor SURF-apparatuur tekenen gebruikers een gebruikersovereenkomst waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren de apparatuur veilig te gebruiken.	BIV-Basis	2.0
	6.03.5	SURF zorgt ervoor dat medewerkers voorlichting krijgen over veilig werken online, zodat ze de risico's van digitaal werken en online gedrag kennen (bijvoorbeeld het klikken op onbekende links) en weten hoe ze hiermee moeten omgaan.	BIV-Basis	2.0
	6.03.6	Leidinggevenden attenderen medewerkers regelmatig op het belang van training op het gebied van informatiebeveiliging en privacy en stimuleert hen actief deze periodiek te volgen. Leidinggevenden zorgen ervoor dat hun medewerkers bekend zijn met het ICT-reglement (AUP).	BIV-Basis	2.0
	6.03.7	Medewerkers die toegang hebben tot strikt vertrouwelijk informatie, krijgen van hun leidinggevende uitdrukkelijke instructie over hoe zij hiermee moeten omgaan, wat hun verantwoordelijkheid is en dat ze hierop worden gecontroleerd.	IV-Hoog	2.0
	6.03.8	Bestuurders volgen aantoonbaar opleiding en training zodat zij in staat zijn op het gebied van cyberveiligheid risico's te identificeren en de aanpak van risicomanagement te beoordelen.	BIV-basis	2.0
Disciplinaire procedure	6.04	SURF heeft een disciplinaire procedure vastgesteld en gecommuniceerd. Deze kan worden gevolgd als medewerkers bewust inbreuk op de informatiebeveiliging plegen. In de arbeidsvoorwaarden wordt hierop geattendeerd.	BIV-Basis	2.0
	6.04.1	In overige relevante documenten naast het ICT-reglement (AUP) en de gedragscode wijst SURF medewerkers op mogelijke disciplinaire maatregelen.	BIV-Basis	2.0
	6.04.2	Medewerkers die vanuit hun functie of rol met gevoelige dataverwerkingen in aanraking komen, worden door hun leidinggevende erop geattendeerd dat de rol die zij vervullen extra zorgvuldigheid vraagt om securitybeleid en -maatregelen toe te passen en dat eerder disciplinaire maatregelen worden genomen bij bewuste overtreding vanwege de aard van de verwerkingen.	IV-Hoog	2.0
Verantwoordelijkheden na beëindiging of	6.05	SURF heeft een procedure vastgesteld over de manier waarop verantwoordelijkheden en rechten worden overgedragen of van kracht blijven bij wijziging of beëindiging van het dienstverband.	BIV-Basis	2.0

6. Mensgericht	BIS-ID	Beheersmaatregel	BIV	Versie
wijziging van het dienstverband		Medewerkers ontvangen van SURF instructie over verantwoordelijkheden rondom informatiebeveiliging die van kracht blijven na functiewijziging of -beëindiging. Deze procedure wordt jaarlijks geëvalueerd.		
	6.05.1	Als je dienstverband wijzigt of eindigt, pas je de door SURF vastgestelde procedure toe voor het overdragen van verantwoordelijkheden en rechten.	BIV-Basis	2.0
Vertrouwelijkheids- of geheimhoudingsovereenkomst	6.06	SURF heeft een vastgestelde modelovereenkomst voor geheimhouding waarin afspraken staan over de bescherming van informatie. Deze wordt waar relevant toegepast en ondertekend door medewerkers en andere externe partijen.	BIV-Basis	2.0
Werken op afstand	6.07	SURF neemt beveiligingsmaatregelen om informatie te beschermen die buiten de fysieke locaties van SURF wordt benaderd en verwerkt als personeel op afstand werkt.	BIV-Basis	2.0
Melden van informatiebeveiligingsgebeurtenissen	6.08	SURF zorgt ervoor dat medewerkers op een makkelijke manier verdachte gebeurtenissen c.q. (mogelijke) incidenten kunnen melden.	BIV-Basis	2.0
	6.08.1	Medewerkers weten hoe ze met securityincidenten moeten omgaan.	BIV-Basis	2.0
	6.08.2	Er is een procedure voor Coordinated Vulnerability Disclosure (CVD) gepubliceerd en ingericht.	BIV-Basis	2.0
	6.08.3	De dienst meldt securityincidenten zo snel mogelijk bij het SIRT, in ieder geval binnen 24 uur nadat je ervan op de hoogte bent.	BIV-Basis	2.0
	6.08.4	De diensteigenaar is verantwoordelijk voor het (laten) oplossen van securityincidenten.	BIV-Basis	2.0

7 BIS - Fysieke maatregelen

Onderdeel	BIS-ID	Beheersmaatregel	BIV	Versie
Fysieke beveiligingszones	7.01	Binnen SURF zijn zones aangewezen die met fysieke toegangsmaatregelen moeten worden beveiligd omdat ze toegang bieden tot informatie en bedrijfsmiddelen.	BIV-Basis	2.0
Fysieke toegangsbeveiliging	7.02	De fysieke toegang tot beveiligde zones plekken in gebouwen met informatie en bedrijfsmiddelen wordt per zone op een passende manier beschermd.	BIV-Basis	2.0
Kantoren, ruimten en faciliteiten beveiligen	7.03	SURF heeft beleid voor fysieke toegangsbeveiliging vastgesteld en geïmplementeerd met het doel personeel, faciliteiten, etc. tegen potentiële gevaren te beschermen.	BIV-Basis	2.0
	7.03.1	De fysieke toegang tot zones en ruimtes bij SURF is beveiligd via identificatie, authenticatie, en autorisatie (IAM). Waar nodig vindt logging van toegang plaats.	BIV-Basis	2.0
	7.03.2	Voor toegang tot beveiligde zones krijgt iedereen een toegangspas, zodat legitime aanwezigheid kan worden aangetoond.	BIV-Basis	2.0
	7.03.3	Er is een sleutelplan voor het beheren van sleutels c.q. toegangspassen die toegang geven tot beveiligde zones.	BIV-Basis	2.0
Monitoren van fysieke beveiliging	7.04	Gebouw(en) en terrein(en) van SURF worden constant gemonitord op ongeautoriseerde fysieke toegang.	BIV-Basis	2.0
Beschermen tegen fysieke dreigingen en omgevingsdreigingen	7.05	De ICT-infrastructuur wordt op passende wijze beschermd tegen fysieke bedreigingen, zoals brand of overstroming.	BIV-Basis	2.0
Werken in beveiligde zones	7.06	SURF heeft beveiligingsmaatregelen beschreven en geïmplementeerd voor het werken in beveiligde zones.	BIV-Basis	2.0
Clear desk en clear screen	7.07	SURF heeft heldere regels voor het veilig werken op de werkplek opgesteld ('clear desk' en 'clear screen') en gecommuniceerd.	BIV-Basis	2.0

Onderdeel	BIS-ID	Beheersmaatregel	BIV	Versie
	7.07.1	Als een apparaat een bepaalde tijd inactief is, wordt de toegang automatisch vergrendeld. Denk bijvoorbeeld aan schermvergrendeling na inactiviteit van vijf minuten.	BIV-Basis	2.0
	7.07.2	Een sessie remote overnemen kan alleen via dezelfde beveiligde inlogprocedure als waarmee de sessie is gecreëerd. Een remote-sessie vergrendelt automatisch na vijf minuten inactiviteit.	BIV-Basis	2.0
	7.07.3	Als een fysiek token (zoals een yubikey of chipkaart) voor toegang tot een systeem wordt verwijderd, vergrendelt daarmee automatisch de toegang tot dat systeem.	BIV-Basis	2.0
Plaatsing en bescherming van apparatuur.	7.08	Apparatuur is op een veilige plek geplaatst en wordt beschermd.	BIV-Basis	2.0
Beveiliging van bedrijfsmiddelen buiten het terrein.	7.09	SURF zorgt ervoor dat ICT-middelen zijn beschermd als ze zich buiten het SURF-gebouw/-terrein bevinden. Denk b.v. aan encryptie van de harde schijf van laptops en de mogelijkheid tot het wissen van informatie op afstand.	BIV-Basis	2.0
Opslagmedia	7.10	Je zorgt voor adequate beveiliging van verwijderbare opslagmedia zoals usb-sticks, externe harde schijven, in overeenstemming met de classificatie van de opgeslagen gegevens. Dit geldt voor de hele levenscyclus van ingebruikname, transport tot vernietiging.	BIV-Basis	2.0
	7.10.1	Verwijderbare media op voorraad en verwijderbare media met vertrouwelijke informatie bewaar je op een plek die alleen toegankelijk is voor bevoegden.	BIV-Basis	2.0
	7.10.2	Je gebruikt geen verwijderbare media voor externe uitwisseling van informatie.	BIV-Basis	2.0
	7.10.3	Printers vragen om authenticatie voor het printen van informatie.	BIV-Basis	2.0
	7.10.4	SURF vraagt om een certificaat van vernietiging als een externe partij een apparaat moet vernietigen of de informatie op verwijderbare media moet wissen.	BIV-Basis	2.0
	7.10.5	Verwijderbare media worden adequaat vernietigd, bijvoorbeeld door verbranding of versnippering.	IV-Hoog	2.0
	7.10.6	Als transport van apparatuur met informatie nodig is, kies je een koerier of transporteur die voldoende betrouwbaar is.	IV-Hoog	2.0
Nutsvoorzieningen	7.11	SURF beschermt informatiesystemen tegen stroomuitval en andere verstoringen die ontstaan door ontregelingen in nutsvoorzieningen.	BIV-Basis	2.0
Beveiliging van bekabeling	7.12	Kabels die in gebruik zijn voor het versturen van gegevens of als ondersteuning van informatiediensten beschermt SURF tegen interceptie, verstoring of schade.	BIV-Basis	2.0
Onderhoud van apparatuur	7.13	Om doorlopend de beschikbaarheid en integriteit van appatuur te borgen, wordt deze apparatuur volgens de voorgeschreven manier onderhouden.	BIV-Basis	2.0
	7.13.1	In het onderhoudscontract met de leverancier van apparatuur is afgesproken dat: er support wordt geleverd tijdens kantooruren de responstijd maximaal 4 uur is binnen kantoortijden	BIV-Basis	2.0
	7.13.2	In het onderhoudscontract met de leverancier van apparatuur is afgesproken: dat er 24/7 support wordt geleverd dat de responstijd maximaal 2 uur is of er vervangende componenten op locatie aanwezig moeten zijn	B-Hoog	2.0
Veilig verwijderen of hergebruiken van apparatuur	7.14	SURF controleert voor vernietiging en/of hergebruik of onderdelen van apparatuur met opslagmedia adequaat zijn gewist/overschreven om er zeker van te zijn dat gevoelige	BIV-Basis	2.0

Onderdeel	BIS-ID	Beheersmaatregel	BIV	Versie
		gegevens en in licentie gegevens software niet meer terug te halen is.		

8 BIS - Technische maatregelen

Onderdeel	BIS-ID	Beheersmaatregel	BIV	Versie
Apparaten voor eindgebruikers (User endpoint devices)	8.01	Zakelijke informatie op beheerde apparaten van eindgebruikers moet adequaat worden beschermd.	BIV-Basis	2.0
	8.01.1	Mobiele apparatuur (zoals een laptop, tablet en smartphone) is zo ingericht dat: het apparaat wordt beheerd en beveiligd via MDM het apparaat is beschermd met toegangsbeveiliging de gegevens op de ingebouwde opslagapparaten zijn beschermd met encryptie het apparaat onderdeel uitmaakt van patchmanagement en hardening SURF zakelijke gegevens van het apparaat op afstand kan wissen (bij actieve verbinding) Periodiek wordt getoetst of de punten in lid 1 t/m 6 worden nageleefd	BIV-Basis	2.0
Speciale toegangsrechten	8.02	Je beperkt de toewijzing en het gebruik van speciale bevoegdheden/machtigingen tot een minimum.	BIV-Basis	2.0
Sessiebeheer voor toegang met speciale rechten	8.02.1	De toegang van gebruikers die voor hun operationele en administratieve taken meer machtigingen nodig hebben in de ICT-infrastructuur, wordt geregeld via een PAM-systeem (Privileged Access Management) met aparte accounts zodat de bedoelde toegang niet beschikbaar is als eindgebruiker. Je controleert jaarlijks of deze uitgegeven bevoegdheden nog kloppen.	BIV-Basis	2.0
	8.02.2	Ieder kwartaal controleer je of de uitgegeven bevoegdheden/ machtigingen nog kloppen.	IV-Hoog	2.0
Beperking toegang tot informatie	8.03	Je zorgt voor beperking van de toegang tot systemen en informatie volgens de voorschriften voor toegangsbeveiliging.	BIV-Basis	2.0
	8.03.1	De dienst voorkomt dat gebruikers toegang krijgen tot gegevens die ze niet nodig hebben, bijvoorbeeld door omgevingen en data te scheiden ("logisch" of fysiek isoleren).	BIV-Basis	2.0
	8.03.2	Gebruikers kunnen alleen die informatie inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak. In systemen en applicaties worden als uitgangspunt de principes 'Least Privilege' en 'Need-to-Know' gehanteerd.	BIV-Basis	2.0
Toegangsbeveiliging op broncode	8.04	Je beschermt lees- en schrijftoegang tot programmabroncode, ontwikkelingstools en softwarebibliotheken op passende wijze.	BIV-Basis	2.0
	8.04.1	Er is bescherming tegen ongewenste en ongeoorloofde wijzigingen in gedeelde opensource-code.	BIV-Basis	2.0
Beveiligde authenticatie	8.05	Je implementeert een passende vorm van authenticatie op basis van het beleid voor toegangsbeheer. De vereiste vorm van authenticatie kan strikter zijn afhankelijk van de rol (denk aan admins of ontwikkelaars).	BIV-Basis	2.0
	8.05.1	Multifactorauthenticatie is verplicht voor toegang tot alle systemen en applicaties (cloud/on-premises).	BIV-Basis	2.0
	8.05.2	Toegang tot systemen en applicaties en interne bedrijfsgegevens is alleen via de interne vertrouwde zone mogelijk	BIV-Basis	2.0
	8.05.3	Je geeft externe leveranciers alleen toegang tot het netwerk wanneer dat nodig is. Je legt van tevoren vast hoe, waarvoor	BIV-Basis	2.0

Onderdeel	BIS-ID	Beheersmaatregel	BIV	Versie
		en voor hoe lang de rechten zijn toegekend en je logt de toegang.		
Capaciteitsbeheer	8.06	Je beschrijft de capactiteitsvereisten voor verwerking, gegevensopslag en bestandsopslag en controleert de systeemprestaties hierop, zodat je kunnen bijstellen als de capaciteit een kritiek punt bereikt.	BIV-Basis	2.0
	8.06.1	Er zijn maatregelen getroffen zodat we mogelijke aanvallen, zoals een DDoS-aanval, signaleren en er adequaat op kunnen reageren.	BIV-Basis	2.0
	8.06.2	De ICT-resources (netwerk- en diskruimte en CPU-capaciteit) zijn structureel niet meer dan 90% in gebruik. Er is 24/7 monitoring op toename van incidentele overschrijdingen, zodat actie kan worden ondernomen als dat nodig is.	B-Hoog	2.0
Bescherming tegen malware	8.07	Je hebt goede bescherming tegen malware ingeregeld, ondersteund door passende awareness van gebruikers.	BIV-Basis	2.0
	8.07.1	Alle ontvangen bestanden scan je vóór gebruik op malware. Je voert daarnaast regelmatig een malwarescan uit.	BIV-Basis	2.0
	8.07.2	SURF en/of de dienst scant e-mailberichten op spam, virussen en andere kwaadaardige software. Dit gebeurt geautomatiseerd.	BIV-Basis	2.0
	8.07.3	De mogelijkheid tot het downloaden van bestanden is beperkt op basis van risico en need-of-use. Het downloaden wordt gemonitord, zodat er kan worden ingegrepen.	BIV-Basis	2.0
	8.07.4	Software die malware detecteert en bijbehorende herstelsoftware zijn geïnstalleerd en worden regelmatig geüpdatet.	BIV-Basis	2.0
	8.07.5	De dienst gebruikt de door SURF vastgestelde standaarden tegen: malware phishing afluisteren (encryptie) modificatie (SPF, DKIM, DMARC, securityinstellingen)	BIV-Basis	2.0
Beheer van technische kwetsbaarheden	8.08	Je verzamelt informatie over technische kwetsbaarheden zodat je maatregelen kunt nemen om systemen, gegevens en hardware passend te beveiligen.	BIV-Basis	2.0
Registratie en oplossing van kwetsbaarheden	8.08.1	Je zorgt voor geautomatiseerde kwetsbaarhedenscans op je systeem. De resultaten hiervan registreer je in een overzicht inclusief de status van afhandeling. Hierbij houd je rekening met de voorschriften van de procedure Patchmanagement.	BIV-Basis	2.0
Geautomatiseerd scannen op kwetsbaarheden	8.08.2	Je voert minimaal eens per maand een geautomatiseerde kwetsbaarheidsscan uit op de ICT-systemen. Dit gebeurt vanuit een apart account dat in de monitoring kan worden onderscheiden.	BIV-Basis	2.0
Geautomatiseerd scannen op kwetsbaarheid van toepassingen	8.08.3	Je voert minimaal eens per kwartaal een geautomatiseerde kwetsbaarheidscan uit op de toepassing/(web)applicatie. Dit gebeurt vanuit een apart account dat in de monitoring kan worden onderscheiden.	BIV-Basis	2.0
	8.08.4	Je zorgt ervoor dat je patchmanagement inricht voor alle hard- en software. Dit doe je aan de hand van de voorschriften volgens de SURF-brede procedure Patchmanagement.	BIV-Basis	2.0
	8.08.5	Als je een securitypatch met een hoge prioriteit niet tijdig kunt uitrollen, meld je dit bij het SIRT. Verder neem je in de tussentijd maatregelen of een work-around om het systeem/de applicatie te beschermen tegen misbruik van kwetsbaarheden.	BIV-Basis	2.0

Onderdeel	BIS-ID	Beheersmaatregel	BIV	Versie
	8.08.6	Je past hardening toe op systemen: alleen de noodzakelijke onderdelen draaien. Overbodige componenten, services en software zijn uitgeschakeld.	BIV-Basis	2.0
Configuratiebeheer	8.09	De dienst documenteert de configuratieinstellingen van hardware, software, diensten en netwerken en stelt deze vast. Dat geldt ook voor de beveiligingsconfiguraties. Je controleert regelmatig of de instellingen moet worden bijgesteld.	BIV-Basis	2.0
Basisconfiguratie	8.09.1	De dienst werkt met een best practice of standaard voor de beveiligingsconfiguratie van het systeem.	BIV-Basis	2.0
	8.09.2	Je monitort of de configuratie-instellingen niet onbedoeld of zonder autorisatie worden gewijzigd. Dit gebeurt bij voorkeur geautomatiseerd.	BIV-Basis	
Wissen van Informatie	8.10	Als digitale informatie niet meer nodig is, wordt dit gewist. Je houdt rekening met (maximale) bewaartermijnen.	BIV-Basis	2.0
Maskeren van informatie	8.11	Je past datamaskering toe waar dat nodig is om te voorzien in de principes least-privilege/need-to-know.	BIV-Basis	2.0
Voorkomen van gegevenslekken (data leakage prevention)	8.12	Als je gevoelige informatie verwerkt, zorg je voor maatregelen op de gebruikte systemen, netwerken en apparaten, die het lekken van gegevens voorkomen door detectie.	BIV-Basis	2.0
Back-up van informatie	8.13	De dienst maakt en test regelmatig back-ups van informatie, software en images volgens de afgesproken procedure voor back-ups.	BIV-Basis	2.0
	8.13.1	Er is een procedure voor back-up en herstel (restore) vastgesteld waarin je de eisen voor het bewaren, beschermen en testen van de back-ups beschrijft.	BIV-Basis	2.0
	8.13.2	Je test het terugzetten van gegevens uit back-ups minimaal jaarlijks en je test dit sowieso na een grote wijziging om je ervan te verzekeren dat je de back-up betrouwbaar is in noodgevallen.	BIV-Basis	2.0
	8.13.3	Om beschadiging van de back-up tijdens een calamiteit te voorkomen, moet er minimaal één kopie van de back-up op een andere locatie (off-site) worden bewaard.	BIV-Basis	2.0
	8.13.4	Je hebt een risicoafweging gemaakt en op basis daarvan bepaald: wat het maximaal toegestane dataverlies is wat de maximale hersteltijd is na een incident.	BIV-Basis	2.0
	8.13.5	Het maximaal toegestane dataverlies na een incident is een uur.	B-Hoog	2.0
Redundantie van informatieverwerkings-faciliteiten	8.14	Om aan de eisen voor beschikbaarheid te kunnen voldoen, moeten informatieverwerkende faciliteiten voldoende redundant zijn uitgevoerd.	BIV-Basis	2.0
	8.14.1	De maximale hersteltijd na een incident, calamiteit of uitval informatieverwerkende faciliteit is 2 uur (binnen reguliere kantooruren).	B-Hoog	2.0
Logging	8.15	Je zorgt voor logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd en vastgelegd. De logbestanden zijn beschermd tegen aanpassing of verwijdering en de inhoud ervan wordt regelmatig geanalyseerd.	BIV-Basis	2.0
	8.15.1	Alle soorten verwerkingen - lezen, schrijven, updaten, deleten, exporteren - van gegevens in systemen en applicaties worden gelogd.	BIV-Basis	2.0
	8.15.2	Een logregel bevat minimaal de gebeurtenis: de informatie die nodig is om het incident met hoge mate van	BIV-Basis	2.0

Onderdeel	BIS-ID	Beheersmaatregel	BIV	Versie
		zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling (bijvoorbeeld: lezen, schrijven, modificeren en verwijderen); de datum en het tijdstip van de gebeurtenis.		
	8.15.3	Je voorkomt dat logregels informatie bevatten die de beveiliging kunnen compromitteren (zoals een plaintext wachtwoord).	BIV-Basis	2.0
	8.15.4	Je stuurt alle authenticatielogs door naar de centrale loggingserver van IS/SecOps. Je samplet netwerkflow-informatie en stuurt dit naar een centrale loggingserver.	BIV-Basis	2.0
	8.15.5	Je zorgt voor een actueel totaaloverzicht van de verschillende logbestanden met hun opslaglocatie.	BIV-Basis	2.0
	8.15.6	Logbestanden bewaar je minimaal zes maanden. Binnen die periode blijft de beschikbaarheid van de loginformatie gegarandeerd voor eventuele loganalyse. Ook de toegang tot logbestanden wordt gelogd.	BIV-Basis	2.0
	8.15.7	Er is een (onafhankelijke) interne auditprocedure die halfjaarlijks toetst of logbestanden ongewijzigd zijn.	IV-Hoog	2.0
	8.15.8	Het wijzigen, verwijderen van loggegevens of poging daartoe, wordt zo snel mogelijk gemeld als securityincident bij het SIRT.	IV-Hoog	2.0
	8.15.9	Alle acties van systeemadmins worden gelogd.	IV-Hoog	2.0
Monitoren van activiteiten	8.16	SURF monitort netwerken, systemen en applicaties op afwijkend gedrag, zodat tijdig reageren op waarschuwingen mogelijk is. Er zijn maatregelen om mogelijke incidenten te evalueren.	BIV-Basis	2.0
Accountbewaking	8.16.1	Maandelijks rapporteer/registreer je voor de actieve accounts: het aantal uitsluitingen de accountstatus (met waar relevant de einddatum van het account en/of de datum waarop het account wordt opgeheven)	BIV-Basis	2.0
	8.16.2	Je implementeert een systeem voor geautomatiseerde monitoring van logbestanden dat een melding doet als het onregelmatigheden c.q. potentiële risico's signaleert.	IV-Hoog	2.0
Opsporen en voorkomen van exfiltratie van gegevens	8.16.3	Om ongewenst kopiëren en downloaden van data te beperken, dectecteren de dienst grote pieken in netwerkgebruik/bandbreedte. Beheerders en/of gebruikers ontvangen bericht/een waarschuwing als er grote hoeveelheden informatie worden gedownload.	IV-Hoog	2.0
Sessie- en identiteitsbewaking	8.16.4	Via sessie- en identiteitsbewaking (op basis van context en gedrag) detecteer c.q. voorkom je ongeautoriseerde gebruikersactiviteiten	IV-Hoog	2.0
Netwerkinbraakdetectie en -preventiesystemen	8.16.5	We weten wat we als normaal netwerk- en applicatieverkeer beschouwen als baseline. Zo kunnen we afwijkingen van deze basis detecteren en blokkeren. Aan de hand van deze baseline worden de kritieke ICT-diensten gemonitord met netwerkinbraakdetectie en -preventiesystemen.	IV-Hoog	2.0
Kloksynchronisatie	8.17	Je zorgt ervoor dat de systeemklokken van informatieverwerkende systemen met een door SURF goedgekeurde tijdsbron worden gesynchroniseerd.	BIV-Basis	2.0
	8.17.1	Het systeem bevat de juiste tijd, tijdzone (lokale tijdzone) en datum.	BIV-Basis	2.0

Onderdeel	BIS-ID	Beheersmaatregel	BIV	Versie
Gebruik van speciale systeemhulpmiddelen	8.18	Gebruikers vragen goedkeuring voor het inzetten van speciale systeemhulpmiddelen die beveiligingsmaatregelen kunnen beperken of omzeilen.	BIV-Basis	2.0
	8.18.1	De dienst logt het gebruik van speciale systeemhulpmiddelen.	BIV-Basis	2.0
Software installeren op operationele systemen	8.19	Om veilig software op apparaten en systemen te kunnen installeren, stelt het team voorschriften op die worden gevolgd.	BIV-Basis	2.0
	8.19.1	Gebruikers kunnen op hun werkomgeving software installeren. IS monitort de werkomgeving, de geïnstalleerde software en verdacht gedrag.	BIV-Basis	2.0
Netwerkbeveiliging	8.20	SURF zorgt voor bescherming van informatie in systemen en applicaties door het beveiligen en beheren van netwerken en netwerkapparaten.	BIV-Basis	2.0
Toegangscontrole tot het netwerk	8.20.1	Een gebruiker krijgt alleen toegang tot het netwerk op basis van passende identificatie en authenticatie. Niet geïdentificeerde gebruikers krijgen geen toegang tot het netwerk (hooguit tot het gastennetwerk).	BIV-Basis	2.0
Beveiliging van netwerkdiensten	8.21	SURF heeft voor alle netwerkdiensten bepaald welk dienstverleningsniveau en welke beveiligingsmaatregelen nodig zijn. Dit wordt gemonitord.	BIV-Basis	2.0
	8.21.1	SURF bewaakt en analyseert het inkomend en uitgaand dataverkeer om kwaadaardige elementen te detecteren. Dit gebeurt met voorzieningen zoals het Nationaal Detectie Netwerk dat wordt ingezet op basis van een risicoinschatting. Dat gebeurt aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	BIV-Basis	2.0
	8.21.2	SURF filtert inkomend en uitgaand netwerkverkeer, waarbij de inzet wordt bepaald op basis van een risicoinschatting. Dat gebeurt aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	BIV-Basis	2.0
	8.21.3	Gebruikers en apparaten mogen alleen op het bedrijfsnetwerk (bedraad en draadloos) aansluiten na authenticatie/goedkeuring.	BIV-Basis	2.0
	8.21.4	Om vanaf een externe locatie toegang te krijgen tot het interne netwerk, gebruiken we een VPN-server met multifactorauthenticatie (MFA).	BIV-Basis	2.0
	8.21.5	Verbindingen (bedraad en draadloos) buiten de vertrouwde zone worden versleuteld.	BIV-Basis	2.0
	8.21.6	Nieuwe dreigingen die de detectieoplossing (zie 8.21.1) detecteert, worden gemeld en behandeld door het SIRT. Dit gebeurt bij voorkeur via geautomatiseerde mechanismen (threat intelligence sharing) en er wordt hierbij rekening gehouden met de geldende juridische kaders.	BIV-Basis	2.0
Netwerksegmentatie	8.22	In de netwerken van SURF zijn groepen van informatiediensten, -systemen en gebruikers van elkaar gescheiden.	BIV-Basis	2.0
	8.22.1	Bij het gebruik van VLANs neem je alle VLANs in een overzicht op. Je maakt duidelijk hoe de VLAN's zijn beveiligd (toegang, scheiding, koppelingen).	BIV-Basis	2.0
	8.22.2	De beveiliging van ICT-voorzieningen vindt plaats op basis van het geformuleerde securityniveau volgens een gestructureerde VLAN-indeling.	BIV-Basis	2.0
Toepassen van webfilters	8.23	De organisatie past webfilters toe zodat de toegang tot bepaalde externe websites kan worden geblokkeerd als deze gebruikers mogelijk aan kwaadaardige inhoud blootstellen.	BIV-Basis	2.0
Gebruik van cryptografie	8.24	SURF heeft basisregels als voorschrift vastgesteld voor effectief gebruik van cryptografie en het beheer van cryptografische sleutels. Deze regels worden toegepast.	BIV-Basis	2.0

Onderdeel	BIS-ID	Beheersmaatregel	BIV	Versie
	8.24.1	Je past standaard sterke encryptiemethoden toe volgens passende normen en standaarden, waaronder de normen van het Forum Standaardisatie.	BIV-Basis	2.0
	8.24.2	De dienst legt voor de eigen dienst de volgende regels voor cryptografie vast: wanneer en waarvoor je encryptie gebruikt; wie verantwoordelijk is voor de implementatie; wie verantwoordelijk is voor het sleutelbeheer; welke normen je als basis gebruikt voor encryptie en de manier waarop de normen van het Forum Standaardisatie worden toegepast; hoe je het beschermingsniveau vaststelt; voor communicatie tussen organisaties maak je onderling afspraken.	BIV-Basis	2.0
	8.24.3	Je gebruikt een door SURF goedgekeurde CA (certificate-authority), bij voorkeur SURFcertificaten.	BIV-Basis	2.0
	8.24.4	Voor het beheer van cryptografische sleutels hanteer je de uitgangspunten van ISO 11770 (deel 3). Deze standaard gaat specifiek over securitytechnieken voor informatiebeveiliging.	BIV-Basis	2.0
Beveiligen tijdens de ontwikkelcyclus	8.25	Het team past vooraf vastgestelde regels toe voor het veilig ontwikkelen van software en systemen.	BIV-Basis	2.0
	8.25.1	Bij de ontwikkeling van webtoepassingen neem je voor de beveiliging passende maatregelen, waarbij de OWASP Secure Development als uitgangspunt geldt.	BIV-Basis	2.0
	8.25.2	Het testen en ontwikkelen van software en systemen wordt uitgevoerd op basis van de OTAP-methodiek.	BIV-Basis	2.0
Toepassingsbeveiligingseisen	8.26	Voor het ontwikkelen of aanschaffen van toepassingen stel je eisen op voor de informatiebeveiliging. Deze eisen leg je vast (met de diensteigenaar of in het contract met de leverancier).	BIV-Basis	2.0
Veilige systeemarchitectuur en technische uitgangspunten	8.27	Er zijn technische uitgangspunten vastgesteld voor het ontwerpen van veilige informatiesystemen. Je controleert regelmatig of de uitgangspunten nog aansluiten bij de actuele situatie.	BIV-Basis	2.0
Server- en applicatie-infrastructuur niet gedeeld	8.27.1	IT-services draaien in een eigen virtuele omgeving, zodat kwetsbaarheden bij een service geen toegang geven tot andere services.	BIV-Basis	2.0
Veilig coderen	8.28	Als je software ontwikkelt (ook als je dat iemand anders voor SURF laat doen), pas dan je de principes voor veilig coderen toe.	BIV-Basis	2.0
Testen van de beveiliging tijdens ontwikkeling en acceptatie	8.29	Tijdens het ontwikkelen en testen van software controleer je of de informatiebeveiliging voldoet aan de vooraf bepaalde eisen voor die beveiliging.	BIV-Basis	2.0
Penetratietesten	8.29.1	De dienst voert regelmatig pentesten uit. De benodigde frequentie is afhankelijk van de risicoanalyse. In ieder geval volgt een pentest in deze situaties: voor ingebruikname van nieuwe ICT na grote updates na grote wijzigingen Dit gebeurt door een vertrouwde partij (preferred supplier).	BIV-Basis	2.0
	8.29.2	Voordat je een systeem of applicatie in gebruik neemt, voer je een acceptatietest uit. Deze test is van tevoren beschreven en volgt een gestructeerde testmethode en is bijvoorkeur geautomatiseerd.	BIV-Basis	2.0
Uitbestede systeemontwikkeling	8.30	Je zorgt voor aansturing en controle van uitbestede systeem- of softwareontwikkeling. Je bewaakt de activiteiten en beoordeelt of ze voldoen aan de gestelde security-eisen.	BIV-Basis	2.0

Onderdeel	BIS-ID	Beheersmaatregel	BIV	Versie
	8.30.1	Bij een aanbestedingstraject bepaal je vooraf welk beschermingsniveau nodig is door een classificatie. Die classificatie maakt duidelijk welke verplichte beveiligingsmaatregelen je moet uitvragen bij de leverancier.	BIV-Basis	2.0
Scheiding van ontwikkel-, test- en productieomgevingen	8.31	De ontwikkel-, test- en productieomgevingen zijn gescheiden en beveiligd.	BIV-Basis	2.0
	8.31.1	Je mag niet testen in de productieomgeving, tenzij de diensteigenaar hiervoor van tevoren schriftelijk toestemming geeft.	BIV-Basis	2.0
	8.31.2	Je test wijzigingen voordat je ze in productie brengt. Alleen als de diensteigenaar van tevoren schriftelijk toestemming geeft, mag je hiervan afwijken.	BIV-Basis	2.0
Wijzigingsbeheer	8.32	Je volgt een procedure voor wijzigingsbeheer als je veranderingen doorvoert in informatieverwerkende systemen.	BIV-Basis	2.0
Noodgevallen	8.32.1	Als een verandering direct moet worden doorgevoerd, spreken we van een 'noodverandering'. Om te borgen dat dit kan plaatsvinden met minimale impact op systemen en toepassingen, moet dat op een gestandaardiseerde manier worden gedaan. Hiervoor wordt een noodprocedure vastgesteld voor wijzigingsbeheer. Deze procedure is gedocumenteerd, geautoriseerd en bekend.	B-Hoog	2.0
	8.32.2	In de procedure voor wijzigingsbeheer is ten minste aandacht voor: a. de administratie van wijzigingen; b. een risicoafweging van mogelijke gevolgen van de wijzigingen; c. een goedkeuringsprocedure voor wijzigingen.	BIV-Basis	2.0
	8.32.3	Voor het wijzigingsbeheer wordt een algemeen geaccepteerd framework zoals FitSM of ITIL gebruikt.	BIV-Basis	2.0
Testinformatie	8.33	Testgegevens moeten passend zijn geselecteerd, beschermd en beheerd.	BIV-Basis	2.0
	8.33.1	Je gebruikt geen productiedata in de testomgeving Voor de testomgeving gelden dezelfde beveiligingsmaatregelen als voor de productieomgeving.	BIV-Basis	2.0
	8.33.2	Als het gebruik van productiedata in een testomgeving onvermijdelijk is, dan wordt deze data geminimaliseerd en bij voorkeur geanonimiseerd dan wel gepseudonimiseerd.	BIV-Basis	2.0
Bescherming van informatiesystemen tijdens audits	8.34	Om een goed verloop van audits (zoals een pentest) te borgen en impact op productiesystemen te voorkomen, beperkt het onderzoek zich tot het noodzakelijke. Het verantwoordelijke management maakt hierover goede afspraken met de tester.	BIV-Basis	2.0