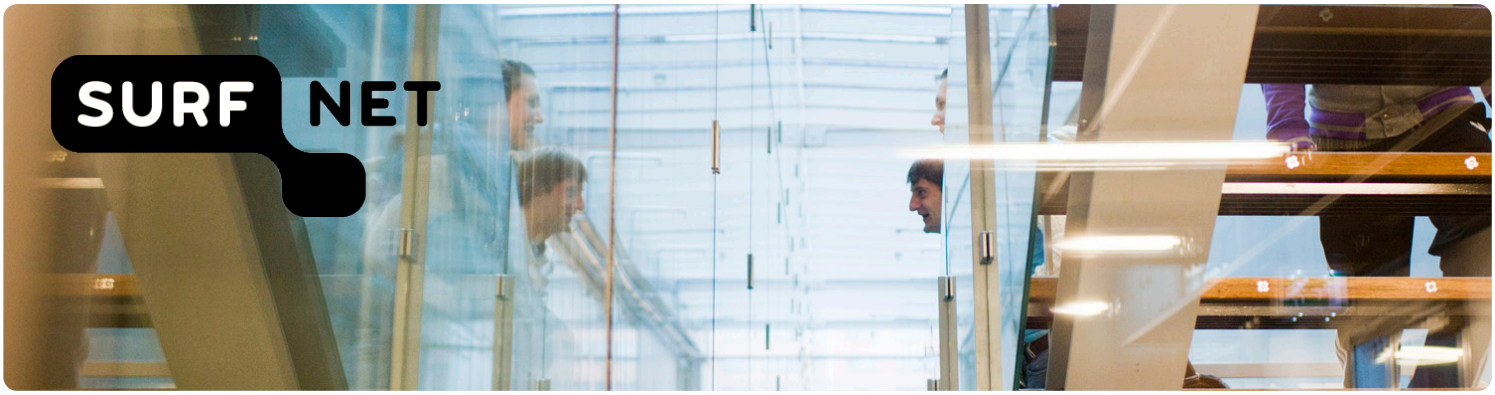


Baseline Informatiebeveiliging HO (BIHO)

Auteur(s): SCIPR (SURFibo)

Versie: 1.0

Datum: 1 mei 2015

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

088 - 787 30 00
admin@surfnet.nl
www.surfnet.nl

ING Bank NL54INGB0005936709
KvK Utrecht 30090777
BTW NL 0089.60.173.B01

Inhoudsopgave

SURF Community voor Informatiebeveiliging en PRivacy, voorheen SURFibo) is een Community of Practice met als doelen het actief stimuleren van en richting geven aan informatiebeveiliging en privacy binnen het hoger onderwijs (universiteiten, hogescholen, onderzoeksinstellingen en universitair medische centra). Dit doet SCIPR onder andere door het leveren van praktisch bruikbare adviezen, beleid en leidraden.

Dit document is vlak voor de naamswijziging van SURFibo naar SCIPR geschreven. Waar in de tekst SURFibo wordt genoemd, moer SCIPR gelezen worden.

Meer informatie over SURFibo staat op www.surf.nl onder het thema ‘Beveiliging en Privacy’.

Versiebeheer:

Maart 2015	Eerste versie Baseline informatiebeveiliging HO

1 Inleiding

Het door SURFibo ontwikkelde model informatiebeveiligingsbeleid stelt dat het Hoger Onderwijs met betrekking tot informatiebeveiliging de relevante maatregelen conform ISO-27002 zal treffen. De Nederlandse overheid hanteert deze ISO-standaard ook als norm. De praktijk wijst uit dat het invoeren van deze ISO-standaard niet eenvoudig is, met als belangrijke oorzaak zijn grote abstractheid waardoor er veel discussie kan zijn over de vertaling in concrete maatregelen.

De overheid heeft het 'ICT-deel' van haar tactische variant van de ISO-27002, de Baseline Informatiebeveiliging Rijksoverheid-Tactisch NormenKader (BIR-TNK), doorvertaald naar operationele maatregelen en opgenomen in de BIR-OH (Operationele Handreiking). Ook in het Hoger Onderwijs is behoefte aan meer concrete beveiligingsmaatregelen. In dit document wordt de BIR verder toegelicht, waarom deze ook voor het Hoger Onderwijs geschikt is en hoe deze Baseline Informatiebeveiliging HO (BIHO) toegepast kan worden.

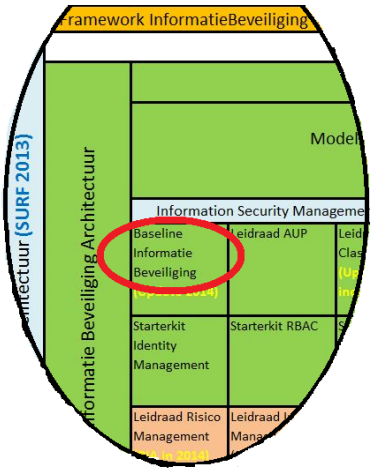
Dit document is bedoeld voor de gebruikers van de maatregelen in het Hoger Onderwijs: de functionarissen informatiebeveiliging zoals security officers, projectleiders van ICT-projecten, ICT-architecten en ICT beheerders.

2 Context

De normen en maatregelen in de BIR zijn gebaseerd op een vertrouwelijkheidsniveau dat hoort bij gegevens met de classificatie ‘Departementaal Vertrouwelijk’, vergelijkbaar met ‘Voor Intern Gebruik’ en het niveau WBP risicoklasse II : verhoogd risico. Dit type gegevens komt ook veelvuldig voor in het Hoger Onderwijs. SURFibo heeft vastgesteld dat het risicoprofiel voor het Hoger Onderwijs en Onderzoek zoals weergegeven in het “Cyberdreigingsbeeld Sector Hoger Onderwijs en Wetenschappelijk Onderzoek” (2105) veel overeenkomst vertoont met het risicoprofiel van Rijksoverheid. Vanwege de grote overeenkomsten in vertrouwelijkheidsniveau en risicoprofiel stelt SURFibo dat de BIR (inclusief de Rijks-specifieke maatregelen) als basis kan dienen voor een baseline informatiebeveiliging voor instellingen in het Hoger Onderwijs (BIHO).

Hoe past deze BIHO in het SURFibo Framework Informatiebeveiliging, waarvan een gedeelte in onderstaande uitsnede is weergegeven? Relevant in het kader van de BIR-OH binnen het framework zijn de volgende documenten:

Product	**Inhoud**	**Dd**
HORA	Een set architectuurmodellen en –principes voor het hoger onderwijs, geïnspireerd op de NORA. Bevat IB-principes en classificaties.	07-2014
Starterkit informatiebeveiliging	Een uitgewerkte procesgerichte aanpak (in fasen) om informatiebeveiliging op gang te brengen en houden.	12-2010
Model beleid IB	Template informatiebeveiligingsbeleid.	05-2015
Normenkader HO / SURFaudit	***85*** normen uit ISO 27002-2013 voor het hoger onderwijs, als basis voor de SURFaudit door SURF stuurgroep Informatiebeveiliging en privacy geaccordeerd.	
Baseline Informatiebeveiliging HO (BIHO)	Operationele set maatregelen voor het HO op basis van BIR-TNK en BIR-OH	Nu



Juridisch normenkader Cloud Services	Toetsmodel waaraan de diensten van een leverancier (van cloudservices) getoetst wordt.	11-2013	
Technische handreikingen	Defacto standaards zoals OWASP.	Divers	

Bij het opstellen van de set operationele maatregelen voor het Hoger Onderwijs op basis van de BIR is geconstateerd dat het onderscheid tussen de tactische normen uit de BIR-TNK en de operationele maatregelen uit de BIR-OH niet consequent wordt gehanteerd.

Daarom is besloten bij het samenstellen van de 'best practice' maatregelen set voor het HO, de BIHO uit beide documenten te putten.

De BIHO bestaat uit twee delen, het eerste deel bevat de normen uit het normenkader HO aangevuld met concrete maatregelen uit de BIR en in sommige gevallen is daar '***evidence***'[1] of ***UMCCloud***[2] aan toegevoegd. Het tweede deel bevat normen uit de BIR-TNK die niet in het normenkader HO voorkomen. Het Rijk stelt deze normen verplicht, het is voorstelbaar dat de BIHO en BIR-TNK naar elkaar zullen groeien.

Het is niet verplicht om de 'best practice' letterlijk over te nemen, maar door deze zo volledig mogelijk te volgen, komt de instelling in lijn met het normenkader HO/ SURFaudit normenkader. Het advies aan de instellingen is om de invulling van alle maatregelen conform het principe "pas toe of leg uit" vast te leggen.

In bijlage III is de BIHO opgenomen, deze is ook in Excelformaat te downloaden van de SURFibo site.

[1] de evidence-lijst uit SURFaudit, opgesteld door internal -auditors HO

[2] "normdocument clouddiensten" van de gezamenlijke Universitaire Medische Centra

3 Toepassen BIHO binnen de instelling

Geadviseerd wordt om de ICT-maatregelen uit de BIHO als volgt toe te passen:

1. Stel vast dat de set 'best practice' ICT-beveiligingsmaatregelen de norm is;
2. Bepaal de gap met de set 'best practice' ICT-beveiligingsmaatregelen, daarvoor kan het onderstaand schema worden gebruikt:

GAP-analyse				Impactanalyse			
Aanwezig Is de maatregel geïmplementeerd **ja/nee/** **gedeeltelijk/ nvt/onbekend**	**Hoe geïmplementeerd Omschrijving hoe en waar (instellingsbreed /onderdeel) geïmplementeerd**	**Eigenaar van de maatregel naam /afdeling**		**Status**	**Actiehouder Wie is aanspreekbaar/ verantwoordelijk voor implementatie van de maatregel**	**Planning Datum gereed**	**Geaccepteerd risico = management-besluit**

In de kolom „Aanwezig" kunnen de volgende keuzes gemaakt worden:

- Ja: De maatregel is aanwezig. Vul ook de vindplaats in, wie de maatregel uitvoert, waar de maatregel is vastgelegd en overige bijzonderheden.
- Nee: Er is niets gevonden.
- Gedeeltelijk: De maatregel is gedeeltelijk geïmplementeerd.
- Niet van toepassing: De maatregel is niet van toepassing. Vul daarbij ook een reden in!
- Onbekend: Onduidelijk of er iets is dat voldoet.

Vervolgens kan het deel 'Impactanalyse' worden ingevuld, door voor de nog niet genomen maatregelen of de onbekende maatregelen kan een status worden aangegeven:

- Geïmplementeerd: Een maatregel is volledig geïmplementeerd.
- Deels geïmplementeerd: Een maatregel is deels aanwezig.

- Te implementeren: De maatregel gaat geïmplementeerd worden binnen afzienbare tijd.
- Niet geïmplementeerd: De maatregel moet nog geïmplementeerd worden.

- Niet van toepassing: De maatregel is niet van toepassing.
- Nog niet onderzocht: De maatregel is nog niet onderzocht.
- Overgedragen: De maatregel is overgedragen (bijvoorbeeld aan een andere beheerorganisatie).
- Geaccepteerd risico: Een maatregel wordt niet genomen, het risico dat gelopen wordt door het niet nemen wordt geaccepteerd.

3. Vervolgens kan een plan van aanpak worden opgesteld waarin wordt beschreven hoe de uitkomsten van de GAP-analyse worden afgehandeld. Dit plan van aanpak is daarmee onderdeel van de PDCA-cyclus.

4. Tenslotte kan een peer-review of een externe audit uitgevoerd worden om te checken of de juiste maatregelen zijn genomen en of (op basis van de evidence-lijst) het gewenste volwassenheidsniveau is bereikt.

BIJLAGE I: Tabel relevante documenten

Product	Inhoud	Dd
Starterkit informatiebeveiliging	Een uitgewerkte procesgerichte aanpak (in fasen) om informatiebeveiliging op gang te brengen en houden.	12-2010
Model beleid IB	SURFibo Template informatiebeveiligingsbeleid	05-2015
NEN-ISO 27001:2013	Internationale specificatie van eisen waaraan een ISMS (Information Security Management System) ofwel managementsysteem voor informatiebeveiliging) moet voldoen.	2013
NEN-ISO 27002:2013	Een praktische set maatregelen waarmee informatiebeveiliging geïmplementeerd kan worden.	2013
SURFaudit 6-cluster	De normenset (85 normen) door SURFibo opgesteld voor het hoger onderwijs opgesteld op basis van ISO-27002:2013	02-2015
Juridisch normenkader Cloud Services	SURF Toetsmodel waaraan de diensten van een leverancier van cloudservices getoetst kan worden op security & privacy.	11-2013
BIR TNK	Het tactische normenkader van de BIR. De TNK is verplicht bij de Rijksoverheid (Pas toe of leg uit / comply or explain). Het is een verbijzondering van NEN-ISO 27002. Het beoogde niveau van de baseline is “departementaal vertrouwelijk en WBP risicoklasse II”	12-2-2012
QuickScan BIR	Het uitvoeren van de QuickScan BIR geeft aan of de BIR maatregelen voldoende zijn voor beveiliging van specifieke processen met ondersteunende informatiesystemen.	21-01-2014
Technische baselines	Baselines zoals de Application Security Verification Standaard van OWASP, de technical baselines van ENISA, de standaarden die door het NIST zijn voorgesteld en het raamwerk beveiliging van web applicaties door het NCSC. (De facto standaards)	
HORA	Een set architectuurmodellen en –principes voor het hoger onderwijs, geïnspireerd op de NORA.	07-2014

	Bevat beperkt (enkele principes) rond IB.	
IBA	SURFibo InformatieBeveiligings Architectuur	11-2012

BIJLAGE II: Overzicht geraadpleegde externe bronnen

BIR-OH (www.earonline.nl/images/.../BIR_Operationele_Handreiking_v1_0.pdf)

ENISA (http://www.enisa.europa.eu/)

Relevante maatregelen in:

- http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures/technical-guideline-on-minimum-security-measures
- http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting/technical-guideline-on-incident-reporting
- http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/brokerage-model-for-network-and-information-security-in-education
- http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
- http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/recommended-cryptographic-measures-securing-personal-data

NIST (http://www.nist.gov/information-technology-portal.cfm)

Interessant is de configuratiehandleiding die voor veelgebruikte IT componenten beschikbaar is:

- https://web.nvd.nist.gov/view/ncp/repository?startIndex=0
- met bijvoorbeeld voor FireFox (via een zusterorganisatie Center for Internet Security): https://benchmarks.cisecurity.org/tools2/CIS_Mozilla_Firefox_24_ESR_Benchmark_v1.0.0.pdf

OWASP (http://www.owasp.org/)

OWASP levert vooral de Application Security Verification Standaard (https://www.owasp.org/images/5/58/OWASP_ASVS_Version_2.pdf) en drie How-to's:

How to develop secure applications: https://github.com/OWASP/DevGuide met meest concreet https://github.com/OWASP/DevGuide/tree/master/03-Build, ideaal voor ontwikkelaars, de How to test application security (een uitgebreide, praktische gids hoe te testen) en de How to code review.

NCSC (www.ncsc.nl)

Interessant zijn de alerts (bekende kwetsbaarheden met oplossing) en het raamwerk beveiliging webapplicaties:

- https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen

- https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/raamwerk-beveiliging-webapplicaties.html

SANS (www.sans.org)

4 BIJLAGE III: maatregelen set Baseline Informatiebeveiliging HO

Legenda:

Bronnen:

BIR	Baseline Informatiebeveiliging Rijksdienst
BIR-TNK	BIR-Tactisch Normenkader
BIR-OH	BIR-Operationele Handreiking
Evidence	Element uit de evidence-lijst opgesteld door internal-auditors HO
ISO	Element uit ISO27002:2013
UMCcloud	Element uit "normdocument clouddiensten" van de gezamenlijke Universitaire Medice Centra
NORA	Nederlandse Overheid Referentie Architectuur
(O)	Maatregel uit <bron> is aangepast voor de Onderwijssector

Afkortingen en Begrippen

RA(S)CI matrix matrix met rollen in een proces: Responsible, Accountable, (to offer Support,) to be Consulted, to be Informed

BIA	Business Impact Analyses
PIA	Privacy Impact Assessment
OTAP	Ontwikkeling, Test, Acceptatie en Productie
BYOD	Bring Your Own Device
DMZ	DeMilitarized Zone
NAT	Network Address Translation: een technologie waarbij een prive-adresrange wordt verbonden met internet via een router met 1 openbaar netwerkadres
DNS	Domein Name System
spoofing	Zich voordoen als iemand/iets anders (andermans naam, IP-adres etc.)
zero-footprint	Applicaties kunnen worden gebruikt zonder software installatie op de client en zonder achterlating van applicatiedata op de client
reverse proxy	Een proxy server die namens een client data ophaalt bij meerder servers, doorgaans in een intern netwerk.
hardened	Een verhoogd beveiligingsniveau door beperking van het aantal kwetsbare configuratieonderdelen
multifunctionals	Apparaten met meerdere functionele doelen, meestal printen, kopiëren en scannen/faxen

Hoofdstuk 1: Beleid en organisatie

Nr. SURF-audit	ISO-27002:2013	Norm	Maatregel	Bron
1.1	5.1.1.1	**Beleidsregels voor informatiebeveiliging:** Ten behoeve van informatiebeveiliging is een reeks beleidsregels gedefinieerd en goedgekeurd door het bestuur.	Het bestuur van de instelling stelt beleid voor informatiebeveiliging vast.	BIR-TNK
1.2	5.1.1.2	**Beleidsregels voor informatiebeveiliging**: De beleidsregels voor informatiebeveiliging zijn gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Het door het bestuur vastgestelde informatiebeveiligingbeleid wordt gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen (bijv. in nieuwsbrieven, op interne websites en in jaargesprekken met medewerkers)	Evidence

1.3	5.1.2	**Beoordeling van het informatiebeveiligingsbeleid:** Het beleid voor informatiebeveiliging wordt met geplande tussenpozen of als zich significante veranderingen voordoen, beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	De informatiebeveiligingsfunctionaris biedt jaarlijks een verslag over de kwaliteit van informatiebeveiliging aan aan bestuur en CIO. Als onderdeel van de jaarrekeningcontrole beoordeelt de huisaccountant jaarlijks de informatiebeveiliging. De instelling laat zich tweejaarlijks beoordelen tijdens een peer-review	BIR-TNK
1.4	6.1.1	**Taken en verantwoordelijkheden informatiebeveiliging:** Alle verantwoordelijkheden bij informatiebeveiliging zijn gedefinieerd en toegewezen.	(O) Het lijnmanagement waarborgt dat de informatiebeveiligingsdoelstellingen worden vastgesteld, voldoen aan de kaders zoals gesteld in het beleidsdocument en zijn geïntegreerd in de relevante processen.	BIR-TNK
			(O) Functiebeschrijvingen, mandateringsbesluiten en/of RACI matrices bevatten verantwoordelijkheden voor het opstellen, onderhouden, vaststellen van en toezicht houden op informatiebeveiliging.	BIR-TNK
			(O) Er is een disciplinair proces vastgelegd voor medewerkers die inbreuk maken op het beveiligings- en/of privacybeleid.	BIR-TNK
1.5	6.1.5	**Informatiebeveiliging in projectbeheer:** Informatiebeveiliging komt aan de orde in projectbeheer, ongeacht het soort project.	De ontwikkel- en projectmethodieken van de organisatie beschrijven de vereiste aandacht voor informatiebeveiliging, bevat templates met beveiligingsparagraaf en geeft een duidelijke rol voor de informatiebeveiligingsfunctionaris. Een BIA is verplicht bij projecten met grote impact of hoge risicoklasse en betreft het persoonsgegevens dan is een PIA verplicht.	Evidence
1.6	6.2.1.1	**Beleid voor mobiele apparatuur:** Beleid en ondersteunende beveiligingsmaatregelen zijn vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	Per risicoklasse is vastgesteld of, en welke, mobiele datadragers worden toegestaan. Toegang tot gegevensbronnen wordt technisch (onafhankelijk van de locatie) afgedwongen.	BIR-OH

1.7	8.2.1	**Classificatie van informatie:** Informatie is geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	(O) De organisatie heeft een informatie classificatierichtlijn (zoals de SURFibo "Richtlijn classificatie") opgesteld.	BIR-TNK
			(O) De eigenaar van de informatie kent een classificatie voor beschikbaarheid, integriteit, vertrouwelijkheid en eventuele andere kwaliteitscriteria toe.	BIR-TNK
			De classificatie wordt jaarlijks en bij grote wijzigingen uitgevoerd dan wel herijkt.	Evidence
1.8	8.2.2	**Informatie labelen:** Om informatie te labelen is een passende reeks procedures ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	De organisatie heeft procedures voor het labelen van informatie vastgesteld en gecommuniceerd. Te denken valt aan het labelen van met name papieren documenten, dossiers en backups.	BIR-TNK
1.9	10.1.1.1	**Beleid inzake het gebruik van cryptografische beheersmaatregelen:** Ter bescherming van informatie is een beleid voor het gebruik van cryptografische beheersmaatregelen ontwikkeld en geïmplementeerd	De organisatie heeft middels beleid vastgesteld welke cryptografische voorzieningen voor welke toepassingen ingezet worden.	BIR-OH
			De data op harddisks in laptops is versleuteld (volgens het pre-boot harddisk encryptie principe).	BIR-OH
			Vertrouwelijke gegevens worden alleen versleuteld opgeslagen op mobiele datadragers. (Zie https://www.aivd.nl/onderwerpen/infobeveiliging/beveiligingsproducte/goedgekeurde/)	BIR-OH

1.10	10.1.1.2	**Beleid inzake het gebruik van cryptografische beheers-maatregelen:** Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van crypto grafische beheersmaatregelen wordt geïmplementeerd.	(O) De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria, zoals: - NIST (US)/CSE (Canada) FIPS 140-2 (http://en.wikipedia.org/wiki/FIPS_140); - het Nationaal Bureau voor Verbindingsbeveiliging (AIVD/NBV) op https://www.aivd.nl/onderwerpen/infobeveiliging/beveiligingsproducte/inzetadviezen/	BIR-TNK
			Daar waar mogelijk zijn ICT producten gebruikt die volgens een internationaal geaccepteerde standaard/organisatie geëvalueerd zijn. Waar het niet mogelijk is met goedgekeurde producten te werken wordt gebruik gemaakt van robuuste algoritmen met een voldoende lange sleutel. Voor verbindings- en dataencryptie is dit minimaal AES met een sleutellengte van 256 bits of gelijkwaardig. Voor hash algoritmen is dit minimaal SHA2 of gelijkwaardig.	BIR-OH
			Zie BIR-OH aanbeveling bij 10.1.1.1 hierboven.	BIR-OH
1.11	11.2.5	**Verwijdering van bedrijfsmiddelen:** Apparatuur, informatie en software wordt niet zonder toestemming vooraf van de locatie meegenomen.	De ICT gedragsregels bevatten de clausule dat apparatuur, informatie en programmatuur van de organisatie pas na toestemming van de locatie kan worden meegenomen.	BIR-TNK

1.12	13.2.1	**Beleid en procedures voor informatietransport:** Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, zijn formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht.	(O) Bij transport van vertrouwelijke informatie over onvertrouwde netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast.	BIR-TNK BIR-OH
			(O) Er zijn procedures opgesteld en geïmplementeerd voor opslag van vertrouwelijke informatie op verwijderbare media.	BIR-TNK
			(O) Verwijderbare media met vertrouwelijke informatie mogen niet onbeheerd worden achtergelaten op plaatsen die toegankelijk zijn zonder toegangscontrole	BIR-TNK
			(O) Het meenemen van instellingsvertrouwelijke informatie buiten gecontroleerd gebied vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is.	BIR-TNK
			(O) Fysieke verzending van bijzondere informatie dient te geschieden met goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.	BIR-TNK
			(O) Digitale documenten waar derden rechten aan kunnen ontlenen worden verzonden met gebruikmaking van een certificaat uitgegeven door een erkende root CA (Certificate Authority) en CSP (Certificate Service Provider). .	BIR-TNK
			(O) Er is een (spam) filter geactiveerd voor e-mail berichten.	BIR-TNK
			Er worden standaard communicatieprotocollen gebruikt die geen afbreuk doen aan het gewenste beveiligingsniveau.	BIR-OH

1.13	13.2.2	**Overeenkomsten over informatietransport:** Er zijn overeenkomsten vastgesteld voor het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	ISO
1.14	14.1.1	**Analyse en specificatie van informatiebeveiligingseisen:** De eisen die verband houden met informatiebeveiliging zijn opgenomen in de eisen voor nieuwe informatiesystemen en voor uitbreidingen van bestaande informatiesystemen	De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Evidence
1.15	15.1.2	**Opnemen van beveiligingsaspecten in leveranciersovereen-komsten:** Alle relevante informatiebeveiligingseisen zijn 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.	(O)Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie (bijv. risicoklasse van WBP) heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn.	BIR-TNK
			Bij overeenkomsten met (cloud) leveranciers wordt het Juridisch normenkader van SURF toegepast.	Evidence
			(O) Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkerovereenkomst (conform WBP artikel 14) afgesloten.	BIR-TNK
1.16	15.1.3	**Toeleveringsketen van informatie- en communicatie-technologie:** Overeenkomsten met leveranciers bevatten eisen die betrekking hebben op deinformatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	Als er gebruikt gemaakt wordt van onderaannemers dan gelden daar dezelfde beveiligingseisen voor als voor de contractant. De hoofdaannemer is verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken. (Bij toepassing van het Juridisch normenkader van SURF is aan deze eis voldaan.)	BIR-TNK

1.17	16.1.1	**Verantwoordelijkheden en procedures:** Directieverantwoordelijkheden en -procedures zijn vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen	ISO
			Beveiligingsincidenten worden meteen (volgens een vooraf opgestelde procedure) aan de (Corporate) Information Security Officer en/of ICT-beveiligingsmanager gemeld. Bewijsmateriaal wordt hierbij overhandigd.	BIR-OH
1.18	16.1.2	**Rapportage van informatiebeveiligingsgebeurtenissen:** Informatiebeveiligingsgebeurtenissen worden zo snel mogelijk via de juiste leidinggevende niveaus gerapporteerd.	(O) Er is een contactpersoon aangewezen voor het rapporteren van beveiligingsincidenten. Voor integriteitsschendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt.	BIR-TNK
			Procedures zijn schriftelijk vastgelegd en maatregelen zijn aanwezig om alle delen en /of de functionaliteit van een clouddienst onmiddelijk buiten gebruik te stellen in geval van een beveiligingsincident.	UMCcloud
1.19	18.1.3	**Beschermen van registraties:** Registraties worden in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	a) De instelling verstrekt richtlijnen voor het bewaren, opslaan, behandelen en verwijderen van registraties en informatie; b) De instelling stelt een bewaarschema op waarin registraties en de periode dat ze moeten worden bewaard, zijn vastgelegd; c) De instelling houdt een inventarisoverzicht bij van bronnen van belangrijke informatie.	BIR-TNK

1.20	18.1.4	**Privacy en bescherming van persoonsgegevens:** Privacy en bescherming van persoonsgegevens worden, voor zover van toepassing, gewaarborgd in overeenstemming met relevante wet- en regelgeving.	a) Alle verwerkingen waarin persoonsgegevens zijn opgenomen, zijn geïnventariseerd; b) Relevante wet- en regelgeving is geïnventariseerd; c) Passende maatregelen voor beveiliging zijn vastgesteld; d) Vastgestelde maatregelen zijn geïmplementeerd; e) Maatregelen worden jaarlijks gecontroleerd op juiste implementatie.	Evidence
1.21	6.1.2.1	**Scheiding van taken:** Conflicterende taken en verantwoordelijkheden zijn gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	1. Niemand in een organisatie of proces mag op uitvoerend niveau rechten hebben om een gehele cyclus van handelingen in een kritisch informatiesysteem te beheersen. Dit in verband met het risico dat hij of zij zichzelf of anderen onrechtmatig bevoordeelt of de organisatie schade toe brengt. Dit geldt voor zowel informatieverwerking als beheeracties. 2. Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerswerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstak en alleen wanneer ingelogd als gebruiker. 3. Vóór de verwerking van gegevens die de integriteit van kritieke informatie of kritieke informatie systemen kunnen aantasten worden deze gegevens door een tweede persoon geïnspecteerd en geaccepteerd. Van de acceptatie wordt een log bijgehouden. 4. Verantwoordelijkheden voor beheer en wijziging van gegevens en bijbehorende informatiesysteemfuncties moeten eenduidig toegewezen zijn aan één specifieke (beheerders)rol.	BIR-TNK

Hoofdstuk 2: Personeel, studenten en gasten

Nr. SURF-audit	ISO-27002:2013	Norm	Maatregel	Bron
2.1	7.1.2	**Arbeidsvoorwaarden:** De contractuele overeenkomst met medewerkers en contractanten vermeldt hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie.	De algemene voorwaarden van het (arbeids)contract van medewerkers en contractanten bevatten de wederzijdse verantwoordelijkheden ten aanzien van beveiliging. Het is aantoonbaar dat medewerkers bekend zijn met hun verantwoordelijkheden op het gebied van beveiliging.	BIR-TNK
			(O) Indien een medewerker of contractant speciale verantwoordelijkheden heeft t.a.v. informatiebeveiliging dan is hem dat voor indiensttreding (of bij functiewijziging), bij voorkeur in de aanstellingsbrief of bij het afsluiten van het contract, aantoonbaar duidelijk gemaakt.	BIR-TNK

2.2	7.2.2	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging:** Alle medewerkers van de organisatie en, voor zover relevant, contractanten krijgen een passende bewustzijnsopleiding en -training en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten ten aanzien van het gevaar van virussen en dergelijke, zoals: - publicatie/verspreiding beeidsregels - periodieke awareness programma's zoals via nieuwsbrieven/flyers; - installatie van beveiligingsprogrammatuur die waarschuwt bij onvertrouwde content; - periodieke bespreking van ICT gedragsregels.	ISO
2.3	9.2.6	**Toegangsrechten intrekken of aanpassen:** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten worden bij beëindiging van hun dienstverband, contract of overeenkomst verwijderd, en bij wijzigingen worden ze aangepast.		ISO
2.4	11.2.9	**‘Clear desk’- en ‘clear screen’-beleid:** Er is een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen' beleid voor informatieverwerkende faciliteiten ingesteld.	(O) Schermbeveiligingsprogrammatuur (een screensaver) maakt na een periode van inactiviteit van maximaal 15 minuten alle informatie op het beeldscherm onleesbaar en ontoegankelijk.	BIR-TNK
			(O) Werkstation lock wordt automatisch geactiveerd bij het verwijderen van een token (indien aanwezig).	BIR-TNK
			Op mobiele werkplekken wordt het zero-footprint principe toegepast.	BIR-OH
			Adresboeken en telefoongidsen waarin locaties met gevoelige IT voorzieningen staan zijn niet aanwezig in vrij toegankelijke gebieden.	Evidence

2.5	13.2.4	**Vertrouwelijkheids- of geheimhoudingsovereenkomst:** Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, zijn vastgesteld en worden regelmatig beoordeeld en gedocumenteerd.	De organisatie heeft actuele vertrouwelijkheids- of geheimhoudingsovereenkomsten in gebruik.	Evidence
2.6	16.1.3	**Rapportage van zwakke plekken in de informatiebeveiliging:** Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie wordt geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	a) De ICT gedragsregels dragen gebruikers op vermeende of waargenomen zwakke beveiligingsplekken te melden; b) Meldpunten zijn gecommuniceerd aan alle werknemers, ingehuurd personeel en externe gebruikers.	Evidence
2.7	7.1.1.1	**Screening:** Verificatie van de achtergrond van alle kandidaten voor een dienstverband wordt uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en staat in verhouding tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Bij aanstelling worden de gegevens die de medewerker heeft verstrekt over zijn arbeidsverleden en scholing geverifieerd. Voor vertrouwensfuncties of functies die vanwege hun rol toegang tot gevoelige of vertrouwelijke gegevens hebben (zoals bijv. IT-beheerders) kan overwogen een relevante Verklaring omtrent Gedrag (VOG) te vragen of een via veiligheidsonderzoek een Verklaring geen Bezwaar (VGB) te verkrijgen.	BIR-TNK

Hoofdstuk 3: Ruimtes en apparatuur

Nr. SURF-audit	ISO-27002:2013	Norm	Maatregel	Bron
3.1	6.2.1.2	**Beleid voor mobiele apparatuur:** Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.		ISO
3.2	8.3.2	**Verwijderen van media:** Media worden overeenkomstig formele procedures op een veilige en beveiligde manier verwijderd als ze niet langer nodig zijn.	(O) Er zijn procedures vastgesteld en in werking voor verwijderen van vertrouwelijke data en de vernietiging van verwijderbare media. Verwijderen van data wordt gedaan met een Secure Erase voor apparaten waar dit mogelijk is. In overige gevallen wordt de data twee keer overschreven met vaste data, één keer met random data en vervolgens wordt geverifieerd of het overschrijven is gelukt. Zie ook 9.2.6	BIR-TNK
			Backup media worden pas na vernietiging van de data erop hergebruikt voor andere systemen.	BIR-OH

3.3	11.1.1	**Fysieke beveiligingszone:** Beveiligingszones zijn gedefinieerd en worden gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	(O) Serverruimtes, datacenters en daar aan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende best practices. Een goed voorbeeld van zo'n best practice is Telecommunication Infrastructure Standard for Data Centers (TIA-942).	BIR-TNK
3.4	11.1.2	**Fysieke toegangsbeveiliging:** Beveiligde gebieden zijn beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	1. Zones zijn bepaald; 2. Toegangsbeveiliging tot deze zones is beschreven; 3. Maatregelen voor toegangsbeveiliging zijn actueel een aanwezig.	Evidence
			(O) Er vindt minimaal één keer per half jaar een controle/evaluatie plaats op de autorisaties voor fysieke toegang tot beveiligde zones.	BIR-TNK
3.5	11.1.3	**Kantoren, ruimten en faciliteiten beveiligen:** Voor kantoren, ruimten en faciliteiten is fysieke beveiliging ontworpen en deze wordt toegepast.	(O) Ten behoeve van opslag van vertrouwelijke informatie vindt actief beheer (sleutelafspraken, sleutelplan) van kasten en kluizen plaats.	BIR-TNK
			Fysieke toegang tot de multifunctionals van administratieve afdelingen is niet mogelijk vanuit publieke ruimtes. Is dit niet gewenst dan wordt beveiligd printen ingericht.	BIR-OH

3.6	11.1.4	**Beschermen tegen bedreigingen van buitenaf:** Tegen natuurrampen, kwaadwillige aanvallen of ongelukken is fysieke bescherming ontworpen en deze wordt toegepast.	1. Fysieke maatregelen tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vorm van natuurlijke of menselijke calamiteiten zijn vastgesteld; 2. Vastgestelde maatregelen zijn actueel en aanwezig.	BIR-TNK
			(O) Bij het betrekken van nieuwe gebouwen wordt een locatie gekozen waarbij rekening wordt gehouden met de kans op en de gevolgen van natuurrampen en door mensen veroorzaakte rampen.	BIR-TNK
			(O) Er is door de brandweer goedgekeurde en voor de situatie geschikte brandblusapparatuur geplaatst en aangesloten. Dit wordt jaarlijks gecontroleerd.	BIR-TNK
3.7	11.1.5	**Werken in beveiligde gebieden:** Voor het werken in beveiligde gebieden zijn procedures ontwikkeld en deze worden toegepast.	1. Procedures/ werkinstructies/ richtlijnen voor werken in beveiligde ruimtes zijn aanwezig en actueel; 2. Procedures, werkinstructies of richtlijnen zijn initieel gecommuniceerd en blijvend vindbaar voor de medewerkers, zoals via intranet waarin is beschreven de "op te vragen informatie" mbt fysieke maatregelen voor belangrijke ruimtes en het handboek BHV.	Evidence
3.8	11.1.6	**Laad- en loslocatie:** Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, worden beheerst, en zo mogelijk afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	Maatregel is al opgenomen in 11.1.2.	Evidence
			(O) Er bestaat een procedure voor het omgaan met verdachte pakketten en brieven in postkamers en laad- en losruimten.	BIR-TNK

3.9	11.2.1	**Plaatsing en bescherming van apparatuur:** Apparatuur is zodanig geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	Er is beleid en/of een Plan van Aanpak opgesteld waarin het proces en de instrumenten voor plaatsing van bedrijfskritische apparatuur zoveel mogelijk te standaardiseren en te automatiseren.	Evidence
			(O) De toegang voor onderhoud op afstand [aan toepassingen met een verhoogd risico] door een leverancier wordt alleen opengesteld op basis een wijzigingsverzoek of storingsmelding.	BIR-TNK
			Servers bevinden zich in een afgesloten ruimte, waarbij alleen geautoriseerd personeel fysiek toegang heeft tot de systemen.	BIR-OH
			De draadloze toegangspunten zijn dusdanig gepositioneerd dat men op de daarvoor bestemde plaatsen betrouwbaar gebruik kan maken van het draadloze netwerk.	BIR-OH
			De draadloze toegangspunten zijn dusdanig gepositioneerd dat er onderling geen interferentie optreed.	BIR-OH
			De draadloze toegangspunten zijn fysiek onbereikbaar voor onbevoegden zodat onbeschikbaarheid door fysiek ingrijpen voorkomen wordt.	BIR-OH
3.10	11.2.2	**Nutsvoorzieningen:** Apparatuur is beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.	1. Lijst met essentiele apparatuur is aanwezig; 2. Essentiele apparatuur is beschermd tegen stroomuitval en andere storingen, zoals door: - overspanningsbeveiliging; - ontworpen en ingerichte operationele noodstroomvoorziening(en); - regelmatige inspecties en noodstroomtests.	Evidence

3.11	11.2.3	**Beveiliging van bekabeling:** Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, zijn tegen interceptie of beschadiging beschermd.	1. Maatregelen voor beveiligen van voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt zijn vastgesteld in overeenstemming met de risicoklasse; 2. Maatregelen zijn ingericht en actueel.	Evidence
3.12	11.2.4	**Onderhoud van apparatuur:** Apparatuur wordt op correcte wijze onderhouden, om de continue beschikbaarheid en integriteit ervan te waarborgen.	(O) Reparatie en onderhoud van apparatuur (hardware) vindt op locatie plaats door bevoegd personeel, tenzij er geen data op het apparaat aanwezig of toegankelijk is.	BIR-TNK
			1. Beleid voor classificatie, waarborgen en onderhouden van apparatuur is aanwezig en actueel; 2. Formele verantwoordelijkheden voor onderhoud zijn vastgelegd; 3. Onderhoudscontracten voor onderhoud van belangrijke apparatuur zijn afgesloten.	Evidence
3.13	11.2.6	**Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein:** Bedrijfsmiddelen die zich buiten het terrein bevinden worden beveiligd waarbij rekening wordt gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	a) De risico's van het werken met bedrijfsmiddelen buiten het terrein zijn geïnventariseerd; b) Beveiligingsmaatregelen passend bij het risiconiveau zijn getroffen. Te denken valt aan: beperkingen in gebruiksmogelijkheden, versleuteling van gegevens en verbindingen, communicatie van gedragsregels, speciaal ingerichte apparatuur en verzekering.	Evidence
			(O) Bij melding van verlies of diefstal [van een mobiel apparaat] wordt de communicatiemogelijkheid met de centrale applicaties afgesloten.	BIR-TNK

3.14	11.2.7	**Veilig verwijderen of hergebruiken van apparatuur:** Alle onderdelen van de apparatuur die opslagmedia bevatten, 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.	(O) Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de beheersorganisatie ingeleverd. De beheerorganisatie zorgt voor een verantwoorde afvoer zodat er geen data op het apparaat aanwezig of toegankelijk is. Als dit niet kan wordt het apparaat of de informatiedrager fysiek vernietigd. Het afvoeren of vernietigen wordt per organisatieonderdeel geregistreerd.	BIR-TNK
			(O) Hergebruik van apparatuur buiten de organisatie is slechts toegestaan indien de informatie is verwijderd met een voldoende veilige methode. Een veilige methode is Secure Erase voor apparaten die dit ondersteunen. In overige gevallen wordt de data twee keer overschreven met vaste data, één keer met random data en vervolgens wordt geverifieerd of het verschrijven is gelukt.	BIR-TNK
			(O) Indien de multifunctional opslagmedia bevat worden deze op veilige wijze gewist of vernietigd voordat de multifunctional afgevoerd wordt.	BIR-OH
3.15	12.4.4	**Kloksynchronisatie:** De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein worden gesynchroniseerd met één referentietijdbron.	Om een goede analyse van incidenten mogelijk te maken hebben logregels een maximale afwijking van de lokale standaardtijd (UTC) van 500 milliseconden.	BIR-OH

Hoofdstuk 4: Continuïteit

Nr. SURF-audit	ISO-27002:2013	Norm	Maatregel	Bron
4.1	12.1.2	**Wijzigingsbeheer:** Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging worden beheerst.	(O) Instellingen van informatiebeveiligingsfuncties (b.v. security software) op het koppelvlak tussen vertrouwde en onvertrouwde netwerken, worden automatisch op wijzigingen gecontroleerd.	BIR-TNK
			(O) Verantwoordelijkheden voor beheer en wijziging van gegevens en bijbehorende informatiesysteemfuncties moeten eenduidig toegewezen zijn aan één specifieke (beheerders)rol.	BIR-TNK
			(O) Vóór de verwerking van gegevens die de integriteit van kritieke informatie of kritieke informatie systemen kunnen aantasten worden deze gegevens door een tweede persoon geïnspecteerd en geaccepteerd. Van de acceptatie wordt een log bijgehouden.	BIR-TNK
			1. het *Change Management* proces is ingericht en in gebruik; 2. De organisatie werkt volgens OTAP richtlijnen (Ontwikkeling, Test, Acceptatie en Productie); 3. Projecten houden rekening met aspecten rond	Evidence

			informatiebeveiliging.	
4.2	12.1.4	**Scheiding van ontwikkel-, test- en productieomgevingen** Ontwikkel-, test- en productieomgevingen zijn gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Er zijn minimaal logisch gescheiden systemen voor Ontwikkeling, Test en/of Acceptatie en Productie (OTAP). De systemen en applicaties in deze zones beïnvloeden systemen en applicaties in andere zones niet.	BIR-TNK
			Gebruikers hebben gescheiden gebruiksprofielen voor Ontwikkeling, Test en/of Acceptatie en Productiesystemen om het risico van fouten te verminderen. Het moet duidelijk zichtbaar zijn in welk systeem gewerkt wordt.	BIR-TNK
			(O) Indien er een experimenteer of laboratorium omgeving is, is deze fysiek gescheiden van de productieomgeving.	BIR-TNK
			Het netwerk is minimaal logisch gescheiden van andere niet-relevante netwerken (waaronder Ontwikkel, Test en Acceptatie netwerken).	BIR-OH
			Updates op besturingssystemen worden eerst getest in een testomgeving om te controleren of de juiste werking van de systemen niet wordt beïnvloed.	BIR-OH
4.3	12.2.1.1	**Beheersmaatregelen tegen malware:** Ter bescherming tegen malware zijn beheersmaatregelen voor detectie, preventie en herstel geïmplementeerd.	(O) Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats.	BIR-TNK
			(O) Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag,	BIR-TNK

			(automatisch) plaats.	
			(O) Er zijn maatregelen om verspreiding van virussen tegen te gaan en daarmee schade te beperken (bijv. quarantaine en compartimentering).	BIR-TNK
			(R) Gegevensuitwisseling tussen vertrouwde en onvertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.	BIR-TNK
			(O) Binnenkomende programmatuur (zowel op fysieke media als gedownload) wordt gecontroleerd op ongeautoriseerde wijzigingen indien de leverancier daartoe een checksum of certificaat aanbiedt.	BIR-TNK
			(O) Er zijn, waar mogelijk, voorzieningen om de actualiteit van anti-malware programmatuur op mobiele apparaten te garanderen.	BIR-TNK
			Binnen het netwerk zijn compartimenten gecreëerd die in geval van een besmetting kunnen worden afgeschakeld van de rest van het netwerk (Quarantaine).	BIR-OH
			Netwerkverkeer wordt gecontroleerd op de aanwezigheid van malware.	BIR-OH
			Een reverse proxy controleert op de juiste syntax en format van de informatie aan de hand van de specificaties behorend bij de applicatie en blokkeert ongeldige datastromen.	BIR-OH
			Een Intrusion Detection Systeem detecteert netwerk gebaseerde aanvallen middels signatures, protocol validation en anomaly detection	BIR-OH

			Software updates worden binnen de afgesproken en vastgelegde periode geïnstalleerd.	BIR-OH
			Virus scanners op servers, werkstations en netwerk zijn van verschillende leveranciers en bevatten verschillende engines	BIR-OH
			Het besturingssysteem gebruikt beveiligingssoftware waaronder anti – virussoftware, tools tegen spyware; anti-phishingsoftware, encryptiesoftware en een (alleen centraal) configureerbare lokale firewall.	BIR-OH
			De virus scanner controleert bestanden periodiek (interval vooraf afgesproken en vastgelegd) en op het moment dat ze geopend worden.	BIR-OH
			Voor servers geldt dat periodiek (interval vooraf afgesproken en vastgelegd) wordt gecontroleerd op virussen en andere malware in de bestanden die zijn opgeslagen.	BIR-OH
			Een virusscanner detecteert ongebruikelijk gedrag van applicaties	BIR-OH
			Alle aanvallen op systemen worden gedetecteerd en waar mogelijk ook op systeem niveau tegengehouden.	BIR-OH
4.4	12.2.1.2	**Beheersmaatregelen tegen malware:** Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers omtrent bescherming tegen malware te vergroten.	Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten ten aanzien van het gevaar van virussen en dergelijke, zoals: - periodieke awareness programma's zoals via nieuwsbrieven/flyers; - installatie van beveiligingsprogrammatuur die waarschuwt bij onvertrouwde content; - periodieke bespreking van ICT gedragsregels.	Evidence

4.5	12.3.1.1	**Back-up van informatie:** Regelmatig worden back-up kopieën van informatie, software en systeemafbeeldingen gemaakt.	Voor in ieder geval alle concerninformatie zijn backup-procedures ingericht met een vaste frequentie. Backups worden op ten minste 5 kilometer afstand van de productieomgeving opgeslagen.	Evidence
			Dagelijks wordt een incrementele backup gemaakt van de data.	BIR-OH
			Wekelijks wordt een full backup gemaakt van de data.	BIR-OH
			Dagelijkse backups worden 1 maand bewaard.	BIR-OH
			Wekelijkse backups worden 3 maanden bewaard	BIR-OH
4.6	12.3.1.2	**Back-up van informatie:** Gemaakte back ups worden regelmatig getest conform het back-up beleid.	1. Actueel backupbeleid is aanwezig; 2. Integriteit van backups worden automatisch gecontroleerd na aanmaken; 3. Via periodieke restores worden backups getest.	Evidence
			Iedere 3 maanden wordt er een restore-test uitgevoerd om te controleren of de opgeslagen data ook echt terug gehaald kan worden.	BIR-OH
4.7	12.5.1	**Software installeren op operationele systemen:** Om het op operationele systemen installeren van software te beheersen zijn procedures geïmplementeerd. (wijziging)	installatie van software geschiedt volgens gestandaardiseerde en beschreven procedures	ISO
4.8	12.6.1	**Beheer van technische kwetsbaarheden:** Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt wordt tijdig verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden wordt geëvalueerd en er worden passende maatregelen genomen om het risico dat ermee	(O) Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches worden ingepland bij de eerst volgende onderhoudsronde.	BIR-TNK

		samenhangt aan te pakken.		
			Software updates worden, na een impact analyse, geïnstalleerd binnen de vooraf afgesproken periode.	BIR-OH
			Als kritisch getypeerde updates/patches die van een vertrouwde en geautoriseerde bron komen worden, na een impact analyse, op zo kort mogelijke termijn geïnstalleerd.	BIR-OH
			Malware patterns/signatures die van een vertrouwde bron en geautoriseerde komen worden (na beoordeling en impact analyse) op zo kort mogelijke termijn toegevoegd.	BIR-OH
			Updates op besturingssystemen worden eerst getest in een testomgeving om te controleren of de juiste werking van de systemen niet wordt beïnvloed.	BIR-OH
			Security updates en patches worden, na impact analyse, op zo kort mogelijke termijn ingevoerd op de productieomgeving.	BIR-OH
			Updates voor applicaties moeten eerst worden getest om te controleren of de juiste werking van de systemen niet wordt beïnvloed.	BIR-OH
4.9	12.6.2	**Beperkingen voor het installeren van software:** Voor het door gebruikers installeren van software zijn regels vastgesteld en geïmplementeerd.		ISO

4.10	14.2.6	**Beveiligde ontwikkelomgeving:** Organisaties stellen beveiligde ontwikkelomgevingen vast en beveiligen deze passend voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Met betrekking tot de gehele levenscyclus van systeemontwikkeling en integratie stellen organisaties beveiligde OTAP omgevingen vast en beveiligen deze passend.	Evidence
			Richtlijnen en procedures voor het beheer en de beveiliging van testgegevens zijn schriftelijk vastgelegd. Testen met persoonsgevens worden alleen gedaan als deze zijn gefingeerd of adequaat geanonimiseerd.	UMCcloud
4.11	15.2.2	**Beheer van veranderingen in dienstverlening van leveranciers:** Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Veranderingen in de dienstverlening van leveranciers worden beheerd en contractueel vastgelegd.	ISO
4.12	16.1.4	**Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen:** Informatiebeveiligingsgebeurtenissen worden beoordeeld en er wordt geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Het indicent management proces is ingericht en in gebruik.	Evidence
4.13	16.1.5	**Respons op informatiebeveiligingsincidenten:** Op informatiebeveiligingsincidenten wordt gereageerd in overeenstemming met de gedocumenteerde procedures.	1. Het indicent management proces ingericht en in gebruik; 2. Managementverantwoordelijkheden zijn vastgelegd en gecommuniceerd.	Evidence
4.14	17.1.2	**Informatiebeveiligingscontinuïteit implementeren:** De organisatie heeft processen, procedures en beheersmaatregelen vastgesteld, gedocumenteerd en geïmplementeerd om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een	1. Actueel continuiteits- en calamiteitenplan is aanwezig; 2. Escalatiekanalen zijn bepaald en gecommuniceerd; 3. Verantwoordelijkheiden zijn vastgelegd en gecommuniceerd; 4. Verschillende typen calamiteitenoefening worden periodiek	Evidence

		ongunstige situatie te waarborgen en handhaaft deze.	uitgevoerd.	
			(O) Er worden beperkingen opgelegd aan gebruikers en systemen ten aanzien van het gebruik van gemeenschappelijke middelen, zodat een enkele gebruiker (of systeem) niet meer van deze middelen kan opeisen dan nodig is voor de uitvoering van zijn of haar taak en daarmee de beschikbaarheid van systemen voor andere gebruikers (of systemen) in gevaar kan brengen.	BIR-TNK
			(O) In koppelpunten met externe of onvertrouwde zones worden maatregelen getroffen om (D)DOS ((Distributed) Denial of Service attacks) aanvallen te signaleren en hierop te reageren. Het gaat hier om aanvallen die erop gericht zijn de verwerkingscapaciteit zodanig te laten vollopen, dat onbereikbaarheid of uitval van computers het gevolg is.	BIR-TNK
			(O) Calamiteitenplannen worden gebruikt in de jaarlijkse bewustwording-, training- en testactiviteiten.	BIR-TNK
			(O) Er worden minimaal jaarlijks oefeningen en testen gehouden om de bedrijfscontinuïteitsplannen en mate van readiness van de organisatie te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.	BIR-TNK
			Er zijn beschikbaarheidseisen gedefinieerd en vastgelegd.	BIR-OH
			Bij redundantie kan er zodanig overgeschakeld worden naar het redundante systeem (hardware + software/applicatie) dat de vereiste beschikbaarheid wordt behaald	BIR-OH

			Een koppelvlak heeft een vooraf afgesproken en vastgelegde beschikbaarheid.	BIR-OH
4.15	17.2.1	**Beschikbaarheid van informatie verwerkende faciliteiten:** Informatieverwerkende faciliteiten worden met voldoende redundantie geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	BIR-TNK

Hoofdstuk 5: Vertrouwelijkheid en integriteit

Nr. SURF-audit	ISO-27002:2013	Norm	Maatregel	Bron
5.1	9.1.1	**Beleid voor toegangsbeveiliging:** Een beleid voor toegangsbeveiliging is vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Op bedrijfs- en beveiligingseisen gebaseerd beleid voor (logische) toegangsbeveiliging is vastgesteld, gedocumenteerd en beoordeeld.	Evidence
			Applicaties en gebruikers op werkplekken krijgen niet meer rechten dan noodzakelijk is voor de uitvoering.	BIR-OH
5.2	9.1.2	**Toegang tot netwerken en netwerkdiensten:** Gebruikers krijgen alleen toegang tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	(O) Alleen geïdentificeerde en geauthenticeerde apparatuur kan worden aangesloten op een vertrouwde zone. Eigen, ongeauthenticeerde, apparatuur (Bring Your Own Device) wordt alleen aangesloten op een onvertrouwde zone.	BIR-TNK
5.3	9.2.1	**Registratie en afmelden van gebruikers:** Een formele registratie- en afmeldingsprocedure is geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	ISO

			(O) Wachtwoorden voor kritische applicaties hebben een geldigheidsduur van maximaal 3 maanden. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.	BIR-TNK
			(O) Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd.	BIR-TNK
			Extern bereikbare services draaien nooit onder een system/root/admin account, maar altijd onder een account met minimale privileges nodig voor de service.	BIR-OH
			Elke identiteit (persoon of object, b.v. een server) heeft een unieke gebruikersnaam/identifier.	BIR-OH
			Gebruikers moeten zich minimaal op basis van gebruikersnaam en wachtwoord authenticeren.	BIR-OH
			Account met kritische rechten (zoals beheeraccounts) die een vooraf bepaalde periode niet worden gebruikt, worden geblokkeerd. Overige accounts die een vooraf afgesproken periode niet worden gebruikt, worden onderzocht om te bepalen of het account verwijderd kan worden.	BIR-OH
			De expiratiedatum van een account is gekoppeld aan het moment dat de relatie van de gebruiker met de organisatie eindigt.	BIR-OH
			Iedere gebruiker meldt zich aan op het netwerk met een unieke identiteit	BIR-OH

			Bij uitbesteding aan een cloudleverancier wordt het Juridisch normenkader van SURF toegepast. Daardoor worden de volgende richtlijnen en procedures voor toegangsbeheersing van clouddienst geregeld: - registratie van interne en externe gebruikers, inclusief de uitgegeven bevoegdheden - formele en schriftelijke toestemming van de gebruikers voorafgaande aan het gebruik van Clouddienst en de inhoud hiervan, bijv. door de gedwongen acceptatie van de relevante voorwaarden op het moment van de registratie als een gebruiker van Clouddienst - uitgifte, wijziging en inname van inlognaam en wachtwoord - periodieke controle van uitgegeven autorisaties.	UMCcloud
			Wachtwoorden hebben de volgende eigenschappen: - minimale lengte 8 karakters - combinatie van cijfers, letters en minimaal één speciaal karakter - wijzigingsfrequentie maximaal één jaar (voor kritische applicaties maximaal 3 maanden) - blokkeren van de toegang, na vijf verkeerde inlogpogingen - resetten van geblokkeerde accounts.	UMCcloud
5.4	9.2.2	**Gebruikers toegang verlenen:** Een formele gebruikerstoegangsverleningsprocedure is geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	(O) Authenticatiegegevens worden bijgehouden in één bronbestand zodat consistentie is gegarandeerd.	BIR-TNK
			(O) Op basis van een risicoafweging wordt bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	BIR-TNK
			Een identiteit mag alleen de rechten bezitten die nodig zijn voor het uitvoeren van een bepaalde taak. Voorbeelden zijn lees- en	BIR-OH

			schrijfrechten, toegangsrechten.	
			Autorisatie van gebruikers vindt plaats met onderscheid naar rechten voor lezen, toevoegen, wijzigen en verwijderen van gegevens.	UMCcloud
			Gebruikers van systemen voor samenwerking hebben inzicht in wie toegang hebben tot gemeenschappelijke folders en mappen.	UMCcloud
5.5	9.2.3	**Beheren van speciale toegangsrechten:** De toewijzing en het gebruik van speciale bevoegdheden zijn beperkt en worden beheerst.	(O) Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerswerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.	BIR-TNK
			(O) Applicaties mogen niet onnodig en niet langer dan noodzakelijk onder een systeemaccount (een privileged user zoals adminstrator of root) draaien. Direct na het uitvoeren van handelingen waar hogere rechten voor nodig zijn, wordt weer teruggeschakeld naar het niveau van een gewone gebruiker (een unprivileged user).	BIR-TNK
			Er zijn gescheiden, persoonsgebonden, accounts voor beheer- en gebruikerstaken.	BIR-OH
			Toegang tot de BIOS/Firmware is voorzien van een wachtwoord	BIR-OH
			Gebruikers kunnen niet ongeautoriseerd lokale administrator rechten verkrijgen.	BIR-OH
			De op de werkplek aangeboden applicaties hebben geen hoge of systeemrechten nodig om op de werkplek te functioneren. Deze kunnen dus met de standaard gebruikersrechten functioneren.	BIR-OH

			De systeemprocessen draaien onder een eigen account.	BIR-OH
			Het is mogelijk om de rechten per identiteit of per rol te specificeren (Discretionary access control of role based access control) of de criteria waaraan de identiteit moet voldoen om toegang tot de applicatie te krijgen (attribute based access control of claims based access control).	BIR-OH
			Er zijn gescheiden, persoonsgebonden, accounts voor beheer- en gebruikerstaken.	BIR-OH
5.6	9.2.4	**Beheer van geheime authenticatie-informatie van gebruikers:** Het toewijzen van geheime authenticatie-informatie wordt beheerst via een formeel beheersproces.	Wachtwoorden worden eenzijdig vercijferd opgeslagen.	BIR-OH
			Wachtwoorden, en bij voorkeur ook gebruikersnamen, worden altijd vercijferd verzonden.	BIR-OH
			Er wordt gebruik gemaakt van moderne standaards voor het vercijfereren van wachtwoorden.	BIR-OH
5.7	9.3.1	**Geheime authenticatie-informatie gebruiken:** Van gebruikers wordt verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	1. Er is wachtwoordbeleid en dat wordt uitgedragen. Bijvoorbeeld via een nieuwsbrief, flyers of campagnes met betrekking tot goede beveiligingsgewoontes en gebruik van wachtwoorden; 2. Het wachtwoordbeleid is ingeregeld in applicaties en systemen (eisen aan het wachtwoord).	Evidence
			Het is met gebruikersaccounts niet mogelijk automatisch in te loggen (anders dan nodig voor Single Sign On). Alleen systeemprocessen met functionele accounts mogen geautomatiseerd aanloggen.	BIR-OH

			Het is een natuurlijke persoon niet toegestaan om automatisch in te loggen. Alleen batch- en soortgelijke systeemprocessen is het onder vooraf vastgestelde criteria toegestaan automatisch in te loggen.	BIR-OH
			Automatisch onder een gebruikersaccount inloggen na het opstarten is niet toegestaan. (Single sign on is wel mogelijk, deze eis geldt alleen voor initiële werkplekauthenticatie)	BIR-OH
5.8	9.4.1	**Beperking toegang tot informatie:** Toegang tot informatie en systeemfuncties van toepassingen is beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	1. Middels een risicoanalyse houdt de organisatie rekening met het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten 2. Er zijn maatregelen getroffen die de authenticiteit en integriteit van berichten garanderen.	Evidence
			(O) Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.	BIR-TNK
			(O) Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.	BIR-TNK
			(O) Een beheerder gebruikt two-factor authenticatie voor het beheer van kritische apparaten. B.v. een sleutel tot beveiligde ruimte en een password of een token en een password.	BIR-TNK
			Om lokaal data op te slaan is een aparte partitie beschikbaar. De partitie waar het besturingssyteem op staat is niet door de gebruiker aan te passen.	BIR-OH
			Alle ingevoerde gegevens worden gecontroleerd op juistheid en geldigheid, zodat foutieve invoer tot een minimum wordt beperkt. Ongeldige invoer wordt niet geaccepteerd.	BIR-OH

			Indien dubbele invoer tot inconsistentie kan leiden (niet idempotente berichten) wordt er gecontroleerd op dubbele invoer van gegevens. Bij detectie wordt de gebruiker gewaarschuwd.	BIR-OH
			Een applicatie biedt geen mogelijkheid voor gebruikers tot het versturen van spamberichten.	BIR-OH
			Als bepaalde informatie op meerdere plaatsen wordt bijgehouden, wordt periodiek (interval vooraf afgesproken en vastgelegd) gecontroleerd of de informatie consistent is.	BIR-OH
			Applicaties maken gebruik van gebruikersauthenticatie om te voorkomen dat ongeautoriseerde personen toegang hebben tot de applicatie.	BIR-OH
			Waar mogelijk worden prepared statements gebruikt voor queries.	BIR-OH
			Waar mogelijk wordt de zender van de data geverifieerd (whitelisting)	BIR-OH
			Bij werken op afstand is 2-factor authenticatie vereist, in combinatie met een veilige toegangsmethode.	BIR-OH
			Ongeautoriseerde toegang tot het netwerk is niet mogelijk.	BIR-OH
5.9	9.4.2	**Beveiligde inlogprocedures:** Indien het beleid voor toegangsbeveiliging dit vereist, wordt toegang tot systemen en toepassingen beheerst door een beveiligde inlogprocedure.	(O) Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie.	BIR-TNK
			(O) Nadat voor een gebruikersnaam 5 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lockout periode ingesteld kan worden, dan wordt het	BIR-TNK

			account geblokkeerd totdat de gebruiker verzoekt deze lockout op te heffen of het wachtwoord te resetten.	
			Systeem- en netwerkbeheer en functioneel beheer accounts worden altijd geauthenticeerd door middel van 2-factor authenticatie.	BIR-OH
			Initiële wachtwoorden voldoen aan vooraf gestelde criteria (voor format en geldigheidsduur) en mogen eenmalig, uniek per gebruiker, gebruikt worden.	BIR-OH
			Wanneer een inlogingpoging een vooraf afgesproken aantal malen mislukt, wordt het account voor een vooraf afgesproken periode geblokkeerd. Betreft het een beheeraccount, dan wordt dat account geblokkeerd en pas na verificatie van rechtmatigheid handmatig gereset.	BIR-OH
			Een wachtwoord mag niet getoond worden.	BIR-OH
			Bij het login scherm wordt een melding getoond waarin genoemd wordt dat ongeautoriseerd inloggen en misbruik strafbaar is.	BIR-OH
			Het tonen van het laatst ingelogde account is niet toegestaan.	BIR-OH
			De beveiligingsmiddelen die worden ingezet voor de toegangsbeveiliging (o.a. sleutels, codes, biometrie en smartcards) dienen: - vrij te zijn van bekende zwaktes dan wel dienen er aanvullende maatregelen te worden getroffen zodat bekende zwaktes niet misbruikt kunnen worden. - waarborgen te bieden tegen ongeautoriseerd kopiëren - alleen overhandigd te worden aan geregistreerde personen - geheime sleutels worden alleen op veilige media opgeslagen bij	BIR-OH

			de CA.	
			Gebruikers krijgen na een succesvolle login te zien wanneer ze daarvoor ingelogd zijn geweest.	UMCcloud
5.10	10.1.2.1	**Sleutelbeheer:** Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels tijdens hun gehele levenscyclus is een beleid ontwikkeld en geïmplementeerd.	Er bestaan vaste procedures die creatie, opslag, distributie, gebruik, archivering en vernieiting van cryptografische sleutels weergeven en beschrijven.	Evidence
5.11	10.1.2.2	**Sleutelbeheer:** Er wordt gebruik gemaakt van tools om cryptografische sleutels tijdens hun gehele levenscyclus adequaat te beheren.	Tools voor creatie, opslag, distributie, gebruik, archivering en vernieiting van cryptografische sleutels zijn geïnstalleerd en in gebruik.	Evidence
5.12	12.4.2	**Beschermen van informatie in logbestanden:** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Aanpassingen in de logging worden op een separaat systeem gelogd worden om fraude te detecteren.	BIR-OH
			De integriteit van logbestanden moet worden gewaarborgd, schrijftoegang moet zoveel mogelijk worden beperkt (write-once).	BIR-OH
			Logging informatie mag alleen door geautoriseerde personen benaderd worden.	BIR-OH
			Alleen geautoriseerde systemen kunnen in de centrale log-database schrijven.	BIR-OH
			Het overschrijven of verwijderen van logbestanden wordt in het	BIR-OH

			nieuwe logbestand gelogd.	
5.13	13.1.1	**Beheersmaatregelen voor netwerken:** Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	(O) De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze staan. Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.	BIR-TNK
			(O) Elke zone heeft een gedefinieerd beveiligingsniveau zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.	BIR-TNK
			(O) Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.	BIR-TNK
			Informatie over de datastromen is alleen inzichtelijk voor geautoriseerde personen en informatiebeveiligers.	BIR-OH
			Zones kunnen worden onderscheiden door gebruikmaking van routering van datastromen, verificatie van de bron- en de bestemmingsadressen, door toepassing van verschillende protocollen, encryptietechnologie, partitionering of virtualisatie van servers, maar ook door fysieke scheiding.	NORA
5.14	13.1.2	**Beveiliging van netwerkdiensten:** Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten zijn geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor	Er zijn beschikbaarheidseisen gedefinieerd en vastgelegd.	BIR-OH

		diensten die intern worden geleverd als voor uitbestede diensten.		
			Kritische netwerkdiensten en webapplicaties zijn beschikbaar zoals gedefinieerd vooraf afgesproken en vastgelegd.	BIR-OH
			Alle systemen binnen de DMZ zijn ‘gehardened’ waarbij rekening gehouden is met het hogere dreigingsprofiel.	BIR-OH
5.15	13.1.3	**Scheiding in netwerken:** Groepen van informatiediensten, -gebruikers en -systemen zijn op netwerken gescheiden.	(O) Gevoelige systemen (met hoge beschikbaarheid of grote vertrouwelijkheid) behoren een eigen vast toegewezen (geïsoleerde) computeromgeving te hebben. Isoleren kan worden bereikt door fysieke of logische methoden.	BIR-TNK
			Het koppelvlak [met niet vertrouwde netwerken] heeft een default deny policy (voor netwerkpoorten) en alleen geautoriseerd dataverkeer is toegestaan.	BIR-OH
			Rechtstreekse verbinding tussen systemen binnen het productie netwerk en systemen in het onvertrouwde netwerk worden voorkomen.	BIR-OH
			Per risicoklasse is vastgesteld of, en welke, mobiele datadragers worden toegestaan. Toegang tot gegevensbronnen wordt technisch (onafhankelijk van de locatie) afgedwongen.	BIR-OH
			Het is niet mogelijk om verschillende netwerken via de werkplek te verbinden.	BIR-OH
			Alle netwerk multifunctionals worden logisch afgeschermd van de werkstations.	BIR-OH

			Netwerk multifunctionals worden logisch afgeschermd van systemen waarmee geen communicatie nodig is.	BIR-OH
			Er worden geen vertrouwde netwerken met onvertrouwde netwerken worden gekoppeld via de op de multifunctional aangesloten apparatuur (bijvoorbeeld fax).	BIR-OH
			Op de netwerkcomponenten voor het draadloze netwerk draaien geen overbodige diensten.	BIR-OH
			Draadloze netwerken voor verschillende doeleinden zijn minimaal logisch van elkaar gescheiden.	BIR-OH
			De DMZ is ontkoppeld van het onvertrouwde netwerk door toepassing van het patroon “Beveiligd koppelvlak voor onvertrouwde netwerken”.	BIR-OH
			De DMZ is ontkoppeld van het interne netwerk door minimaal toepassing van het patroon “Beveiligd koppelvlak voor vertrouwde netwerken”.	BIR-OH
			Het netwerk van de DMZ is fysieke gescheiden van andere netwerken.	BIR-OH
			Externe routers en firewalls zijn als volgt geconfigureerd: - gebruik van één toegangspunt (‘chokepoint’) - volgens standaarden van de leverancier(s) en algemeen geaccepteerde regels - gebruik makend van redundantie (‘Defense in Depth’) - met gebruik van verschillende soorten van beveiligingsmiddelen (‘Diversity of Defense’) - wanneer een beveiligingsmiddel faalt mag geen toegang worden verleend (‘Failure Mode’)	UMCcloud

			- met gebruik van ‘statefull inspection’. Er is een limitatief overzicht van toegestane routeringen van en naar zones (IP ranges), en daarbij toegestane protocollen en poorten. Alle niet expliciet toegestane verkeersstromen zijn geblokkeerd (deny all). Er wordt gebruik gemaakt van NAT en beveiligingsmaatregelen tegen DNS spoofing en zone transfers zijn genomen.	
5.16	13.2.3	**Elektronische berichten**: Informatie die is opgenomen in elektronische berichten wordt passend beschermd.	Bij computer-computercommunicatie dienen de geheime sleutels op de communicerende machines te worden bewaard maar dan moeten aantoonbare voldoende fysieke en logische beveiligingsmaatregelen zijn toegepast.	BIR-OH
			De middelen voor de externe gegevensuitwisseling hebben de volgende eigenschappen: - standaard bevestiging van verzending en van ontvangst - middelen voor de waarborging van de integriteit en vertrouwelijkheid van het berichtenverkeer met gebruik van versleuteling (minimaal 1024 bits en gebruik van een sterk algoritme). - middelen voor onweerlegbaarheid (‘non-repudiation’).	UMCcloud
5.17	14.1.3	**Transacties van toepassingen beschermen:** Informatie die deel uitmaakt van transacties van toepassingen wordt beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	1. Middels een risicoanalyse houdt de organisatie rekening met het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten 2. Er zijn maatregelen getroffen die de authenticiteit en integriteit van berichten garanderen.	Evidence
			1. Communicatie tussen partijen is met protocollen beveiligd; 2. Certificaten, zoals digitale handtekeningen voor gebruikers, zijn in gebruik om de echtheid van partijen te bewijzen.	Evidence

			Het is mogelijk om [met voldoende sterke encryptie] versleutelde informatie over het netwerk te versturen	BIR-OH
			Berichten, die van derden zijn ontvangen en naar derden zijn verzonden, worden minimaal gebufferd totdat er voldoende zekerheid is over de integere verwerking.	NORA
			De omgeving maakt gebruik van https en is voorzien van een officieel certificaat met organisatie validatie, check op adres, KvK gegevens e.d.	UMCcloud
			De middelen voor de externe gegevensuitwisseling hebben de volgende eigenschappen: - standaard bevestiging van verzending en van ontvangst - middelen voor de waarborging van de integriteit en vertrouwelijkheid van het berichtenverkeer met gebruik van versleuteling (minimaal 1024 bits en gebruik van een sterk algoritme). middelen voor onweerlegbaarheid (‘non-repudiation’).	UMCcloud

Hoofdstuk 6: Controle en logging

Nr. SURF-audit	ISO-27002:2013	Norm	Maatregel	Bron
6.1	9.2.5	**Beoordeling van toegangsrechten van gebruikers:** Eigenaren van bedrijfsmiddelen beoordelen toegangsrechten van gebruikers regelmatig.	Eigenaren van bedrijfsmiddelen beoordelen periodiek, conform vastgesteld beleid, de toegangsrechten van gebruikers.	Evidence
6.2	12.4.1	**Gebeurtenissen registreren:** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, worden gemaakt, bewaard en regelmatig beoordeeld.	Een logregel moet de volgende informatie bevatten: - Datum, tijdstip en tijdzone, minimaal tot op secondeniveau - gebruikersnaam/identificatie - werkstation/locatie informatie - activiteit/gebeurtenis (zie 10.10.2.1) - het object waarop de activiteit werd uitgevoerd - indien relevant, het resultaat van de activiteit	BIR-OH
			(O) In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, enz.).	BIR-TNK

(O) Logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren aangesloten op een Security Information and Event Management systeem (SIEM15) waarmee meldingen en alarmoproepen aan de beheerorganisatie gegeven worden. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.	BIR-TNK
(O) Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.	BIR-TNK
(O) De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de systeemeigenaar. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.	BIR-TNK
(O) Informatie over de beveiligingsrelevante handelingen van de gebruiker wordt regelmatig nagekeken. De IBF bekijkt maandelijks een samenvatting van de informatie.	BIR-TNK
Informatie over de inkomende en uitgaande datastromen wordt minimaal 3 maanden bewaard (niet de inhoud van de datastroom maar o.a. timestamp, bron IP/poort, doel IP/poort, protocol).	BIR-OH
IDS alerts worden geanalyseerd.	BIR-OH
Informatie over de inkomende en uitgaande datastromen wordt minimaal 3 maanden bewaard (niet de inhoud van de datastroom maar timestamp, bron IP/poort, doel IP/poort, protocol)	BIR-OH
Een virusscanner detecteert ongebruikelijk gedrag van applicaties	BIR-OH

			Applicaties slaan loggegevens op van beveiligings-relevante informatie. Voorbeelden hiervan zijn: gelukte en mislukte login-pogingen, toegang tot data, poging tot uitvoeren van acties waar de gebruiker geen rechten voor heeft en software-crashes.	BIR-OH
			Meldingen over de status van de multifunctional worden doorgestuurd naar beheer.	BIR-OH
			Authenticatie is altijd herleidbaar tot één persoon. Indien groepsaccounts nodig zijn worden aanvullende maatregelen genomen om herleidbaarheid tot één persoon te garanderen.	BIR-OH
			De volgende typen informatie moeten gelogd worden: - authenticatie pogingen (al dan niet succesvol) - gedetecteerde malware (wormen/virussen/spyware e.d.) - toegang tot gedeelde bestanden/informatie - beheeracties van beheerders - storingen in de dienstverlening - significante gebruikershandelingen (zoals mutatie stamgegevens, opstarten batches en betalingen).	BIR-OH
			Logregels hebben een volgnummer en een timestamp, waardoor verwijderde regels gedetecteerd kunnen worden.	BIR-OH
			Beveiligingsinstellingen dienen te worden gemonitord, en wijzigingen van beveiligingsinstellingen gelogd.	BIR-OH
			Wijzigingen in firewall instellingen en firewall acties worden gelogd.	BIR-OH
			Rapportage over logging-informatie met betrekking tot beveiliging wordt periodiek (interval volgens vooraf afgesproken en vastgestelde periode; maandelijks is werkbaar) opgeleverd aan de	BIR-OH

			(Corporate) Information Security Officer.	
			Voor archivering van (centrale) logbestanden dient een hash van het logbestand gemaakt te worden, die apart wordt gearchiveerd.	BIR-OH
			Pogingen voor het verkrijgen van toegang tot de clouddienst worden gelogd. De logfile wordt voor analysedoeleinden bewaard.	UMCcloud
			Clouddienst bevat mogelijkheden voor de logging van activiteiten (invoer van gegevens, opslag van gegevens, verwerking van gegevens, verzending en ontvangst van berichten, autorisatiebeheer, etc.).	UMCcloud
6.3	12.4.3	**Logbestanden van beheerders en operators:** Activiteiten van systeembeheerders en -operators worden vastgelegd en de logbestanden worden beschermd en regelmatig beoordeeld.	Activiteiten van systeemadministrators en systeemoperators worden automatisch vastgelegd in logbestanden. De logbestanden worden periodiek beoordeeld door security officer, leidinggevende of audit organisatie.	Evidence
			Gebruik van lokale administrator rechten is zichtbaar voor geautoriseerde personen.	BIR-OH
6.4	14.2.7	**Uitbestede softwareontwikkeling:** Uitbestede systeemontwikkeling staat onder supervisie van en wordt gemonitord door de organisatie.	1. Spreek met de leverancier de eisen af en leg deze schriftelijk vast; 2. Beoordeel de naleving periodiek en/of laat een onafhankelijke derde de naleving controleren.	Evidence
			Richtlijnen en procedures voor wijzigingsbeheer en versiebeheer zijn schriftelijk vastgelegd.	UMCcloud

6.5	14.2.8	**Testen van systeembeveiliging:** Tijdens ontwikkelactiviteiten wordt de beveiligingsfunctionaliteit getest.	[Cloud]Dienst is ontwikkeld met gebruik van veilig programmeren (zie bijvoorbeeld www.owasp.org, www.ncsc.nl en www.sans.org).	ISO UMCcloud
6.6	14.2.9	**Systeemacceptatietests:** Voor nieuwe informatiesystemen, upgrades en nieuwe versies worden programma's voor het uitvoeren van acceptatietests en gerelateerde criteria vastgesteld.	a) Op alle wijzigingen vindt formele acceptatietest plaats alvorens deze in productie worden genomen; b) Test wordt uitgevoerd door representatieve en deskundige gebruikers; c) Acceptatie vindt plaats op basis van (vooraf) vastgestelde acceptatiecriteria.	Evidence
			(O) Van acceptatietesten wordt een verslag opgesteld.	BIR-TNK
			Er zijn acceptatiecriteria vastgesteld voor het testen van de beveiliging. Dit betreft minimaal OWASP13 of gelijkwaardig.	BIR-TNK
6.7	15.2.1	**Monitoring en beoordeling van dienstverlening van leveranciers:** Organisaties monitoren, beoordelen en auditen regelmatig de dienstverlening van leveranciers.	De Processen Contractmanagement en Service Level Management zijn ingericht.	Evidence
			Het geheel van organisatorische en technische beveiligingsmaatregelen wordt jaarlijks gecontroleerd door een onafhankelijke externe partij.	UMCcloud

6.8	16.1.7	**Verzamelen van bewijsmateriaal:** De organisatie heeft procedures gedefinieerd voor het identificeren, verzamelen,verkrijgen en bewaren van informatie die als bewijs kan dienen en past deze toe.	Voor de belangrijkste bedrijfsprocessen heeft de instelling procedures gedefiniëerd en toegepast voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Evidence
			(O) De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de systeemeigenaar. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.	BIR-TNK
6.9	18.2.2	**Naleving van beveiligingsbeleid en –normen:** De directie beoordeelt regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	1. Beveiligingsbeleid en -normen zijn bekend bij het management; 2. Het management beschikt over de relevante rapportages rondom beveiliging zoals al dan niet automatisch gegenereerde rapportages en complianceverklaringen.	Evidence
			Rapportage over logging-informatie met betrekking tot beveiliging wordt periodiek (interval volgens vooraf afgesproken en vastgestelde periode; maandelijks is werkbaar) opgeleverd aan de (Corporate) Information Security Officer.	BIR-OH
6.10	18.2.3	**Beoordeling van technische naleving:** Informatiesystemen worden regelmatig beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	a) Verantwoordelijkheden voor controles rond informatiebeveiliging zijn in functiebeschrijvingen opgenomen; b) Technische normen en richtlijnen zijn beschikbaar actueel; c) Tools om geautomatiseerd te testen zijn ingericht en actueel; d) Bekwaam personeel dat controles uit kan voeren is beschikbaar.	Evidence
			De Service Provider controleert de beveiliging van de clouddienst op periodieke basis door het (laten) uitvoeren van een penetratietest.	UMCcloud