

Technisch informatiebeveiligingsbeleid

Inhoud

1	Inleiding	3
2	Human resources.....	4
2.1	Basisprincipes	4
2.2	Algemeen.....	4
2.3	Voorafgaand aan het dienstverband	4
2.4	Tijdens het dienstverband	4
2.5	Beëindiging en wijziging van dienstverband.....	5
3	Werken op afstand	5
3.1	Basisprincipes	5
3.2	User endpoint devices	5
3.3	Beheersmaatregelen voor werken op afstand	5
3.4	Installeren van software op operationele systemen	5
3.5	Webfiltering.....	6
4	Informatie & bedrijfsmiddelen	6
4.1	Basisprincipes	6
4.2	Soorten bedrijfsmiddelen	6
4.3	Algemeen.....	6
4.4	Inventarisatie	6
4.5	Classificatie	7
4.6	Behandelen.....	7
4.7	Classificatie labels	7
4.8	Wissen van informatie	7
4.9	Maskeren van gegevens	7
4.10	Voorkomen van gegevenslekken (Data leakage prevention)	8
5	Toegangsbeveiliging	8
5.1	Basisprincipes	8
5.2	Toegangsbeveiliging.....	8
5.2.1	Identificatie	8
5.2.2	Authenticatie	8
5.2.3	Autorisatie	9
5.3	Speciale toegangsrechten.....	9
5.4	Logging.....	9

6	Fysieke beveiliging	9
6.1	Doelstellingen	9
6.2	Beveiligde gebieden.....	9
6.3	Fysieke beveiliging locatie (Amstelveen)	9
6.3.1	Informatie	9
6.3.2	Apparatuur.....	9
6.3.3	Risicoprofiel	10
6.4	Beveiligde zones kantoor Kok Advies (Amstelveen)	10
6.5	Fysieke beveiliging van apparatuur	10
6.5.1	Plaatsen en beschermen van apparatuur	10
6.5.2	Beveiligen van bedrijfsmiddelen buiten het terrein	11
6.5.3	Opslagmedia	11
6.5.4	Nutsvoorzieningen	11
6.5.5	Beveiligen van bekabeling	11
6.5.6	Onderhoud van apparatuur	11
6.5.7	Veilig verwijderen of hergebruiken van apparatuur.....	11
6.6	Monitoren en meten	12
7	Dreigingen & kwetsbaarheden	12
7.1	Basisprincipes	12
7.2	Eisen m.b.t. dreigingen & kwetsbaarheden.....	12
7.3	Uitbesteding	12
7.4	Bescherming tegen kwetsbaarheden op de verschillende omgevingen	12
7.5	Patch management.....	13
8	Monitoring & capaciteitsbeheer.....	13
8.1	Eisen m.b.t. monitoring	13
9	Back-up	13
9.1	Basisprincipes	13
9.2	Eisen voor back-up.....	14
10	Logging.....	14
10.1	Basisprincipes	14
10.2	Eisen voor logbestanden.....	14
10.3	Kloksynchronisatie	15
11	Communicatiebeveiliging & cryptografie	15
11.1	Basisprincipes	15
11.2	Eisen voor communicatiebeveiliging	15
11.2.1	Communicatiebeveiliging per omgeving	15

11.3	Eisen voor cryptografie	16
12	Software development	17
12.1	Basisprincipes	17
12.2	Eisen voor software development	17
12.3	Uitbesteding van software development	17
13	Ontwikkeling van informatieverwerkende faciliteiten	17
13.1	Basisprincipes	17
13.2	Ontwikkeling van informatieverwerkende faciliteiten per omgeving	17
14	Leveranciersrelaties	18
14.1	Basisprincipes	18
14.2	Eisen voor leveranciersrelaties	18
15	Informatiebeveiligingsincidenten	18
15.1	Basisprincipes	18
15.2	Eisen voor informatiebeveiligingsincidenten	18
16	ICT-continuïteit	19
17	Naleving	19
18	Overige	19
18.1	Bedieningsprocedures	19

1 Inleiding

Dit document beschrijft het beleid voor een aantal technische informatiebeveiligingsonderwerpen. In dit beleid wordt veelal globaal onderscheidt gemaakt in vier typen informatieverwerkende faciliteiten, namelijk:

- FinRust applicatie (Azure)
- Lokaal netwerk (kantoor)
- SaaS applicaties
- User endpoint devices

Deze verschillende informatieverwerkende faciliteiten worden hieronder verder toegelicht.

FinRust applicatie (Azure)
De FinRust applicatie draait op de public cloud van Microsoft Azure. Met het oog op informatiebeveiliging is dit de meest kritieke omgeving. De Azure omgeving wordt beheerd door strategisch leverancier Eforah.
Lokaal netwerk (kantoor)
FinRust is grotendeels locatieonafhankelijk. De organisatie maakt gebruik van de kantoorlocatie van Kok Advies in Amstelveen. Er wordt hier gebruik gemaakt van een werkplek met een internetverbinding, vergelijkbaar met thuiswerkplekken.
SaaS applicaties

FinRust maakt op grote schaal gebruik van SaaS applicaties. Dit betreft toepassingen die in de cloud zijn ondergebracht en via een internetverbinding te benaderen zijn. De IT componenten zijn volledig uitbesteed aan de aanbieders van deze SaaS applicaties.

User endpoint devices

User endpoint devices zijn apparaten waarmee gebruikers informatie van FinRust kunnen benaderen die zich bevindt op andere online omgevingen. Voorbeelden van deze user endpoint devices zijn laptops, desktops en smart phones. FinRust verstrekt haar medewerkers geen user endpoint devices. Alle medewerkers maken gebruik van hun eigen user endpoint devices. Deze user endpoint devices moeten wel voldoen aan de eisen uit dit technisch informatiebeveiligingsbeleid.

2 Human resources

2.1 Basisprincipes

- Het voorkomen van informatiebeveiligingsincidenten door onbewuste fouten van welwillende medewerkers.
- Het voorkomen van informatiebeveiligingsincidenten door bewuste fouten van kwaadwillen (of lakse) medewerkers.

2.2 Algemeen

- FinRust hanteert een in- en uit dienst procedure voor respectievelijk nieuwe medewerkers en medewerkers die de organisatie verlaten. Dit borgt dat medewerkers tijdens hun dienstverband toegang hebben tot de juiste informatie, en na hun dienstverband juist geen toegang meer hebben tot informatie van de organisatie. Sinds de overname van FinRust door Blinqx worden steeds meer processen (deels) door Blinqx gedaan. Op HR-gebied betekent dit dat de screening van een nieuwe medewerkers (deels) is uitbesteed aan Validata.

2.3 Voorafgaand aan het dienstverband

- FinRust hanteert de volgende eisen voor het screenen van nieuwe medewerkers:
 - Interviews
 - Verificatie van de persoonlijke identiteit
 - Verificatie van diploma's
 - Verificatie van referenties
 - Verklaring Omtrent het Gedrag (VOG)
- FinRust heeft een arbeidsovereenkomst met haar medewerkers die minimaal de volgende componenten bevat:
 - Verwijzing naar het informatiebeveiligingsbeleid
 - Geheimhouding
- Om alle stappen voorafgaand aan het dienstverband te borgen hanteert de organisatie een in dienst check list.

2.4 Tijdens het dienstverband

- De directie is verantwoordelijk voor het motiveren van werknemers om het beleid, de processen en de procedures m.b.t. informatiebeveiliging na te leven.
- Om het informatiebeveiligingsbewustzijn van de organisatie op een hoog niveau te houden, organiseert FinRust de volgende evenementen:
 - Informatiebeveiliging is standaard onderdeel van de onboarding van nieuwe medewerkers.

- Informatiebeveiliging is integraal onderdeel van de periodieke ISMS meetings.
- Periodieke bewustzijnsessie m.b.t. informatiebeveiliging.

2.5 Beëindiging en wijziging van dienstverband

- Bij beëindiging of wijziging van het dienstverband geldt het volgende:
 - De werknemer moet op de hoogte worden gebracht van de verantwoordelijkheden en plichten die van toepassing blijven.
 - Toegangsrechten moeten worden ingetrokken of aangepast.
 - Mobiele apparaten moeten worden teruggegeven (indien van toepassing).
- Om alle stappen bij beëindiging en wijziging van dienstverband te borgen hanteert de organisatie een uit dienst check list.

3 Werken op afstand

3.1 Basisprincipes

- Veilig werken op user endpoint devices vanaf elke locatie.

3.2 User endpoint devices

Medewerkers van FinRust maken gebruik van hun eigen user endpoint device (BYOD), of krijgen deze aangeleverd vanuit FinRust. Deze user endpoint devices moeten wel voldoen aan de onderstaande eisen.

3.3 Beheersmaatregelen voor werken op afstand

Voor werken op afstand met user endpoint devices (laptops) zijn minimaal de volgende beheersmaatregelen van toepassing:

- Disk encryptie
- Password en/of biometrische bescherming
- Anti-virus (OS native anti-virus)
 - Xprotect voor Mac
 - Defender voor Windows

3.4 Installeren van software op operationele systemen

- Medewerkers van FinRust hebben vrijheid om software te installeren op hun user endpoint devices.
- Medewerkers worden, middels het bewustzijnsprogramma, gemotiveerd om zorgvuldig om te gaan met het installeren van software op user endpoint devices.
- Medewerkers worden, middels het bewustzijnsprogramma, gemotiveerd om informatie m.b.t. bedrijfsvoering niet op te slaan op hun user endpoint devices.
- Met behulp van anti-virus software wordt geborgd dat eventuele malware wordt herkend op user endpoint devices.
- In de praktijk gebruiken medewerkers voor hun werkzaamheden vrijwel uitsluitend SaaS applicaties. In de praktijk wordt relatief weinig software geïnstalleerd op de user endpoint devices naast de gerenommeerde software, zoals Microsoft Office, Adobe Reader, enz.
- De online omgevingen waar informatie m.b.t. de bedrijfsvoering staat, zijn dusdanig beveiligd dat het risico op infectie door user endpoint devices met kwaadaardige software wordt beperkt.

3.5 Webfiltering

- Medewerkers worden, middels het bewustzijnsprogramma, gemotiveerd om zorgvuldig om te gaan met het bezoeken en downloaden van informatie op het internet.
- In Xprotect en Microsoft Defender zit voldoende functionaliteit om infectie door het bezoek aan kwaadaardige websites te voorkomen. FinRust heeft besloten dat er geen aanvullende technische maatregelen noodzakelijk zijn.

4 Informatie & bedrijfsmiddelen

4.1 Basisprincipes

- Bedrijfsmiddelen worden passend beveiligd o.b.v. de informatie die ermee wordt verwerkt.
- Informatie wordt eenduidig behandeld o.b.v. de betreffende classificatie.
- 'Blind spots' in de inventarisatie van bedrijfsmiddelen worden voorkomen.

4.2 Soorten bedrijfsmiddelen

In relatie tot informatiebeveiliging onderscheidt FinRust de onderstaande categorieën informatie en daaraan gerelateerde bedrijfsmiddelen.

Categorie	Beschrijving
Informatie	Alles dat informatie is.
Software	Alle applicaties die informatie verwerken.
Hardware	Alle fysieke apparatuur waar informatie staat opgeslagen.
Services	Alle diensten die worden gebruikt voor de verwerking van informatie.
Gebieden	Overal waar informatie fysiek is ondergebracht.

4.3 Algemeen

- Voor het inventariseren, classificeren, labelen en behandelen van informatie wordt een vaste procedure gevolgd.

4.4 Inventarisatie

FinRust onderscheidt twee soorten overzichten voor het vastleggen van bedrijfsmiddelen die gerelateerd zijn aan informatie

Overzicht	Beschrijving
Inventaris van bedrijfsmiddelen	<p>De inventaris van alle soorten informatie en daaraan gerelateerde bedrijfsmiddelen op een hoog niveau.</p> <p><i>Voorbeelden: Persoonsgegevens van klanten, salarisgegevens van medewerkers, laptops in het algemeen, file servers in het algemeen, database servers in het algemeen, applicaties, etc.</i></p>
CMDB	<p>In een CMDB staan alle individuele bedrijfsmiddelen geregistreerd.</p> <p>Informatie en gerelateerde bedrijfsmiddelen m.b.t. de primaire dienstverlening is grotendeels ondergebracht bij strategische leveranciers.</p> <p>User endpoint devices zijn grotendeels eigendom van de medewerkers zelf. Deze apparaten bevatten lokaal geen</p>

	<p>informatie uit het primaire proces. Ze worden uitsluitend gebruikt om informatie te benaderen die is ondergebracht op de daarvoor bedoelde online omgevingen.</p> <p>Omdat FinRust zelf geen bedrijfsmiddelen beheert die informatie uit het primaire proces verwerken, is er voor gekozen om geen CMDB op te stellen.</p>
--	---

4.5 Classificatie

- Alle soorten informatie en gerelateerde bedrijfsmiddelen worden door de eigenaar beoordeeld op beschikbaarheid (B), integriteit (I) en vertrouwelijkheid (V). Deze beoordeling leidt tot een score voor B, I & V, waarvan het resultaat wordt geregistreerd in de inventaris.
- De criteria voor het beoordelen van de beschikbaarheid, integriteit en vertrouwelijkheid wordt vooraf vastgesteld.

4.6 Behandelen

- De wijze waarop informatie behandeld moet worden (o.b.v. de bijbehorende classificatie) is beschreven in het overzicht behandelen van informatie.
- Medewerkers worden bewust gemaakt van de wijze waarop ze, in lijn met het betreffende overzicht, met informatie moeten omgaan.
- De regels, die beschrijven hoe om te gaan met informatie, samen met de vele beheersmaatregelen die technisch zijn afgedwongen, moeten borgen dat gegevenslekken worden voorkomen.

4.7 Classificatie labels

- De gedefinieerde classificatie labels worden toegekend o.b.v. de BIV scores. Deze BIV scores zijn daarmee de onderbouwing voor de gekozen classificatie labels.
- Classificatie labels wordt (waar mogelijk) zo veel mogelijk toegepast op het niveau van systemen, applicaties, mappen en (SharePoint) sites.
- Waar het toekennen van classificatie labels op dit niveau niet mogelijk is, worden medewerkers bewust gemaakt van de classificatie van de betreffende systemen, applicaties, mappen en (SharePoint) sites.
- Individuele documenten worden uitsluitend gelabeld indien dit wordt vereist in het overzicht m.b.t. de omgang met informatie.

4.8 Wissen van informatie

- Apparatuur die geschikt voor hergebruik wordt gewiped en teruggebracht naar fabrieksinstellingen.
- Informatie op papier wordt vernietigd, zodat het niet meer leesbaar en te reconstrueren is.

4.9 Maskeren van gegevens

- Het maskeren van gegevens is in het primaire proces van FinRust potentieel van toepassing bij de volgende toepassingen:
 - **Het analyseren van problemen met berekeningen in de FinRust applicatie.**
Binnen het analyseproces van problemen met berekeningen worden gegevens geanonimiseerd.
 - **Het analyseren van problemen met brondata in de FinRust applicatie.**
Binnen het analyseproces van problemen met brondata moet deze brondata

opgevraagd worden. Om deze gegevens goed te analyseren is het niet mogelijk om deze te maskeren. Deze gegevens worden tijdelijk opgeslagen binnen de Microsoft 365 omgeving van FinRust. Deze gegevens worden (na afronding van de analyse) met enige regelmaat opgeschoond.

4.10 Voorkomen van gegevenslekken (Data leakage prevention)

- FinRust neemt verschillende maatregelen om gegevenslekken te voorkomen, zoals:
 - Beperking van toegang tot omgevingen met vertrouwelijke gegevens.
 - Encryptie van 'data in rest' en 'data in transit'.
 - Bewustwording van de medewerkers die met vertrouwelijke gegevens omgaan.
 - Regels voor het omgaan met vertrouwelijke gegevens.
 - Patch management om kwetsbaarheden in systemen en applicaties met vertrouwelijke gegevens te voorkomen.
 - Enz.
- FinRust heeft vastgesteld dat er op dit moment geen aanvullende maatregelen nodig zijn m.b.t. het voorkomen van gegevenslekken.

5 Toegangsbeveiliging

5.1 Basisprincipes

- Het voorkomen van ongeautoriseerde toegang tot informatie van FinRust.
- Toegang tot informatie wordt toegekend o.b.v. het need-to-know principe.

5.2 Toegangsbeveiliging

- Fysieke en logische toegangsrechten zijn toegekend op het niveau van individuele medewerkers in overeenstemming met de autorisatiematrix.

5.2.1 Identificatie

- De volledige levenscyclus van identiteiten wordt beheerd met behulp van een passende procedure voor het toekennen, wijzigen en intrekken van de toegangsrechten die aan deze identiteiten zijn gekoppeld.
- Identiteiten zijn herleidbaar naar een individu. Het gebruik van groepsaccounts wordt beperkt tot het strikt noodzakelijke.

5.2.2 Authenticatie

- Multi-factor authenticatie wordt toegepast waar dit technisch mogelijk is.
- Onder andere de volgende authenticatiefactoren worden toegepast:
 - iets dat je weet (bijvoorbeeld een wachtwoord).
 - iets dat je hebt (bijvoorbeeld een mobiele telefoon, hardware token, IP, etc.)
 - iets dat je bent (bijvoorbeeld een vingerafdruk, gezichtsherkenning, etc.)
- Single sign-on wordt voor een gedeelte van de applicaties en systemen afgedwongen.
- Wachtwoorden voldoen aan een minimale complexiteit in overeenstemming met de best practices van Microsoft.
- Wachtwoorden worden uitsluitend beheerd in een password management tool.
- Medewerkers gaan zorgvuldig met authenticatie-informatie om in overeenstemming met het handboek informatiebeveiliging.

5.2.3 Autorisatie

- Fysieke en logische toegangsrechten worden toegekend in overeenstemming met de autorisatiematrix.
- Medewerkers hebben uitsluitend toegang tot persoonlijke gezondheidsinformatie indien zij een directe zorgrelatie hebben met degene die deze persoonlijke gezondheidsinformatie betreft.
- De autorisatiematrix wordt uitsluitend aangepast door de eigenaren van de betreffende systemen en applicaties. Daarbij mogen deze eigenaren uitsluitend de autorisaties van hun eigen systemen en applicaties aanpassen.
- Toegangsrechten worden periodiek gecontroleerd in overeenstemming met de operationele planning.

5.3 Speciale toegangsrechten

- Het toekennen van speciale toegangsrechten wordt beperkt tot het minimum.
- Speciale toegangsrechten worden geregistreerd in de autorisatiematrix.

5.4 Logging

- Informatie m.b.t. inlogpogingen wordt gelogd in overeenstemming met het beleid voor logging.

6 Fysieke beveiliging

6.1 Doelstellingen

- Het beschermen van informatie tegen fysieke risico's

6.2 Beveiligde gebieden

FinRust applicatie (Azure)
Fysieke beveiliging is grotendeels uitbesteed aan Microsoft Azure. Prestaties m.b.t. fysieke beveiliging zijn, waar relevant, onderdeel van de periodieke leveranciersbeoordeling.
Lokaal netwerk (kantoor)
FinRust is grotendeels locatieafhankelijk. De organisatie maakt gebruik van de kantoorlocatie van Kok Advies in Amstelveen. Er wordt hier gebruik gemaakt van een werkplek met een internetverbinding, vergelijkbaar met thuiswerkplekken.
SaaS applicaties
Fysieke beveiliging is grotendeels uitbesteed aan leveranciers van SaaS applicaties. Prestaties m.b.t. fysieke beveiliging zijn, waar relevant, onderdeel van de periodieke leveranciersbeoordeling.
User endpoint devices
N.v.t.

6.3 Fysieke beveiliging locatie (Apeldoorn)

6.3.1 Informatie

- Er wordt zo min mogelijk gewerkt met informatie op papier.
- Alle informatie wordt gedigitaliseerd. Nadat het is gedigitaliseerd, wordt het papier vernietigd.
- Digitale informatie van FinRust bevindt zich op de kantoorlocatie alleen op laptops.

6.3.2 Apparatuur

- Op de kantoorlocatie bevindt zich geen apparatuur m.b.t. de primaire dienstverlening.

- Er wordt alleen gebruik gemaakt van netwerkapparatuur t.b.v. de internetverbinding. Deze netwerkapparatuur valt onder de verantwoordelijkheid van Bonenburg Vastgoed, de verhuurder.

6.3.3 Risicoprofiel

Omdat zich op de kantoorlocatie nauwelijks informatie bevindt (zowel op papier als digitaal) is het risicoprofiel van de kantoorlocatie zeer laag.

6.4 Beveiligde zones kantoor Apeldoorn

Classificatie	Gebieden	Informatie	Beheersmaatregelen
Publiek	Het publieke gebied rondom de kantoorlocatie	<ul style="list-style-type: none"> • Uitsluitend publieke informatie. 	<ul style="list-style-type: none"> • Geen aanvullende maatregelen.
Intern	Kantoorlocatie Apeldoorn	<ul style="list-style-type: none"> • Zo min mogelijk interne informatie op papier. • Uitsluitend interne informatie op laptops van de medewerkers 	<ul style="list-style-type: none"> • Voordeur is tijdens kantooruren open. Er is altijd toezicht door medewerkers van Bonenburg • Lift naar 5e verdieping alleen met tag. Openen kantoordeur met sleutel.
Vertrouwelijk	N.v.t.	<ul style="list-style-type: none"> • Geen vertrouwelijke informatie op kantoorlocatie. Geen afgesloten ruimtes. 	N.v.t.
Zeer vertrouwelijk	N.v.t.	Geen vertrouwelijke informatie op kantoorlocatie. Geen afgesloten ruimtes.	N.v.t.

6.5 Fysieke beveiliging van apparatuur

FinRust beheert, in de context van fysieke beveiliging, zelf geen apparatuur. Dit beheer van apparatuur is grotendeels uitbesteed aan strategische leveranciers. Omdat uitbesteding niet ontslaat van verantwoordelijkheid

6.5.1 Plaatsen en beschermen van apparatuur

Voor de plaatsing en bescherming van apparatuur in datacenters gelden de volgende eisen:

- De apparatuur moet ondergebracht zijn op een veilige locatie in overeenstemming met het beleid passende beveiligingsmaatregelen zoals:
 - Uitsluitend toegang voor geautoriseerde personen.
 - Camerabeveiliging.
 - Systemen zijn ondergebracht in afgesloten racks.
- Er wordt voldaan aan de voorwaarden voor het goed functioneren van de apparatuur, zoals:
 - Temperatuur
 - Luchtvochtigheid

6.5.2 Beveiligen van bedrijfsmiddelen buiten het terrein

Voor de beveiliging van apparatuur die zich buiten de beveiligde (datacenter)locaties bevinden gelden de volgende eisen:

- Situaties waarin apparatuur zich buiten de beveiligde gebieden bevinden, moet zo veel mogelijk beperkt worden.
- De beschikbare lokale informatie op de apparatuur moet beperkt worden tot het strikt noodzakelijke.
- De informatie op de apparatuur moet versleuteld zijn in overeenstemming met het beleid voor cryptografie.

6.5.3 Opslagmedia

Het is niet toegestaan om externe opslagmedia (zoals USB sticks) te gebruiken.

6.5.4 Nutsvoorzieningen

Om uitval en schade aan apparatuur te voorkomen is het belangrijk dat nutsvoorzieningen in datacenters goed geregeld zijn. Hiervoor gelden de volgende eisen:

- De apparatuur is aangesloten op een secundaire energiebron voor het geval dat de primaire energiebron uitvalt. Voorbeelden van een secundaire energiebronnen zijn:
 - UPS;
 - Generator/aggregaat;
 - Secundaire stroomtoevoer (bijvoorbeeld van een tweede energieleverancier).
- De correcte werking van de secundaire energiebron wordt regelmatig getest.

6.5.5 Beveiligen van bekabeling

FinRust maakt bij haar (datacenter)leveranciers voornamelijk gebruik van virtuele machines. Met betrekking tot de fysieke hardware waar die virtuele servers op draaien, moet de leverancier in ieder geval de volgende maatregelen nemen m.b.t. het onderhoud van apparatuur:

- Er is monitoring ingericht om de toestand van de apparatuur in de gaten te houden.
- Apparatuur wordt vervangen, zodra de monitoring criteria daar aanleiding toe geven, en vóórdat de apparatuur storing veroorzaakt.
- Indien het vervangen van apparatuur invloed heeft op de beschikbaarheid van de dienstverlening, dan moet er in overleg met FinRust een onderhoudsvenster ingepland worden.

6.5.6 Onderhoud van apparatuur

FinRust maakt bij haar (datacenter)leveranciers voornamelijk gebruik van virtuele machines. Met betrekking tot de fysieke hardware waar die virtuele servers op draaien, moet de leverancier in ieder geval de volgende maatregelen nemen m.b.t. het onderhoud van apparatuur:

- Er is monitoring ingericht om de toestand van de apparatuur in de gaten te houden.
- Apparatuur wordt vervangen, zodra de monitoring criteria daar aanleiding toe geven, en vóórdat de apparatuur storing veroorzaakt.
- Indien het vervangen van apparatuur invloed heeft op de beschikbaarheid van de dienstverlening, dan moet er in overleg met FinRust een onderhoudsvenster ingepland worden.

6.5.7 Veilig verwijderen of hergebruiken van apparatuur

FinRust heeft geen apparatuur in beheer.

6.6 Monitoren en meten

Er zijn geen periodieke controles m.b.t. dit onderwerp.

7 Dreigingen & kwetsbaarheden

7.1 Basisprincipes

- Het inwinnen van informatie over dreigingen en kwetsbaarheden.
- Het voorkomen van schade uit dreigingen die zich manifesteren via kwetsbaarheden.

7.2 Eisen m.b.t. dreigingen & kwetsbaarheden

- Informatie m.b.t. dreigingen en kwetsbaarheden worden ingewonnen m.b.v. relevante bronnen.
 - FinRust is lid van de branchevereniging Contactgroep Automatisering. Via deze branchevereniging worden de volgende bronnen gebruikt:
 - Nieuwsbrief
 - Cybersecurity
 - Cybersecurity > Beveiligingsadviezen
 - Andere geraadpleegde bronnen zijn:
 - NSCS
 - Security.nl
- Informatie over dreigingen en kwetsbaarheden wordt tijdens de periodieke ISMS meeting geanalyseerd. Waar nodig worden acties in gang gezet.
- Het bewustzijn van medewerkers m.b.t. dreigingen, kwetsbaarheden en malware wordt op een passend niveau gehouden.

7.3 Uitbesteding

- Threat intelligence m.b.t. de primaire dienstverlening is grotendeels uitbesteed aan strategische leveranciers Eforah en Microsoft Azure.

7.4 Bescherming tegen kwetsbaarheden op de verschillende omgevingen

FinRust applicatie (Azure)
<ul style="list-style-type: none"> • Op de Azure omgeving zijn passende maatregelen genomen om de FinRust applicatie te beschermen tegen kwetsbaarheden. • Er worden automatische scans uitgevoerd op kwetsbaarheden in software libraries (m.b.v. Snyk). • Er worden periodieke pentests uitgevoerd op de FinRust applicatie.
Lokaal netwerk (kantoor)
Het lokale netwerk is passend beschermd m.b.v. netwerkbeveiliging. Bescherming tegen kwetsbaarheden (o.a. m.b.v een firewall) is daar onderdeel van.
SaaS applicaties
Bescherming tegen kwetsbaarheden is bij SaaS applicaties integraal onderdeel van dienstverlening. Prestaties m.b.t. de bescherming van kwetsbaarheden van SaaS applicaties is, waar relevant, onderdeel van de periodieke leveranciersbeoordeling.
User endpoint devices
User endpoint devices zijn voorzien van anti-malware software om de apparatuur te beschermen tegen kwetsbaarheden.

7.5 Patch management

Eforah hanteert procedures voor:

- Het update van software bibliotheken
- Het doorvoeren van hot-fixes

Procedure voor het doorvoeren van hot-fixes

1. Aanmaken incident aan bij Eforah (FinRust)
2. Maken inschatting urgentie van het incident (Eforah)
3. Ontwikkelen van de hot-fix (Eforah)
4. Testen hot-fix (FinRust & Eforah)
5. Releasen hot-fix naar productie (Eforah)

8 Monitoring & capaciteitsbeheer

- Het detecteren en voorkomen van potentiële informatiebeveiligingsincidenten.

8.1 Eisen m.b.t. monitoring

Voor de verschillende soorten informatieverwerkende faciliteiten hanteert FinRust de onderstaande eisen voor monitoring en capaciteitsbeheer.

<p>FinRust applicatie (Azure)</p> <ul style="list-style-type: none"> • Monitoring van de FinRust applicaties wordt ingericht o.b.v. (minimaal) de onderstaande componenten: <ul style="list-style-type: none"> ○ Beschikbaarheid ○ Capaciteit o.b.v. de onderstaande componenten <ul style="list-style-type: none"> ▪ Opslag ▪ CPU load ▪ Geheugen • Monitoring is ingericht o.b.v. vooraf gedefinieerde thresholds. • Overschreden thresholds forceren een automatische melding die de opvolging ervan borgt. • Monitoring is ingericht m.b.t. de maximale rekencapaciteit van de SQL database.
<p>Lokaal netwerk (kantoor)</p> <p>Het lokale netwerk op de kantoorlocatie in Apeldoorn is niet meer dan een werkplek met internetverbinding. Er bevindt zich op deze locatie geen kritieke informatie uit het primaire proces. Monitoring en capaciteitsbeheer voor het lokale netwerk daarom niet van toepassing.</p>
<p>SaaS applicaties</p> <p>Monitoring en capaciteitsbeheer is bij SaaS applicaties integraal onderdeel van dienstverlening. Prestaties m.b.t. de back-up van SaaS applicaties is, waar relevant, onderdeel van de periodieke leveranciersbeoordeling.</p>
<p>User endpoint devices</p> <p>Op user end points wordt lokaal geen kritieke informatie uit het primaire proces opgeslagen. User end points zijn makkelijk vervangbaar. Monitoring en capaciteitsbeheer is voor deze apparatuur daarom niet van toepassing.</p>

9 Back-up

9.1 Basisprincipes

- Het voorkomen van (onherstelbaar) verlies van informatie.

9.2 Eisen voor back-up

Voor de verschillende soorten informatieverwerkende faciliteiten hanteert FinRust de onderstaande eisen voor back-up.

FinRust applicatie (Azure)		
Back-up strategie		
Rule	Frequentie	Bewaartermijn
1	< 10 minuten	35 dagen
2	Wekelijks	6 maanden
3	Maandelijks	1 jaar
<ul style="list-style-type: none"> • Recovery Point Objective (RPO): < 15 minuten • Recovery Time Objective (RTO): 24 uur • Back-ups worden encrypted opgeslagen via Transparent Data Encryption (TDE). <ul style="list-style-type: none"> ○ Er wordt gebruik gemaakt van een server level encryption key. ○ Microsoft gebruikt AES-256 (Advanced Encryption Standard) als encryptiemethode voor TDE. • Er sprake van geografische spreiding van de back-ups over meerdere regio's van Microsoft Azure. • Er worden periodieke back-up restore tests uitgevoerd in overeenstemming met de operationele planning. 		
Lokaal netwerk (kantoor)		
Het lokale netwerk op de kantoorlocatie in Amstelveen is niet meer dan een werkplek met internetverbinding. Er bevindt zich op deze locatie geen kritieke informatie uit het primaire proces. Een back-up is voor het lokale netwerk daarom niet van toepassing.		
SaaS applicaties		
Back-up is bij SaaS applicaties integraal onderdeel van dienstverlening. Prestaties m.b.t. de back-up van SaaS applicaties is, waar relevant, onderdeel van de periodieke leveranciersbeoordeling.		
User endpoint devices		
Op user end points wordt lokaal geen kritieke informatie uit het primaire proces opgeslagen. User end points zijn makkelijk vervangbaar. Een back-up is voor deze apparatuur daarom niet van toepassing.		

10 Logging

10.1 Basisprincipes

- De mogelijkheid om gebeurtenissen op informatieverwerkende faciliteiten te onderzoeken.
- Het detecteren van activiteiten waarop vroegtijdig actie ondernomen moet worden (monitoring).

10.2 Eisen voor logbestanden

Voor de verschillende soorten informatieverwerkende faciliteiten hanteert FinRust de onderstaande eisen voor logging.

FinRust applicatie (Azure)
Eisen voor logbestanden
<ul style="list-style-type: none"> • Activiteiten in logbestanden zijn ze veel mogelijk herleidbaar naar een individu. • Logbestanden moeten minimaal de volgende systeemactiviteiten vastleggen: <ul style="list-style-type: none"> ○ Activiteiten m.b.t. inloggen van alle gebruikers.

<ul style="list-style-type: none"> ○ Activiteiten m.b.t. aanpassingen in de database. • Data, tijdstippen en details van relevante gebeurtenissen. • De bewaartermijn van logbestanden is minimaal 90 dagen. <ul style="list-style-type: none"> ○ In de praktijk is dat op dit moment ongelimiteerd. • Logbestanden moeten worden beschermd om ongewenste aanpassing te voorkomen. • Er vindt analyse plaats op logbestanden voor de volgende doeleinden: <ul style="list-style-type: none"> ○ Het blokkeren van een account bij herhaalde foutieve inlogpogingen.
Lokaal netwerk (kantoor)
Het lokale netwerk op de kantoorlocatie in Amstelveen is niet meer dan een werkplek met internetverbinding. Er bevindt zich op deze locatie geen kritieke informatie uit het primaire proces. Logging voor het lokale netwerk is daarom niet van toepassing.
SaaS applicaties
Logging is bij SaaS applicaties integraal onderdeel van dienstverlening. Prestaties m.b.t. logging van SaaS applicaties is, waar relevant, onderdeel van de periodieke leveranciersbeoordeling.
User endpoint devices
Op user end points wordt lokaal geen kritieke informatie uit het primaire proces opgeslagen. User end points worden voornamelijk gebruikt om informatie te benaderen op andere (online) omgevingen. Logbestanden zijn meer relevant voor die betreffende omgevingen.

10.3 Kloksynchronisatie

- Informatiesystemen maken gebruik van dezelfde NTP pool.

11 Communicatiebeveiliging & cryptografie

11.1 Basisprincipes

- Netwerken, en netwerkcomponenten, zijn beveiligd.
- Transport van informatie van het ene naar het andere netwerk is beveiligd.
- Zo veel mogelijk informatie is versleuteld (at rest & in transit).
- Cryptografische sleutels worden zorgvuldig beheerd.

11.2 Eisen voor communicatiebeveiliging

- Netwerken zijn voldoende beveiligd om de integriteit en vertrouwelijkheid van informatie te borgen.
- Netwerken worden voldoende onderhouden om de beschikbaarheid van informatie te borgen.
- Apparatuur die via een netwerk vanaf externe locaties benaderd kunnen worden zijn passend beveiligd.
- Firewalls zijn ingericht o.b.v. het “zero trust” principe.
 - Poorten op firewalls staan dicht, tenzij het voor de functionaliteit noodzakelijk is dat ze open staan.
- Informatie binnen netwerken is beveiligd.
 - Toegang tot netwerken is beveiligd m.b.v toegangsbeveiliging o.b.v het “need-to-know” principe.
- Netwerksegmentatie wordt toegepast waar mogelijk.
- Informatie wordt uitsluitend verzonden over beveiligde, versleutelde verbindingen.

11.2.1 Communicatiebeveiliging per omgeving

Hieronder staat beschreven op welke wijze communicatiebeveiliging is ingericht voor de verschillende soorten informatieverwerkende faciliteiten.

FinRust applicatie (Azure)
De FinRust applicatie bevindt zich in Microsoft Azure. Azure biedt standaard een aantal firewall- en netwerkbeveiligingsoplossingen, zoals Azure Firewall, Application Gateway en Network Security Groups (NSG) die helpen bij het beschermen van de netwerkresources.
Lokaal netwerk (kantoor)
<ul style="list-style-type: none"> Er wordt alleen gebruik gemaakt van netwerkapparatuur t.b.v. de internetverbinding. Deze netwerkapparatuur valt onder de verantwoordelijkheid van Bonenburg.
SaaS applicaties
Communicatiebeveiliging is bij SaaS applicaties integraal onderdeel van dienstverlening. Prestaties m.b.t. communicatiebeveiliging van SaaS applicaties is, waar relevant, onderdeel van de periodieke leveranciersbeoordeling.
User endpoint devices
User endpoint devices spelen binnen het onderwerp communicatiebeveiliging ook een belangrijke rol. De maatregelen die genomen zijn om veilig te kunnen werken met user endpoint devices zijn beschreven in het hoofdstuk werken op afstand.

11.3 Eisen voor cryptografie

De onderstaande tabel laat zien welke vormen van encryptie van toepassing kunnen zijn op de verschillende soorten informatiesystemen en -verwerkers op basis de 'state of data'.

Data at rest	Cryptografische beheersmaatregelen
User end points	Disk/drive encryption
Servers & systemen	Drive encryption
Wachtwoorden van klantomgevingen	Hashing
Data in transit	Cryptografische beheersmaatregelen
Verbindingen	VPN/TLS/SSH
Web transacties	TLS

FinRust hanteert de onderstaande minimale eisen voor cryptografie.

Beheersmaatregelen	Van toepassing op	Methode	Minimale eis
Disk/drive encryptie	Data at rest	AES	256 bits
File encryptie	Data at rest	AES	256 bits
VPN	Data in transit	AES	256 bits
TLS	Data in transit	TLS	1.2
Hashing	Digitale handtekening, opslag van wachtwoorden	Hashing	SHA-2

In het onderstaande overzicht is per informatieverwerkende faciliteit aangegeven

FinRust applicatie (Azure)
De FinRust applicatie bevindt zich in Microsoft Azure. Zowel in rust als tijdens overdracht, worden gegevens in Azure gecodeerd. Azure SQL Database gebruikt bijvoorbeeld Transparent Data Encryption (TDE) om gegevens in rust te beschermen.
Lokaal netwerk (kantoor)
Om vanaf kantoor online omgevingen (zoals Azure en SaaS applicaties) te bereiken worden uitsluitend beveiligde verbindingen gebruikt die voldoen aan de bovenstaande eisen voor cryptografie.
SaaS applicaties

Cryptografie is bij SaaS applicaties integraal onderdeel van dienstverlening. Prestaties m.b.t. cryptografie van SaaS applicaties is, waar relevant, onderdeel van de periodieke leveranciersbeoordeling.

User endpoint devices

Op user endpoint devices die gebruikt worden voor werkzaamheden van FinRust moet drive encryptie actief zijn in overeenstemming met de bovenstaande eisen voor cryptografie.

12 Software development

12.1 Basisprincipes

- Het gecontroleerd brengen van software code van ontwikkeling naar productie.
- Het voorkomen van kwetsbaarheden in software code.

12.2 Eisen voor software development

- Software wordt gecontroleerd van ontwikkeling naar productie gebracht.
- Er wordt een passende ontwikkelomgeving toegepast met de volgende omgevingen:
 - Development (lokaal en/of Azure)
 - Staging (Azure)
 - Pre-productie (Azure)
 - Productie (Azure)
- Het ontwikkelproces bevat passende controlestappen, zoals code reviews.
- Nieuwe of gewijzigde software code wordt getest, voordat deze naar productie wordt gebracht. De volgende tests zijn van toepassing:
 - Geautomatiseerde unit tests (uitgevoerd door Eforah)
 - Handmatige functionele tests (uitgevoerd door FinRust)
- Er worden passende security tests uitgevoerd om kwetsbaarheden in software te voorkomen. De volgende security tests zijn van toepassing:
 - Automatische scans op kwetsbaarheden in software libraries (m.b.v. Snyk).
 - Periodieke pentests op de FinRust applicatie.
- Alle software code wordt veilig opgeslagen in een code repository (Bitbucket).
- Toegang tot de broncode en de FinRust applicatie wordt beperkt tot het strikt noodzakelijk.
- In de staging omgeving wordt geen productiedata gebruikt.

12.3 Uitbesteding van software development

Software development is volledig uitbesteed aan Eforah. De bovenstaande eisen zijn van toepassing op deze ontwikkeling.

13 Ontwikkeling van informatieverwerkende faciliteiten

13.1 Basisprincipes

- Het borgen van informatiebeveiligings gedurende de volledige levenscyclus van informatieverwerkende faciliteiten.

13.2 Ontwikkeling van informatieverwerkende faciliteiten per omgeving

FinRust applicatie (Azure)

De ontwikkeling van informatieverwerkende faciliteiten van de FinRust omgeving is volledig uitbesteed aan de strategische leveranciers Microsoft Azure en Eforah.

Lokaal netwerk (kantoor)

De ontwikkeling van informatieverwerkende faciliteiten van het lokale netwerk valt onder de verantwoordelijkheid van Kok Advies. Kok Advies heeft deze ontwikkeling volledig uitbesteed aan strategisch leverancier Icotec.

SaaS applicaties

De ontwikkeling van informatieverwerkende faciliteiten is bij SaaS applicaties integraal onderdeel van dienstverlening. Prestaties m.b.t. de ontwikkeling van informatieverwerkende faciliteiten van SaaS applicaties is, waar relevant, onderdeel van de periodieke leveranciersbeoordeling.

User endpoint devices

De ontwikkeling van informatieverwerkende faciliteiten is niet van toepassing op user endpoint devices.

14 Leveranciersrelaties

14.1 Basisprincipes

- Het borgen van informatiebeveiligingseisen door de gehele toeleveringsketen.

14.2 Eisen voor leveranciersrelaties

- Relevante eisen voor informatiebeveiliging zijn, waar mogelijk, onderdeel van de overeenkomsten met leveranciers.
- Alle leveranciers die relevant zijn voor informatiebeveiliging zijn gedefinieerd in het leveranciersoverzicht.
- Nieuwe leveranciers moeten voldoen aan de eisen van FinRust. Om dit vast te stellen wordt het leveranciersbeoordelingsformulier gebruikt.
- Leveranciers worden geclassificeerd o.b.v. de informatie die er wordt verwerkt. Deze classificatie wordt gedocumenteerd in het leveranciersoverzicht.
- Alle leveranciers die relevant zijn voor informatiebeveiliging worden periodiek beoordeeld m.b.v. het leveranciersbeoordelingsformulier.
- De frequentie waarin een bepaalde leverancier wordt beoordeeld is vastgelegd in het leveranciersoverzicht. Deze frequentie is gebaseerd op de classificatie van de betreffende leverancier.
- Bevindingen uit de leveranciersbeoordeling worden opgevolgd.

15 Informatiebeveiligingsincidenten

15.1 Basisprincipes

- Het voorkomen van informatiebeveiligingsincidenten¹ die voortkomen uit informatiebeveiligingsgebeurtenissen².
- Het beperken van schade door adequate oplossing van informatiebeveiligingsincidenten.
- Het voorkomen van herhaling van informatiebeveiligingsincidenten.

15.2 Eisen voor informatiebeveiligingsincidenten

- De verwerking van informatiebeveiligingsincidenten vindt plaats in overeenstemming met de procedure voor informatiebeveiligingsincidenten.
- Informatiebeveiligingsincidenten worden centraal geregistreerd.

¹ Een afzonderlijke gebeurtenis of een reeks IB gebeurtenissen waarvan het zeer waarschijnlijk is dat deze de bedrijfsactiviteiten compromitteren en de informatiebeveiliging in gevaar brengen.

² Een voorval dat wijst op een mogelijke inbreuk van informatiebeveiliging, of op het falen van beheersmaatregelen.

16 ICT-continuïteit

- FinRust heeft een ICT-Continuïteitsplan opgesteld.

17 Naleving

- FinRust werkt in overeenstemming met:
 - ISO 27001:2022 norm
 - Informatiebeveiligingsbeleid van FinRust
 - Eisen van belanghebbenden
 - Relevante wet- & regelgeving
- FinRust heeft alle wet- & regelgeving die relevant is voor informatiebeveiliging gedocumenteerd. Hierbij worden minimaal de volgende componenten benoemd:
 - De betreffende wet, regel of standaard.
 - De componenten uit de betreffende wet, regel of standaard die van toepassing zijn.
 - De wijze waarop FinRust de wet, regel of standaard heeft geïmplementeerd.
 - De wijze waarop naleving van de wet, regel of standaard wordt geborgd.

18 Overige

18.1 Bedieningsprocedures

FinRust heeft veel IT componenten uitbesteed. Het opstellen en opvolgen van bedieningsprocedures is daarmee grotendeels de verantwoordelijkheid van de betreffende leveranciers. Met betrekking tot de IT componenten die wel door FinRust zelf beheerd worden, geldt dat de benodigde bedieningsprocedures integraal onderdeel zijn van de betreffende systemen en applicaties. Naast het algemene informatiebeveiligingsbeleid zijn geen aanvullende bedieningsprocedures noodzakelijk.