circet
CREATING TELECOM NETWORKS

CIRCET BELGIUM ICT Policy

circet
CREATING TELECOM NETWORKS

Document Information

Author	Tom Van der Aa	
Distribution Approver **(Needed?: ☒Yes/☐No)**	Name Approver : Luc Vranken **(Approved?: ☒Yes/☐No)**	
Version	V1.7	
Classification	**CONFIDENTIALITY** ☐(1)Public ☒(2)company specific ☐(3)Confidential ☐(4)Secret	
Date last modified	17/04/2026	

Document History

Date	Version	Created By	Description of change	Approved by
15/02/2021	V1.0	Tom Van Der Aa	Created the document	Patrick Block
01/03/2021	V3.0	Sophie Decroix	Reviewed and adapted	Tom Van der Aa
05/03/2021	V5.0	An Huybreghts	Reviewed and adapted	Tom Van der Aa
07/03/2021	V6.0	Valeska Crab (DPO)	Reviewed, adapted and approved	Valeska Crab
21/02/2022	V7.0	Guy Boets	Review 2022	Patrick Block
24/03/2022	V8.0	Tom Van der Aa	Review 2022	Guy Boets
03/05/2023	V9.0	Tom Van der Aa	Review 2023	Tom Van der Aa
16/05/2024	V10.0	Tom Van der Aa	Review 2024	Tom Van der Aa
24/03/2025	V11.0	Guy Boets	Review 2025	Tom Van der Aa
15/04/2025	V12.0	An Huybreghts	Reviewed and adapted	Bart Van Rompaey

17/04/2026	V15.0	Guy Boets	Review + Changes	Luc Vranken
10/06/2026	V16.0	An Huybreghts	Review + 19.4 added	Sophie Decroix

Table of content

1 Definities

"ICT":	Informatie en Communicatie Technologie.
"Externen":	Personen die geen werknemerstatuut hebben bij CIRCET BELGIUM (bv. freelancers, consultants, interimkrachten, …)
"Werknemers":	Arbeider of bediende voor onbepaalde of bepaalde duur in dienst van CIRCET.
"Medewerkers":	Werknemers en externen die voor Circet Belgium werken
"N+1":	Lijnverantwoordelijke van de medewerker
"ICT-Medewerkers":	Medewerkers onderdeel van het ICT en ServiceCruiser departement en deze functie uitoefenen ter ondersteuning van klanten van Circet CIRCET BELGIUM.
"Head of Digitalisation":	CIRCET BELGIUM medewerker die de verantwoordelijkheid draagt aangaande het ICT gebeuren binnen CIRCET BELGIUM.
"ICT Operations Manager":	CIRCET BELGIUM medewerker die de verantwoordelijkheid draagt aangaande het operationeel ICT gebeuren binnen CIRCET BELGIUM.
"ICT-Servicedesk Manager":	CIRCET BELGIUM medewerker die de ICT Operations Manager ondersteunt bij het ICT gebeuren binnen CIRCET BELGIUM.
"ICT-Servicedesk":	Een groep van CIRCET BELGIUM servicedesk medewerkers die instaan voor het onderhoud, de installatie en de configuratie van de ICT binnen CIRCET BELGIUM.
"System-Engineer":	CIRCET BELGIUM medewerker die de ICT Operations manager ondersteunt bij het technische aspect van het ICT gebeuren bij CIRCET BELGIUM.
"Key-gebruiker":	CIRCET BELGIUM medewerker uit de operationele afdelingen die samen met de ICT medewerkers instaat voor de inrichting van de bedrijfsapplicaties

"Smart Devices":	Toestellen waarmee informatie ontvangen, geraadpleegd of aangemaakt kan worden. Bv: laptop, desktop, thin client, smartphone, tablet, etc.
"Company Smart Devices":	intelligente Toestellen die eigendom zijn van CIRCET BELGIUM.
"Private Smart Devices":	Intelligente Toestellen die eigendom zijn van de medewerker, bijvoorbeeld privé pc, privé smartphone.
"Other Smart Devices":	Intelligente Toestellen eigendom van derden, bijvoorbeeld klanten, Internet Cafés, familie, etc.
"Server Based Computing":	Van op afstand werken op een server binnen het bedrijf waarbij enkel input/output (scherm/toetsenbord/muis) van de lokale computer gebruikt wordt, bv. Citrix, Windows Virtual desktop etc.

2 Toepassing en verantwoordelijkheden

Deze policy is van toepassing op volgende Belgische vennootschappen

1. Circet Belgium NV
2. Teletronika NV
3. Circet Infratechniek NV
4. Circet Benelux NV
5. Circet Projects NV

Verder benoemd als '**CIRCET BELGIUM' of het 'Bedrijf'.**

De Policy is van toepassing op alle medewerkers van CIRCET BELGIUM

3 Positionering

3.1 De vier P's

Binnen het ICT gebeuren wordt het beleid of management uitgewerkt en uitgevoerd door de vier P's nl.:

- **P**olicies: zijn de algemene afspraken, doelstellingen, ethieken en verantwoordelijkheden die vastgelegd worden.
- **P**roducts: worden ingeschakeld om de policies mogelijk en beheersbaar te maken.
- **P**rocedures: bevatten de handelingen die gevolgd dienen te worden om de Policy waar te kunnen maken.
- **P**eople: centraal blijven de mensen die het geheel doen slagen.

De doelstelling van dit document is gesitueerd rond de POLICY, de richtlijnen voor het dagdagelijks computergebruik. Een weergave van de recentste Policy is terug te vinden op het intranet.

4 Uitgangspunten

CIRCET BELGIUM stelt diverse company smart devices en een centrale ICT-infrastructuur ter beschikking aan haar medewerkers om de uitvoering van de taken gemakkelijker te maken.

De infrastructuur wordt door CIRCET BELGIUM ter beschikking gesteld, up-to-date gehouden en beheerd. Teneinde deze zo goed mogelijk aan te wenden voor de verschillende medewerkers worden hieromtrent afspraken gemaakt.

De finale doelstelling van een duidelijke overeenkomst voor ICT-gebruik is vierledig:

1. De efficiëntiegraad van het gebruik verhogen.
2. Uitsluiten van misbruik van CIRCET BELGIUM materiaal.
3. De ethische code in ere te houden door respectvol te communiceren.
4. De informatieveiligheid waarborgen.

4.1 De evolutie

De evolutie binnen de ICT-wereld gaat vrij snel. Vandaar dat deze Policy op regelmatige basis zal worden bijgestuurd. De laatste versie van dit document is steeds raadpleegbaar op het intranet.

5 Algemeen gebruik van Smart devices

5.1 Algemeen

Aangezien de informatica uitrusting een werkinstrument is dat ter beschikking gesteld wordt voor het uitoefenen van de functie, dient men dit ook met de nodige zorg te behandelen.

Als een voorzichtig en redelijk persoon dient men alert te zijn voor mogelijke gevaren, niet alleen voor het eigen systeem maar tevens voor het netwerk waarvan men deel uitmaakt. Wetende dat men nooit alleen werkt maar gezamenlijk bepaalde resources gebruikt (zoals internet toegang) dient men er tevens over te waken dat men deze niet nodeloos gebruikt. Een verspilling is steeds ten nadele van andere collega's die deze functionaliteit wel nodig hebben voor het uitoefenen van hun functie.

Het gebruik van verwijderbare media storage zoals USB-sticks is geblokkeerd bij CIRCET Belgium. Alternatieven zoals het veilig delen van bestanden met Onedrive zijn beschikbaar. Het beleid binnen de organisatie is om geen data lokaal op te slagen op Company of Private smart devices en enkel gebruik te maken van de Cloud oplossingen zoals OneDrive. Elke medewerker heeft hiervoor een aantal GB-storage beschikbaar.

5.2 Types smart devices

5.2.1 Company smart devices

Een Company Smart device dat ter beschikking gesteld wordt voor telewerk dient met dezelfde zorg behandeld te worden als op het werk. CIRCET Belgium staat in voor het correct werken van de apparatuur, daartegenover staat dat men als medewerker deze correct dient te gebruiken voor het uitoefenen van zijn functie. Het toestel wordt opgeborgen wanneer het niet in gebruik is en vrij van stof en vuil.

Het company smart device staat ter beschikking van de medewerker, het is niet de bedoeling dat andere personen hiervan gebruik maken.

Company smart devices worden geëncrypteerd op basis van Bitlocker technologie.

5.2.2 Private smart devices

Een private smart device (aangekocht op eigen rekening) staat niet onder het beheer van CIRCET Belgium. Elk private smart device staat onder het beheer van de eigenaar, als Bedrijf beschikt men niet over voldoende bevoegdheden om hierop te werken.

De diversiteit aan software, connectiemogelijkheden, evenals het gebrek aan bevoegdheid zorgen ervoor dat CIRCET BELGIUM niet kan garant staan voor een stabiele werkomgeving en continuïteit.

Private smart devices worden en mogen dan ook nóóit geconnecteerd worden met het bedrijfsnetwerk. Dit impliceert dat alle medewerkers moeten werken met ICT-middelen die eigendom zijn van CIRCET Belgium. Voor medewerkers is het wel toegelaten een private smartphone te gebruiken. De medewerker wordt wel verplicht een Circet-container te laten installeren om toegang te krijgen tot, en gebruik te maken van de e-mail-, document- en communicatietools van CIRCET BELGIUM.

Mobile Application management (MAM) wordt afgedwongen op alle private smart devices.

- Beheer van bedrijfsgegevens: MAM zorgt ervoor dat bedrijfsgegevens veilig blijven op privétoestellen. Dit betekent dat je bedrijfsgegevens kunt scheiden van persoonlijke gegevens en ervoor kunt zorgen dat bedrijfsgegevens alleen toegankelijk zijn via goedgekeurde apps.
- Beveiliging en naleving: MAM biedt beveiligingsfuncties zoals het afdwingen van app-beveiligingsbeleid, het versleutelen van bedrijfsgegevens en het voorkomen van datalekken. Dit helpt bij het naleven van bedrijfsbeleid en regelgeving.
- Toegangsbeheer: MAM maakt het mogelijk om toegang tot bedrijfsgegevens te beheren en te controleren. Je kunt bijvoorbeeld bepalen welke apps toegang hebben tot bedrijfsgegevens en welke acties gebruikers kunnen uitvoeren met die gegevens.
- Gebruiksvriendelijke ervaring: MAM biedt een gebruiksvriendelijke ervaring voor werknemers door hen in staat te stellen bedrijfsgegevens te gebruiken op hun privétoestellen zonder dat ze hun persoonlijke gegevens hoeven op te geven.
- Ondersteuning voor verschillende platforms: MAM ondersteunt verschillende mobiele platforms, waaronder Windows, iOS en Android, waardoor het geschikt is voor een breed scala aan privétoestellen.

5.2.3 Other smart devices

Naast company smart devices (eigen aan CIRCET BELGIUM) en private smart devices (eigen aan de medewerker) zijn er nog diverse andere smart devices waarmee een communicatie naar CIRCET BELGIUM mogelijk is.

We denken hierbij aan:

- Smart devices van een klant waarmee CIRCET BELGIUM medewerkers moeten werken om hun job uit te kunnen voeren. Deze smart devices dienen steeds te connecteren op het Guest LAN
    - vb Proximus
- Smart devices van een klant voor testdoeleinden. Deze smart devices dienen steeds te connecteren op het Guest LAN
    - Vb ServiceCruiser: nagaan compatibiliteit met de ServiceCruiser applicatie
- Internet Cafés
    - Deze devices communiceren met de bedrijfsapplicaties via web applicaties zoals Outlook Web Access

5.3 Afbakening van het gebruik

De smart devices door CIRCET BELGIUM verstrekt zijn enkel ter beschikking voor bedrijfsactiviteiten.

Gebruik van de ter beschikking gestelde smart devices is ten stelligste verboden voor:

- Privé bedrijfsactiviteiten (privéfirma);
- Privé gebruik in de vrij tijd (bv. Games);
- Het verdelen of downloaden van illegale software, muziek, films, series of muziek;
- Zichzelf te verrijken (vb Bitcoins minen);
- Het weergeven, opslaan, verwerken, verspreiden of downloaden van seksuele, racistische, discriminerende of aanstootgevende inhoud en/of daaraan gerelateerde doeleinden;
- Het weergeven, opslaan, verwerken, verspreiden of downloaden van gegevens die een aantasting kunnen zijn van de waardigheid van anderen en/of daaraan gerelateerde doeleinden. Onder aantasting wordt onder andere verstaan lasterlijke, onzedelijke, oneervolle communicatie en het hebben van pornografische afbeeldingen in het bijzonder;
- deelname of uitoefenen aan activiteiten welke in strijd zijn met wet- en regelgeving, of welke een aantasting van de integriteit of goede naam van CIRCET BELGIUM kan opleveren;
- deelname aan 'kettingbrieven" of massaal versturen van ongevraagde berichten (spam);
- het verspreiden van gegevens die beschermd zijn door het auteursrecht of andere intellectuele eigendomsrechten, in strijd met de geldende wetgeving;
- Het verzenden van provocerende e-mails;
- Het gebruik van het elektronisch berichtensysteem in het kader van gelijk welke activiteit andere dan de uitoefening van de functie voor CIRCET BELGIUM, ongeacht de aard ervan, hieronder te verstaan: het voeren van (verkiezings)propaganda.

CIRCET BELGIUM draagt ethiek en respect voor collega's hoog in het vaandel. Alle communicatie die ook maar in enige mate als aanstootgevend kan worden ervaren, wordt niet getolereerd.

Het is tevens ook verboden freeware of shareware te installeren. Enkel software met een licentie van CIRCET BELGIUM mag op het toestel worden geïnstalleerd.

5.4 Etiquette

Houd bij het gebruik van de elektronische communicatie steeds rekening met:

- Beleefdheid: gebruik geen compromitterende of aanstootgevende taal.
- Voer geen activiteiten uit die door de wetgever verboden zijn.
- Houd rekening met de anderen. Efficiënt gebruik van elektronische communicatie zorgt ervoor dat de ontvanger geen overlast ervaart.
- Wees bij het opstellen van een e-mail kort, bondig en duidelijk.

5.5 Confidentialiteit

Elke medewerker dient de vertrouwelijkheid te waarborgen voor de documenten die hij/zij binnen de uitoefening van zijn functie heeft aangemaakt, dit onafhankelijk van de locatie waarop deze werden aangemaakt. Deze data blijven te allen tijde eigendom van CIRCET BELGIUM en mogen derhalve niet ter beschikking gesteld worden aan Externen, tenzij dit noodzakelijk is voor de uitoefening van een overeenkomst met deze Externen op voorwaarde dat in deze overeenkomst de nodige confidentialiteitswaarborgen zijn opgenomen.

In het kader van deze confidentialiteit dienen deze documenten dan ook steeds centraal op de informatiesystemen van het Bedrijf opgeslagen te worden.

Gedurende het "offline" werken is de medewerker verantwoordelijk voor het behoud van de confidentialiteit en veiligheidskopijen van zijn documenten.

Medewerkers moeten de "clean desk / clear screen" principes toepassen:

- vergrendel het werkstation als je van de werkplek wegloopt (screen Lock);
- berg vertrouwelijke gegevens op in een afsluitbaar ladeblok of kast;
- gebruik de optie tot beveiligd printen en laat prints niet bij de printer liggen;
- gooi vertrouwelijke (uitgeprinte) gegevens in de grijze container met 'vertrouwelijk papier sticker' of in de papierversnipperaar; De papierbakken op de kantoren zijn niet geschikt voor vertrouwelijke gegevens, omdat deze niet kunnen worden afgesloten.
- zorg ervoor dat een meeting ruimte netjes wordt achtergelaten na gebruik (wis het whiteboard, neem alle documenten mee, etc.).

5.6 Schade, verlies of diefstal van de smart devices

Alle medewerkers aan wie company smart devices of ander ICT-materiaal/infrastructuur ter beschikking gesteld is in het kader van te verrichten arbeid buiten de CIRCET BELGIUM kantoren zijn niet verzekerd tegen alle risico's en verlies met betrekking tot dit materiaal.

De medewerker dient als een voorzichtig en redelijk persoon om te gaan met zijn materialen die ter beschikking zijn gesteld door CIRCET BELGIUM.

Wanneer de medewerker dient te reizen zal hij zijn company smart device steeds als handbagage meenemen. Wanneer de medewerker zich met de auto verplaatst dient hij het device steeds in de koffer te leggen en nooit op de achterbank of passagiersstoel achter te laten.

Indien een company smart device verloren is of gestolen werd, dient de ICT servicedesk te worden verwittigd om het toestel te blokkeren. Indien een private smart device waarop CIRCET applicaties geïnstalleerd staan verloren of gestolen is dient ook de ICT servicedesk te worden verwittigd zodat de applicaties vanop afstand kunnen worden geblokkeerd.

Tevens dient ook onmiddellijk een password reset te worden uitgevoerd op de CIRCET accounts.

5.7 Vervanging en end-of-life van company smart devices

CIRCET BELGIUM zorgt voor vernieuwing van de bedrijfstoestellen wanneer dit vereist is om de functie uit te kunnen voeren. Oude toestellen dienen steeds ingeleverd te worden bij de CIRCET BELGIUM ICT Servicedesk. Dit is eveneens van toepassing voor andere media/toestellen die men niet meer gebruikt, te oud zijn of vervangen worden zoals (niet limitatief): laptops, desktops, harde schijven , usb keys, telefoons, tablets enz.

Bij de inlevering mag er geen gevoelige en/of confidentiële (persoonlijke) data meer aanwezig zijn op de toestellen. De CIRCET BELGIUM ICT Servicedesk zal verder instaan voor het correct "vernietigen" van alle elektronische data dragers.

5.8 Ondersteuning van private smart devices

CIRCET BELGIUM voorziet geen ondersteuning voor private smart devices. Men dient hiervoor zelf in te staan.

Er is een procedure beschikbaar om bedrijfsapplicaties beveiligd te installeren op private smart devices zonder verdere ondersteuning. Hiervoor wordt mobile device management software geïnstalleerd zoals beschreven in de phone policy.

5.9 Blokkering van smart devices

Indien er acties uitgevoerd worden op private smart devices of company smart devices die strijdig zijn met deze ICT-policy dan behoudt CIRCET BELGIUM zich het recht voor om deze smart devices te blokkeren en niet langer toegang tot zijn infrastructuur toe te laten.

Acties die niet toegelaten zijn o.a.:

- Jailbreak, rooting van mobile devices op company smart devices (hacken van de toestellen);
- Illegaal gebruik van APPS company smart devices;
- Raadplegen van CIRCET Mail buiten de voorziene CIRCET software op private smart devices;
- Etc.

5.10 Beveiliging

Company smart devices zijn beveiligd met een pincode. Deze wordt automatisch geactiveerd wanneer het toestel aan de medewerker wordt uitgeleverd.

Private smart devices waarop de beveiligde omgeving staat om de CIRCET applicaties raad te plegen worden ook verplicht een pincode in te stellen.

6 Paswoord policy – Toegang tot het netwerk

6.1 Inleiding

Paswoorden zijn belangrijk voor wat betreft informatieveiligheid. Een eenvoudig paswoord kan leiden tot ongeoorloofde toegang en misbruik van de computersystemen en/of informatie van CIRCET BELGIUM. Alle gebruikers die toegang hebben tot de CIRCET BELGIUM systemen/applicaties zijn verantwoordelijk voor het nemen van volgende stappen om een zo veilig mogelijk paswoord te kiezen.

6.2 Doelstelling

Met deze afspraak wensen we een standaard op te leggen voor het gebruik van "sterke" paswoorden, de bescherming van deze paswoorden en de frequentie van wijziging.

Naast de het gebruik van "sterke" paswoorden wordt ook gebruik gemaakt met "Multi Factor Authenticatie" (MFA).

Indien business applicaties MFA technisch ondersteunen worden deze gelinkt aan het centrale authenticatiemechanisme.

6.3 Bereik (scope) en verantwoordelijkheden

Deze afspraak omvat iedereen (zowel Werknemers als Externen) die beschikt over een CIRCET BELGIUM account of verantwoordelijk is voor een CIRCET BELGIUM account waarmee men toegang verkrijgt tot CIRCET BELGIUM informatie die niet publiek toegankelijk is.

6.4 Afspraken (Policy) voor toegang tot het netwerk

Alle paswoorden moeten minimaal voldoen aan onderstaande eisen voor "strenge" paswoorden:

- Bevat ten minste 16 alfanumerieke karakters
- Mag niet hetzelfde zijn als het voorgaande paswoord.

Moet voldoen aan minimaal 3 van onderstaande vereisten:

- Hoofdletter;
- Kleine letters;
- Bevat minimum één cijfer (0-9);
- Bevat minimaal één speciaal karakter (Voorbeeld:!$%^&*()_+|~-=\`{}[]:";'<>?,/);
- Bevat minimaal één unicode karakter (Voorbeeld: Aziatisch teken).

Wat zijn slechte paswoorden?

- Minder dan 16 karakters;
- Woorden die gemakkelijk teruggevonden kunnen worden in een woordenboek, dialect of voorkomen in een bepaald jargon;

- Die persoonlijke informatie bevatten zoals geboortedatum, adres, gsm-nummer of namen van familie, vrienden, dieren enz.;
- Werk gerelateerde informatie zoals firmanaam, adres enz. ;
- Bepaalde eenvoudige patronen: aaabbb, qwerty, zyxwvuts, of 123321;
- Courante woorden die omgekeerd genoteerd worden of waar men cijfer 1 aan toevoegt;
- Varianten van "Welcome123" "Password123" "Changeme123".

Paswoorden mogen nooit opgeschreven worden.

Voor specifieke business applicaties kan een afwijkende paswoord policy actief zijn indien de applicatie niet gekoppeld is aan het Active directory authenticatiemechanisme.

6.5 Aanmaak van paswoorden

- Alle paswoorden moeten voldoen aan bovenstaande richtlijn.
- Gebruikers mogen niet hetzelfde paswoord gebruiken voor CIRCET BELGIUM accounts als voor niet-CIRCET BELGIUM accounts (privéaccounts).
- Bij voorkeur gebruikt men een ander paswoord voor de applicaties die niet automatisch gekoppeld zijn met het netwerkaccount.
- Een systeem account moet een uniek en verschillend paswoord hebben dat de gebruiker nergens anders reeds in gebruik heeft.
- Wanneer een gebruiker een "initieel" paswoord bekomen heeft van CIRCET BELGIUM IT dan dient de gebruiker dit bij de eerste aanmelding onmiddellijk te wijzigen.

6.6 Wijzigen van paswoorden

- De ICT servicedesk zal bekende lijsten van gelekte paswoorden (vb.HaveIBeenPwned.com) gebruiken om na te gaan of accounts betrokken zijn bij datalekken en hierop ook de nodige acties ondernemen.
- Alle gebruikers en systeem paswoorden moeten minstens 1 maal per jaar gewijzigd worden.

6.7 Bescherming van paswoorden

- Paswoorden mogen niet gedeeld worden. Alle paswoorden moeten behandeld worden als gevoelige en confidentiële CIRCET BELGIUM informatie.
- Paswoorden mogen niet via mail of telefoongesprek bezorgd worden.
- Deel geen paswoorden mee indien via mail/web formulieren hierom gevraagd wordt.
- Gebruik geen hints, bv. mijn familienaam.
- Deel geen paswoorden als je op vakantie gaat, tevens worden paswoorden niet aan familie/vrienden/kennissen bezorgd.
- Schrijf paswoorden niet op, bewaar deze niet in je draagtas, op je bureau of in lades/kasten. Gebruik een paswoord tool zoals KeePass (encryptie) om deze toch op het smart device te bewaren.
- Indien vereist kan de ICT Servicedesk ook Passwordstate voorzien voor het opslaan van bepaalde bedrijfskritische accounts en paswoorden.
- Gebruik niet "wachtwoord onthouden" in browsers of applicaties.
- Wanneer men 5 pogingen ondernomen heeft zonder succes dan wordt de gebruiker geblokkeerd (lockout) gedurende 5 minuten. Indien de gebruiker er niet in slaagt om succesvol aan te melden dient deze de CIRCET BELGIUM ICT Servicedesk te raadplegen om terug toegang te verkrijgen.
- Elke gebruiker die vermoedt dat zijn paswoord gekend/gebruikt werd door anderen dient dit onmiddellijk te melden aan CIRCET BELGIUM ICT Servicedesk en zijn paswoorden allemaal te wijzigen.

6.8 Applicatieontwikkeling

Bij applicatieontwikkeling dient de geschreven software te voldoen aan volgende security vereisten:

- Authenticatie dient te gebeuren op niveau van de individuele gebruiker, generieke accounts zijn niet toegelaten.
- Paswoorden moeten encrypted (hash met salt) opgeslagen worden, niet als "plain tekst". Idealiter dienen zij gekoppeld te zijn aan een identity provider zoals Azure AD.
- Paswoorden moeten ook in transfer (over het netwerk) geëncrypteerd blijven.
- De applicaties moeten voorzien zijn van security rollen, gebruikers met dezelfde rol kunnen dan gemakkelijk elkaars taken overnemen zonder dat het wachtwoord moet bezorgd worden.
- Applicaties moeten voldoen aan recente beveiligingsstandaarden, zoals een recente versie van TLS (Transport Layer Security).

6.9 Paswoorden van leveranciers / opdrachtgevers

Paswoorden van leveranciers of opdrachtgevers worden geëncrypteerd opgeslagen in de CIRCET BELGIUM Password State. Deze dienen steeds met de nodige omzichtigheid behandeld te worden. Paswoorden zijn confidentieel en dienen ook als dusdanig behandeld te worden, zowel tijdens als na de tewerkstellingsperiode bij CIRCET BELGIUM.

Paswoorden worden niet per e-mail verspreid. Bij vragen van een leverancier of opdrachtgever, dient steeds telefonisch contact opgenomen te worden ter verificatie met de betrokkene. Indien mogelijk moet doorverwezen worden naar de verantwoordelijke van de opdrachtgever. Pas na deze verificatie en toestemming van de verantwoordelijke kan dit meegedeeld worden. Indien de verantwoordelijke niet bereikt kon worden kan het paswoord niet worden verspreid.

Hoe kan een paswoord veilig aan een leverancier of opdrachtgever bezorgd worden?

- Indien het gsm-nummer vooraf gekend is, kan men het paswoord via sms bezorgen. Als het GSM nummer niet gekend is, mag dit niet via sms verzonden worden.
- Nadat men zekerheid heeft omtrent de authenticiteit van de betrokkene kan men ook via tools zoals onetimesecret (https://onetimesecret.com/) het paswoord uitwisselen met de betrokkene. De lifetime dient kleiner te zijn dan 12u. Er mag geen identificeerbare informatie in de Onetimesecret pagina staan (niet de gebruikersnaam, link en paswoord samen).

7 Software Installatie Policy

7.1 Doelstelling

Het doel is aan de diverse eindgebruikers een werkomgeving aan te bieden met software en hardware die aangepast zijn aan de functie en de bedrijfsdoelstellingen.

7.2 Huidige Standaard Software

Deze bestaat uit (niet limitatief):

- Microsoft Windows Operating System;
- Microsoft Office;
- Antivirus Software;
- Business Unit gerelateerde software (D365, GO Workflow, Exact, ..).

7.3 Software aanvragen

Indien voor het uitvoeren van een bepaalde functie een (extra) software licentie nodig is, zal dit steeds, na goedkeuring van de N+1, aangevraagd worden via de ITSM tool Xurrent. Slechts na de vereiste goedkeuring en aanvraag kan de installatie verzorgd worden.

7.4 Copyrights en licenties

7.4.1 ICT Verantwoordelijkheden

De software welke door CIRCET BELGIUM ter beschikking gesteld wordt van de eindgebruiker zal steeds voorzien zijn van de nodige licentie.

De ICT servicedesk zal dan ook op regelmatige tijdstippen een scan uitvoeren ter controle van de aanwezige software per bedrijfstoestel.

7.4.2 Verantwoordelijkheden eindgebruikers

Eindgebruikers zullen niet:

- Illegale software kunnen installeren of verspreiden;
- Software kopiëren die onder CIRCET BELGIUM licentie valt.

Opmerking voor ICT & ServiceCruiser Medewerkers

Aangezien CIRCET BELGIUM een eigen ICT afdeling heeft en bovenstaande verantwoordelijkheden bedoeld zijn voor de standaard eindgebruiker dienen we voor deze groep een aanpassing te voorzien.

Als "ICT-medewerker" gelden volgende verantwoordelijkheden:

Additionele legale software downloaden/installeren naast de standaard software op het company smart device kan indien mits akkoord van de N+1. Een licentie zal aangekocht worden door CIRCET BELGIUM wanneer vereist. In het geval van freeware of opensource applicaties dient ook steeds een akkoord te worden gevraagd aan de N+1 en de voorwaarden voor gebruik te worden gerespecteerd.

8 Internet Policy

8.1 Inleiding

Het internet biedt een breed spectrum aan resources en diensten, dit betekent nieuwe opportuniteiten maar ook nieuwe risico's. Deze Policy richt zich dan ook vooral naar de mogelijke risico's.

8.2 Doelstelling

Afspraken omtrent een correct Internetgebruik vastleggen.

8.3 Bereik

De Policy is van toepassing op alle medewerkers van CIRCET BELGIUM en slaat op alle Internetcommunicatie uitgevoerd vanaf alle smart devices in het Bedrijf eigendom van CIRCET BELGIUM en de externe CIRCET BELGIUM smart devices die een connectie maken met het bedrijfsnetwerk.

8.4 Eigendomsrecht

Alle communicatie welke plaatsgrijpt over het bedrijfsnetwerk en niet speciaal geïdentificeerd werd als eigendom van een andere partij wordt beschouwd als eigendom van CIRCET BELGIUM. Het is de doelstelling van CIRCET BELGIUM om mogelijke misbruiken zoals: vreemde indringers, diefstal, vernietiging, wijziging, oneigenlijk gebruik te voorkomen.

Daarnaast wordt eveneens de informatie toebehorend aan derden welke een contractuele band hebben met CIRCET BELGIUM beschermd, dit in overeenstemming met de bestaande contracten en GDPR richtlijnen.

8.5 Informatie-uitwisseling
Binaire bestanden aanwezig op het internet kunnen verschillende risico's inhouden. Het is derhalve niet aangeraden om deze zomaar te downloaden. Binaire bestanden downloaden waar niet uitdrukkelijk de toestemming werd gegeven door de auteur is dan ook verboden. We denken hierbij aan muziekbestanden, videomateriaal, software enz.

Anderzijds mag geen informatie eigen aan CIRCET BELGIUM door een gebruiker op het internet gepubliceerd of verder gedistribueerd worden tenzij dit uitdrukkelijk door de verantwoordelijke werd goedgekeurd.

8.6 Afbakening
Het gebruik van het Internet voor bedrijfsdoeleinden wordt door CIRCET BELGIUM gestimuleerd.

Het management behoudt het recht om het degelijk gebruik van het Internet globaal te controleren zoals vermeld in het arbeidsreglement.

9 E-mail Policy

9.1 Doelstelling
Het maken van afspraken omtrent een correct e-mail gebruik.

9.2 Bereik
De Policy is van toepassing op alle medewerkers van CIRCET BELGIUM en slaat op alle e-mail aanwezig op smart devices onder het beheer of eigendom van het Bedrijf. Deze slaat zowel op de smart devices aanwezig in het Bedrijf als de externe smart devices die een connectie maken met het bedrijfsnetwerk.

CIRCET BELGIUM heeft Microsoft Office 365 gekozen als bedrijfsplatform voor e-mailcommunicatie.

Bedrijfscommunicatie mag uitsluitend gevoerd worden via de CIRCET MS Office 365 omgeving. Alle andere e-mail platformen zoals Gmail, Hotmail,.. enz. zijn hiervoor niet toegelaten tenzij dit uitdrukkelijk goedgekeurd werd door de N+1.

9.3 Eigendomsrecht
Elektronische communicatie wordt aangemoedigd als een productiviteitsverhogend hulpmiddel. De E-mail communicatiesystemen en alle berichten aangemaakt of behandeld door deze systemen, inclusief veiligheidskopieën, zijn eigendom van CIRCET BELGIUM en niet van de gebruikers van de elektronische communicatiediensten.

9.4 Standaard Privileges
Elke medewerker beschikt standaard over "user" permissies, dit betekent dat hij zijn eigen communicatiesysteem alsook de rechten hiertoe voor derden zelf beheert.

9.5 Gebruikers Identificatie
Elke gebruiker beschikt over een uniek gebruikersnaam/paswoord waarmede de elektronische communicatiediensten gebruikt worden. Het paswoord is persoonsgebonden en mag onder geen omstandigheid kenbaar gemaakt worden aan derden.

Indien het E-mailadres doorgegeven wordt aan derden, houd er dan steeds rekening mee dat dit mogelijk "misbruikt" kan worden voor bv. reclamedoeleinden. Bij twijfel mag het persoonlijke CIRCET e-mail adres niet worden doorgegeven.

9.6 Beveiliging inhoud

Standaard wordt de elektronische communicatie niet beveiligd. Indien een beveiliging (versleuteling) gewenst is, dient hiervoor contact opgenomen te worden met de ICT Servicedesk.

Gebruikers dienen er steeds rekening mede te houden dat elektronische communicatie door anderen zou kunnen afgetapt worden, geprint of opgeslagen kan worden.

9.7 Privacy Controle

Medewerkers mogen geen elektronische communicatie onderscheppen, openen (of een poging hiertoe ondernemen) welke niet voor hen bestemd is tenzij dit expliciet toegewezen werd door de N+1.

CIRCET BELGIUM respecteert de rechten van zijn werknemers inclusief de daarbij aansluitende privacy verwachting.

Anderzijds is CIRCET BELGIUM verantwoordelijk voor de beschikbaarheid en beveiliging van zijn elektronische communicatiediensten. Om dit te verwezenlijken kan het occasioneel nodig zijn elektronische communicatie te monitoren.

Hoewel het de medewerker niet toegestaan is om de smart devices aangeboden door het Bedrijf niet te gebruiken voor privédoeleinden, komt het de medewerker toe om, indien hij uitzonderlijk een privémail ontvangt op zijn professioneel e-mailadres, deze onmiddellijk te verwijderen bij voorkeur, of deze duidelijk aan te merken als "privé" en te archiveren.

9.8 E-mail Monitoring – Filtering

CIRCET BELGIUM heeft NIET als doel een regelmatige monitoring van de e-mail inhoud uit te voeren. Doch, de inhoud en het gebruik van de elektronische communicatie kan gemonitord worden voor de doeleinden zoals omschreven in artikel 9 van het arbeidsreglement ("regels mbt het gebruik van elektronische communicatiemiddelen – controlemogelijkheden").

In geval van een sterk vermoeden van of bewezen (deelname aan) frauduleuze, bedrieglijke en/of illegale activiteiten in hoofde van een medewerker van CIRCET BELGIUM binnen de context van diens arbeids- of samenwerkingsovereenkomst behoudt CIRCET BELGIUM zich het recht voor om zichzelf toegang te verschaffen tot de professionele mailbox van de desbetreffende medewerker. Dit gebeurt in overeenstemming met de privacyverklaring en de procedure in artikel 9 van het arbeidsreglement.

De gebruikers zijn hierbij op de hoogte van de mogelijke monitoring Daarnaast worden preventief alle mails gescand door software. Het doel van deze automatische scanning is:

- Blokkeren van e-mail spam;
- Blokkeren van e-mails met niet-ethische inhoud;
- Blokkeren van e-mails met gevaarlijke bijlagen.

9.9 Statistische data

Voor rapporteringdoeleinden zal statistische data bijgehouden worden omtrent de elektronische communicatie. Deze informatie dient om de beschikbaarheid en betrouwbaarheid van het communicatiesysteem te kunnen blijven garanderen.

9.10 Raadplegen op aanvraag

Bij het onderzoeken van een communicatieprobleem kan het noodzakelijk zijn voor de ICT servicedesk om de inhoud hiervan te raadplegen. De ICT servicedesk mag in geen geval de inhoud raadplegen uit eigenbelang (curiositeit). Raadplegen van communicatie dient ook steeds te gebeuren conform het 4 ogen principe.

9.11 Doorsturen (forwarding) van berichten

De informatie is over het algemeen bestemd voor individuele personen en derhalve niet geschikt voor algemene distributie. Informatie eigen aan CIRCET BELGIUM mag niet worden doorgestuurd naar personen niet behorend tot het Bedrijf.

De e-mailcommunicatie is bedrijfscommunicatie, derhalve mag men deze niet automatisch of manueel doorsturen naar privéadressen (persoonlijk of van derden) of naar adressen van klanten waar de CIRCET BELGIUM medewerker ook een mailbox heeft. Uitzonderingen hierop dienen aangevraagd en goedgekeurd te worden door de ICT Servicedesk Manager. Het automatisch doorsturen van e-mails naar privé adressen wordt ook standaard geblokkeerd.

9.12 Bewaren en opruimen van e-mailberichten

Belangrijke communicatie met prospecten/opdrachtgevers die best bewaard wordt, dient steeds in de sharepoint-omgeving of fileserver van het Bedrijf opgeslagen te worden.

Berichten die niet langer nodig zijn voor het Bedrijf dienen op periodieke tijdstippen verwijderd te worden door de gebruikers.

De gebruiker staat persoonlijk in voor het verwijderen van oude berichten zodat de normale werking van het e-mailsysteem kan gegarandeerd worden.

Een online archief is ter beschikking om oudere berichten te bewaren indien noodzakelijk voor het bedrijf.

9.13 Omvang van de berichten

Indien grote bestanden dienen gedeeld te worden met derden wordt aangeraden om dit uit voeren met OneDrive for Business en niet te versturen via E-mail. Het beheer van de toegangen op OneDrive is onder verantwoordelijkheid van de medewerker. Hij/zij dient hier met de nodige aandacht mee om te gaan.

Indien bestanden toch via e-mail dienen verdeeld te worden dient men rekening te houden met volgende:

- Het doorsturen van een document betekent een belasting op de bandbreedte. Binnen het bedrijfsnetwerk is de grootte van de documenten niet gelimiteerd, doch op verschillende e-mailservers binnen het Internet is dit wel het geval.
- Als basisregel mag men aannemen dat de kans dat documenten bij de bestemmeling terecht komen afneemt naarmate deze groter zijn dan 10 MB (Megabyte). Wenst men een quasi zekerheid dat deze de eindbestemming bereiken dan dient men deze kleiner dan 10MB te houden.

9.14 Off-boarding en langdurige afwezigheid

Off-boarding:

In geval van beëindiging van de arbeidsovereenkomst of samenwerkingsovereenkomst, dient de medewerker diens mailbox uiterlijk de dag vóór vertrek op te ruimen opdat er géén privé e-mails meer in de professionele mailbox onder het beheer van CIRCET BELGIUM zitten. Dit dient te gebeuren in de aanwezigheid van de N+1,, een ICT of HR medewerker en kan ofwel door middel van het verwijderen van de desbetreffende privé e-mails, ofwel door ze door te sturen naar een eigen privé e-mailadres. Er zal aan de medewerker gevraagd worden om een verklaring te ondertekenen die bevestigt dat er géén privé-informatie meer aanwezig is in de professionele mailbox.

Uiterlijk op de dag van vertrek zal een automatisch bericht ingesteld worden om correspondenten te informeren van een alternatieve correspondentiemogelijkheid om de continuïteit van de bedrijfsvoering te garanderen. Na vertrek zal de toegang tot de mailbox geblokkeerd worden door IT zonder onnodige vertraging. De mailbox met het automatische "out-of-office"-bericht zal gedurende één maand na vertrek van de medewerker, of, in geval van het vertrek van iemand die een functie binnen het directiecomité of senior management bekleedt, voor zover diens toestemming bekomen is, drie maanden na vertrek actief blijven om de continuïteit van de bedrijfsvoering van CIRCET BELGIUM te garanderen.

Na verloop van deze periode van één maand/drie maanden, behoudt CIRCET zich het recht voor om een PST-file te maken van de professionele mailbox (waarin enkel professionele e-mails zitten). Het e-mailaccount en het e-mailadres zullen vervolgens onherroepelijk verwijderd worden. Indien een PST-file wordt gemaakt, zal deze bewaard worden voor een periode van maximaal 5 jaar voor de continuïteit van de bedrijfsvoering te garanderen en voor bewijsredenen gedurende de duur van een lopende procedure. Toegang tot de PST-file wordt enkel toegestaan in uitzonderlijke omstandigheden voor de vermelde doeleinden. Er moet hiervoor een gemotiveerd verzoek worden ingediend bij ICT Service Desk:

- Indien toegang noodzakelijk is voor de continuïteit van de bedrijfsvoering: de ICT Service Desk manager zal in samenspraak met de direct leidinggevende van de ex-medewerker beslissen over het verzoek tot toegang al dan niet toe te kennen en voor welke duur.
- Indien toegang noodzakelijk is voor bewijsredenen in een procedure: Legal zal een gemotiveerd verzoek indienen, waarna de ICT Service Desk manager de toegang zal geven voor een beperkte termijn.

Langdurige afwezigheid:

In geval van een geplande langdurige afwezigheid zal gelijkaardig te werk gegaan worden met een tijdig ingesteld automatisch "out-of-office"-bericht, inclusief vermelding van een alternatieve correspondentiemogelijkheid, dewelke wordt vastgelegd in samenspraak met de direct leidinggevende. Toegang tot de mailbox zal geblokkeerd worden na vertrek zonder onnodige vertraging, en zonder dat de mailbox verwijderd wordt vooraleer de tewerkstelling en de daarbij horende overeenkomst eventueel definitief beëindigd worden. In geval van ongeplande aanwezigheid zal het ICT Service Desk na toestemming van de direct leidinggevende van de langdurig afwezige medewerker, toekomen om dergelijk automatisch bericht in te stellen, en de betrokken persoon hiervan tijdig en zonder onnodige vertraging in te lichten. Vervolgens wordt de toegang tot de mailbox ook hier geblokkeerd, zonder dat de mailbox verwijderd wordt vooraleer de tewerkstelling en de daarbij horende overeenkomst eventueel definitief beëindigd wordt.

In uitzonderlijke gevallen kan een gemotiveerd verzoek ingediend worden bij IT Service Desk via het daarvoor bestemde ticketsysteem om alsnog toegang tot de mailbox van de langdurig afwezige (ex-)medewerker te bekomen en de geblokkeerde toegang tijdelijk op te heffen indien de desbetreffende mail of informatie op geen andere wijze bekomen kan worden en voor zover daartoe een gerechtvaardigd belang bestaat. Het komt de ICT Service Desk Manager toe om samen met de direct leidinggevende van de afwezige medewerker te beslissen over het verzoek tot uitzonderlijke toegang al dan niet toe te kennen en voor welke duur.

9.15 Verantwoordelijkheden

Volgende verantwoordelijkheden gelden:

- CIRCET BELGIUM ziet toe op de accuraatheid van naleven van e-mail policies en standaarden.
- De ICT servicedesk staat in voor de security vereisten van de diverse smart devices inclusief hardware, software en data beveiliging.
- De ICT servicedesk staat in voor het assisteren bij eventuele problemen bij eindgebruikers

10 Anti-malware Policy

Malware (in al zijn vormen) zijn stukjes programmacode die ontworpen zijn om schade aan te brengen aan de privé- en bedrijfsactiviteiten.

Dit vormt een van de grootste bedreigingen voor de informatietechnologie van bedrijven.

10.1 Achtergrond

Het is belangrijk te weten dat:

- Het eenvoudiger is om te voorkomen dan te genezen. Proactief werken en denken is een must
- Het virus- spyware vrijhouden betekent dat men zich verzet tegen niet geautoriseerde toegang naar data en programma's, alsook het laten automatisch onderhouden van antivirussoftware

10.2 ICT Verantwoordelijkheden

De ICT servicedesk is verantwoordelijk voor:

- Het installeren en onderhouden van antivirussoftware op alle company smart devices
- Het proactief adviseren van eindgebruikers
- Adequaat reageren op Virus-Attacks, verwijderen van virussen, spyware, … en het loggen van deze incidenten

10.3 Verantwoordelijkheden van de eindgebruiker

Richtlijnen voor alle eindgebruikers:

- Een virus wordt nooit met opzet binnengebracht;
- Opletten met surfen naar "verdachte websites" en openen van onbekende bijlages in e-mail. In geval van twijfel steeds de ICT servicedesk contacteren;
- Software, data en code worden niet binnengebracht of uitgevoerd op bedrijfstoestellen indien deze van onbekende oorsprong zijn;
- Indien men het vermoeden heeft dat zijn company smart device besmet is met een computervirus of spyware dan wordt deze onmiddellijk van het netwerk gehaald, afgesloten en wordt de ICT servicedesk op de hoogte gebracht die hierop de nodige stappen onderneemt.