Informatiebeveiliging

Radarbreed

Eigenaar (rol)	*Directie RadarGroep*
Geschreven door	*Coen Ran*
Status	*Vastgesteld*
Laatste update	*30-10-2025*
Volgende geplande Review	*Q3 2026 (Privacybeleid Cyclus)*
Permalink nieuwste versie	*251030 Informatiebeveiligingsbeleid.docx*

Informatiebeveiligingsbeleid voor jou

Dit beleid is een Radarbreed beveiligingsbeleid en legt uit waar jij als medewerker van Radar verantwoordelijk voor bent op het gebied van informatiebeveiliging.

Over dit beleid

Radar bouwt samen met burgers, professionals en opdrachtgevers aan een inclusieve, diverse, weerbare en rechtvaardige wereld. Radar staat voor beweging creëren en verandering teweegbrengen. Wij vragen de mensen en organisaties waarmee wij werken om zich kwetsbaar op te stellen, anders kan er geen verandering zijn. Mensen en organisaties moeten er daarom op kunnen rekenen dat Radar een veilige en slagvaardige partner is.

Beveiliging gaat over het geheel van beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Omdat wij als organisatie steeds meer afhankelijk zijn van technologie, vinden wij het belangrijk dat wij deze goed beveiligen. We zien dit ook in de (toenemende) eisen van onze opdrachtgevers en wet- en regelgeving.

Het doel van dit informatiebeveiligingsbeleid is om de continuïteit van de bedrijfsvoering te waarborgen en beveiligingsincidenten te voorkomen. Mocht er toch iets misgaan, dan beperken we met dit beleid de gevolgen.

Informatiebeveiliging is de verantwoordelijkheid van ons allemaal. Leidinggevenden hebben daarbij een trekkende rol en vormen het voorbeeld voor goede informatiebeveiliging binnen hun team.

1. Basisregels

I. We gaan zorgvuldig om met de informatie van onze klanten en collega’s.

II. Rekening houden met informatiebeveiliging in je werk hoort erbij als medewerker bij Radar.

III. Om te zorgen dat we kunnen ondernemen en vernieuwen, nemen we alleen beveiligingsmaatregelen die werken en alleen als het past bij het risico dat we proberen te beheren.

2. Inloggen en accounts

Multifactor Authenticatie is verplicht voor alle systemen die wij gebruiken binnen Radar. Wanneer een systeem dat we nodig hebben voor het uitvoeren van ons werk dit niet biedt, dan maken wij vóór gebruik een risico analyse en nemen we op basis daarvan eventueel extra maatregelen. De eigenaar van het systeem is hiervoor verantwoordelijk.

Binnen Radar werken wij wachtwoordloos. Met een eenmalige code, die je alleen krijgt nadat je identiteit is geverifieerd, kan je twee aanmeldmethodes instellen:

- De Microsoft Authenticator app, gekoppeld aan de pincode van je telefoon en/of biometrische informatie die alleen op het apparaat zijn opgeslagen.
- Windows Hello for Business, geïntegreerd in je laptop, gekoppeld aan de pincode van je laptop en/of biometrische informatie die alleen op het apparaat zijn opgeslagen.

Om te zorgen dat dit veilige authenticatie methodes zijn, gelden de volgende regels:

- Je mag nooit iemand zonder toezicht toegang geven tot je Radar telefoon of laptop.
- Het delen van de pincode met, of het toevoegen van biometrie van, iemand anders is niet toegestaan.
- De pincode mag niet te raden zijn of hergebruikt van privé apparaten.

Overige authenticatie

Naast de MS365 omgeving heb je wellicht zakelijk ook andere inloggegevens nodig. Wanneer je inloggegevens krijgt van een opdrachtgever, dan moet je voor deze gegevens het beleid van de opdrachtgever volgen. Als dat er niet is of niet duidelijk is, maak je minstens een uniek wachtwoord dat je onthoudt en niet opschrijft.

Verder kan je nog overige inloggegevens nodig hebben voor je werk, zoals voor de bloemenzaak of bol.com. Deze moet je vaak ook delen met een collega. We eisen niet dat je deze allemaal onthoudt, maar ze moeten wel allemaal uniek zijn. Ook is een lijstje in een ‘gewone’ Excel niet veilig genoeg. RadarICT biedt hiervoor als bedrijfsoplossing de wachtwoordmanager Keeper. Het is aan de leidinggevende om in te schatten of de medewerker dit nodig heeft en dit aan te vragen bij ICT.

Zodra je uit dienst bent, wordt al je toegang ingetrokken. Als jij verantwoordelijk bent voor een systeem waarin gebruikersaccounts voorkomen, dan zorg je ervoor dat deze geblokkeerd en/of verwijderd worden wanneer iemand uit dienst gaat.

3. Digitale Werkplek

Binnen de Microsoft365 omgeving van Radar is de afdeling ICT verantwoordelijk voor de beveiliging. De afdeling ICT zorgt ervoor dat je met je account en de daaraan gekoppelde apparaten en apps veilig kunt werken aan je standaard werkzaamheden. Voor bepaalde activiteiten en projecten kunnen extra maatregelen worden afgesproken, daar moet je je dan ook aan houden. Je werkt met de middelen uit de Radar omgeving en gebruikt niet op eigen initiatief privé of nieuwe middelen.

Op de Radar startpagina vind je informatie over hoe je slim en veilig met de systemen werkt, onder andere op de pagina’s ICT en Privacy.

Wanneer je gebruik wilt maken van nieuwe middelen (bijv. een app) die nog niet onder het beheer van RadarICT vallen, dan moet je dat eerst overleggen. Voor RadarAdvies kan dit bij Team Support, de overige onderdelen doen dit bij RadarICT. De nieuwe middelen worden gecontroleerd op nut, overlap, beveiligingsrisico’s en passende licentievormen. Waar nodig worden er extra maatregelen afgesproken.

Wanneer besloten wordt dat de nieuwe middelen niet onder het beheer van ICT komen, dan is de houder van het informatiesysteem verantwoordelijk voor de beveiliging. ICT kan altijd wel adviseren.

Voor het beheer en de beveiliging van de omgeving monitort RadarICT het gebruik van de apparaten en de omgeving en verwerkt deze in logs. In sommige gevallen zijn deze gekoppeld aan actieve controles (alerts), anders ter voorkoming of oplossing van problemen en incidenten. Ook kunnen de logs gebruikt worden bij (verdenking van) misbruik.

Bestanden staan binnen Microsoft365 veilig:

- Wanneer jij bestanden opslaat in OneDrive of Teams, dan staan deze veilig voor je standaard werkzaamheden. Met behulp van versiebeheer en inrichting zijn bestanden tot in ieder geval 90 dagen beschermd tegen verwijdering of wijziging.
- Standaard wordt er op de Radar Windows laptops een back up gemaakt van de mappen 'Bureaublad', Documenten' en 'Afbeeldingen'.
- Sluit je laptop af wanneer je er mee klaar bent, dit zorgt voor encryptie op de bestanden zodat deze bij diefstal of verlies niet kunnen worden uitgelezen.
- Controleer of de synchronisatie van het bestand compleet is voordat je de laptop afsluit (het blauwe wolkje rechts onderin).

Sla bestanden 'goed' op: op de juiste plek en niet te lang

- Gooi bestanden weg als je ze niet meer nodig hebt. Grote mailboxen en dataopslag zorgt voor problemen in de werking van de systemen.
- Zet je bestanden alleen in een Team als je precies weet wie er allemaal bij kunnen.
- Privébestanden op Microsoft365 of op de apparaten draaien gewoon mee in het bedrijfsbeleid.

4. Fysieke werkplek

Clear Desk / Clear Screen

Je zorgt ervoor dat de spullen die je nodig hebt voor je werk goed weggeborgen zijn als je klaar bent of even wegloopt. Papieren gaan in een afgesloten kast, documenten stop je in het juiste mapje. Je doet geen schermpresentaties terwijl je bureaublad vol staat met documenten of terwijl je pop ups krijgt van WhatsApp.

Op kantoor

Wanneer je even wegloopt van je laptop, dan vergrendel je de laptop zodat anderen niet kunnen zien waar je mee bezig bent, of wijzigingen kunnen uitvoeren vanuit jouw account. TIP: de sneltoets hiervoor is ⊞+L . (Het vlaggetje zit links onderin op je toetsenbord.)

De laptop moet worden afgesloten wanneer je deze weglegt, dit activeert een extra encryptie van de bestanden die erop staan.

Onderweg

Zorg ervoor dat je de werkzaamheden aanpast aan de veiligheid van de ruimte. Een belangrijk telefoongesprek doe je niet in de trein. Werken aan een vertrouwelijke rapport doe je niet op een plek waar mensen kunnen meekijken. Je laat je spullen niet onbeheerd achter. Maak geen gebruik van 'gratis' wifi, maar gebruik de hotspot op je telefoon.

Thuis

Thuis gelden dezelfde afspraken als op kantoor. Je werkt gewoon op je Radar apparatuur met je Radar account.

Online vergaderen doe je met de tools van de klant als deze iets verplicht, of, wanneer vanuit Radar geïnitieerd, met Teams. Je zorgt ervoor dat werkdocumenten niet blijven liggen op de keukentafel en dat je gesprekken, net zoals op kantoor, op een passende plek kan houden zonder dat anderen kunnen meeluisteren. Omdat thuis de afstand tot je collega's wat groter is, hou extra rekening met phishing en andere vormen van oplichting. Weet je zeker dat je de juiste persoon op de mail hebt?

Zorg dat je weet wie er gebruik kan maken van je eigen internetverbinding, of gebruik anders je hotspot.

5. Omgang met apparatuur

Je gaat netjes om met de spullen die je van Radar krijgt. Je volgt hierbij minimaal de instructies van RadarICT. Dat betekent o.a. dat je gebruik maakt van de geleverde tassen en hoesjes, of, als je eigen beschermmiddelen gebruikt, dat deze hiervoor geschikt zijn. Dit betekent ook het bewaren van adapters en bijbehorende kabels. Duurzaamheid is hierbij belangrijk, een andere collega zou ook moeten kunnen werken met jouw spullen.

Bij het gebruik van de spullen is een bepaald niveau van privégebruik mogelijk en toegestaan. Zorg hierbij wel dat dit de laptop en je werk niet beïnvloedt. Bij storingen is het mogelijk dat zaken die niet strikt noodzakelijk zijn moeten worden verwijderd van de laptop. Radar is daarbij niet verantwoordelijk voor een back up.

Bij uitgave wordt in AFAS geregistreerd welke spullen je van ons gehad hebt.

6. Veilig (online) communiceren

Bij het ontvangen en verzenden van informatie moeten we er voor zorgen dat het bericht veilig overkomt en bij de juiste persoon terecht komt. Gelukkig hebben we hiervoor makkelijke tools.

Kies bij het (online) communiceren voor de juiste tools. Stuur een groot klantenbestand niet per WhatsApp, gebruik niet je eigen e-mailadres voor het versturen van grote hoeveelheden mail. Je vindt de juiste mogelijkheden op de Privacy pagina en daarnaast kan RadarICT je altijd adviseren.

<u>Doe niet te makkelijk, neem je verantwoordelijkheid:</u>

- Klik niet zomaar een attachment open;
- Stuur gegevens niet als je niet zeker weet waar deze aankomen: een groepsmail is makkelijk, maar of iedereen in de groep ook echt de informatie moet hebben is vaak onoverzichtelijk.

<u>Controleer de bron van de informatie</u>

- Controleer of je de afzender kent (verwachtte je een mail? Herken je het mobiele nummer?).
- Controleer of de inhoud van het bericht jou écht betreft (bijv. zit je wel bij die bank?).
- Controleer of de persoon is die hij/zij zegt: iemand die zich kan identificeren doet dat graag.
- Bij twijfel: neem contact op met RadarICT. Zij hebben liever 1000 keer een vals alarm, dan een keer een inbraak.

<u>Wees zelf een veilige bron van informatie:</u>

- Gebruik bedrijfssystemen bij voorkeur niet voor privézaken; jouw privézaken worden dan bedrijfseigendom.
- Misschien ten overvloede: doe niets illegaals met de bedrijfssystemen.
- Wees professioneel in je communicatie.
- Houd je aan de regels omtrent persoonsgegevens.

6.1 E-mails die je verstuurt zijn uit naam van Radar

- Moet je mailen naar meer dan 50 mensen, maak dan gebruik van speciale tools als Postera of Mailchimp. Anders kan je als spam worden aangeduid.
- Gebruik bij mails naar grote groepen mensen altijd de BCC-functionaliteit.
- Gebruik je Radar e-mailadres bij voorkeur niet privé: als je uit dienst gaat ben je ook je e-mailadres kwijt (bijvoorbeeld je AppleID). Daarnaast vergroot je het risico dat bedrijfsinformatie in de privésfeer terechtkomt (en andersom).

6.2 USB Stick (en alle verwijderbare media)

Op het moment dat je bestanden uit de Radar omgeving overzet naar een USB stick, ben jij er voor verantwoordelijk. Voor direct gebruik mag dit, echter, zorg er wel voor dat de bestanden na afloop weer verwijderd worden. Met collega's deel je altijd via Teams of OneDrive.

Op alle Windows laptops is het mogelijk om een USB stick of externe schijf te laten encrypten door Bitlocker. Je maakt er dan een wachtwoord voor aan. Een ontvanger met een Windows laptop kan deze dan openen. Sla dit wachtwoord netjes op en deel deze via een ander kanaal (bijv. SMS of teams) met de ontvanger nadat ze bevestigd hebben dat ze de stick hebben ontvangen, nooit bij de stick zelf. Berg anders de stick goed op en laat deze niet slingeren.

Steek nooit een onbekende, onbeheerde USB stick in je laptop. Vergelijk het met een lolly die je op de grond vindt, die steek je ook niet in je mond.

6.3 Papier

Bedenk altijd of je informatie wel echt op papier vast moet leggen:

- Uitprinten? Denk aan de bomen!
- Zou je deze info wel opschrijven in je eigen notitieblok: wat als je tas gestolen wordt?

Als het eenmaal op papier staat, bewaar het dan veilig:

- Haal je printje op bij de printer;
- Zorg dat je belangrijke papieren niet rond laat slingeren, ook niet als je even koffie gaat halen;
- Berg papier op een veilige plek op: een postvakje waar iedereen in kan is niet veilig;
- Zorg dat afsluitbare kasten dicht zijn als je weggaat en berg de sleutel goed wordt op.

Zorg voor een goede vernietiging:

- Belangrijke papieren gaan door de versnipperaar of in de blauwe afgesloten bak, niet (thuis) in de gewone papierbak;
- Gooi papieren meteen weg als ze niet meer nodig zijn, dit voorkomt dat je het vergeet (en een volle tas).

Verzend met de juiste bescherming:

- Geef het alleen af aan de juiste persoon;
- Kies de juiste verzendmethode: koerier, aangetekend of toch postzegel?

6.4 Digitaal overdragen

'Gewone' e-mail is als een briefkaart, de postbode kan hem ook lezen. Wanneer wij belangrijke bestanden moeten overdragen via het internet, dan is een gewone e-mail dus niet het juiste middel.

Hieronder staan de mogelijkheden die wel toegestaan zijn:

- Volg de instructies van de klant. Als zij bepaalde methoden als veilig verklaren, dan volgen wij.

Wanneer wij zelf verantwoordelijk zijn, gebruik dan een van de volgende methodes:

- Maak gebruik van encrypted mail (handleiding).
- We kunnen externen uitnodigen om deel te nemen aan een Team. Wanneer de ontvanger een gast is in een van onze Teams of wij bij hen, dan is dat een veilige manier om bestanden te delen. Als jij de eigenaar van een Team bent, dan ben jij verantwoordelijk voor wat de externen kunnen zien binnen het Team.
- Gebruik een versleutelde USB stick.
- File request in OneDrive en Teams (handleiding) is een veilige manier om bestanden te ontvangen van iemand.
- Indien het echt niet anders kan, maak dan gebruik van KPN Secure File Transfer, niet van WeTransfer.