voorschrift

Zakelijk gebruik ICT-diensten en voorzieningen

vastgesteld door	Afdelingshoofd ICT	datum	1-5-2020
		geldig tot	1-5-2021

Werken bij ICTU vraagt om samenwerking, flexibiliteit en vereist dat we op een vertrouwde manier met gegevens omgaan. De ICT-voorzieningen en -diensten die ICTU levert aan haar medewerkers, ondersteunen dit. ICTU beschikt over een moderne werkomgeving, waarbij medewerkers aangeboden ICT-diensten kunnen gebruiken met eigen apparatuur. De dienstverlening van ICTU staat beschreven op het Serviceplein van het ICTU-portaal.

Beleid

Om de integriteit, vertrouwelijkheid en beschikbaarheid van de ICT-diensten (inclusief de zakelijke informatie) van en bij ICTU te borgen, hanteert ICTU een door de directie vastgesteld beveiligings- en privacybeleid. Het informatiebeveiligingsbeleid van ICTU is gebaseerd op de Baseline Informatieveiligheid Overheid (BIO) en bestaat uit het strategische informatiebeveiligingsbeleid en alle operationele security afspraken, ook wel voorschrift of procedure genoemd. het ICTU privacybeleid is gebaseerd op de AVG (Algemene Verordening Gegevensbescherming). Het voorschrift zakelijk gebruikt ICT-diensten is een uitwerking van een thema van het informatiebeveiligingsbeleid.

ICTU heeft de plicht om alle medewerkers te informeren over het geldende beveiligings-beleid en de gedragsregels. Ter ondersteuning daarvan is een aantal basale gedragsregels en beveiligingsrichtlijnen voor apparatuur opgesteld om veilig te kunnen werken voor ICTU. Daarnaast is ter ondersteuning hiervan een infographic gemaakt, die als bijlage beschikbaar is. Zo moet het voor iedere medewerker helder te zijn wat de verwachtingen en afspraken zijn om te werken bij ICTU. Uitgangspunt is daarbij dat integer wordt gehandeld en men prudent omgaat met de informatie en diensten van ICTU.

Scope

Onderstaande regels zijn van toepassing op alle medewerkers (eigen en inhuur) en op alle ICT-middelen (laptops, tablets, mobiele telefoons, opslagmedia, software) die gebruikt worden tijdens het werken voor en/of bij ICTU. De regels zijn van toepassing op het werken met gegevens en diensten van of namens ICTU, ongeacht de locatie waar het werk wordt uitgevoerd. Alle door ICTU beschikbaar gestelde ICT-middelen en -diensten voldoen standaard aan de hier benoemde beveiligingsrichtlijnen.

Voorschrift

A. Algemene regels en gedrag

- **ICTU flex-werkplekken**: Om te kunnen werken bij ICTU en gebruik te kunnen maken van de beschikbaar gestelde digitale diensten, zijn een courante (courant: nog actief ondersteund door leverancier) laptop en mobiele telefoon noodzakelijk. Daarmee kan gebruik gemaakt worden van de door ICTU beschikbaar gestelde ICT-diensten en kan randapparatuur van de ICTU flex-werkplekken worden aangesloten.
  ICTU flex-werkplekken zijn standaard uitgerust met een scherm aangesloten op een USB port-replicator. Om hier gebruik van te maken dient apparatuur de Displaylink standaard te ondersteunen. Voor bepaalde functies (developers) is het werken met een (extra) tweede scherm mogelijk.
  Medewerkers in loondienst bij ICTU, kunnen desgewenst gebruik maken van een door ICTU beschikbaar gestelde laptop die aan dezelfde eisen voldoet.

- **Eigenaarschap:** De medewerker is eigenaar, dan wel hoofdgebruiker, van bij ICTU gebruikte apparatuur (laptop, tablet, telefoon).
  De medewerker gebruikt apparatuur (en bijbehorende accounts en diensten) alleen voor zichzelf en gebruikt geen gedeelde of groepsaccounts. Persoonlijke accountgegevens zijn vertrouwelijk en worden niet gedeeld of verstrekt aan derden.

- **Wissen op afstand:** ICTU behoudt zich het recht om de zakelijke ICTU-informatie en bijbehorende ICTU-accounts op afstand te wissen indien dit noodzakelijk wordt geacht, bijvoorbeeld bij verlies of diefstal. De data wordt hiermee bij voorkeur onherstelbaar gewist.
  De gebruiker dient zelf voldoende maatregelen te treffen, zodat wissen op afstand van andere data mogelijk is. De gebruiker is zelf verantwoordelijk voor het (op afstand) wissen van persoonlijke informatie op mobiele apparaten.

- **Op afstand beheren:** Apparatuur aangesloten op de ICTU-infrastructuur (ICTU flex-werkplek, govroam) mag niet op afstand worden beheerd door derden. Telemetrie of monitoring van apparatuur naar een extern systeem is niet toegestaan. Indien apparatuur van een medewerker wel door een andere partij moet worden beheerd, dan dient dit voorafgaand aan gebruik bij ICTU te worden gemeld (en vastgelegd) bij de ICTU Servicedesk. ICTU kan hier dan rekening mee houden bij de monitoring en detectie op haar netwerk. Standaard dient elke vorm van 'beheer op afstand' uitgeschakeld te zijn. Indien tijdelijk gebruik moet worden gemaakt van beheer op afstand dan is het advies gebruik te maken van een 4G-verbinding buiten het ICTU-netwerk. De gebruiker dient altijd zelf remote beheeractiviteiten te initiëren. Ook voor beheerdoeleinden dient altijd een beveiligde login gebruikt te worden.

- **Personaliseren en modificeren**: Het omzeilen of uitschakelen van de door een leverancier aangebrachte beveiligingsmaatregelen in software (zoals 'jailbreaken' of 'rooten' van telefoons) is niet toegestaan. Apparatuur mag wel gepersonaliseerd worden.

- **Privé gebruik:** Door ICTU aangeboden ICT-diensten en apparatuur (internettoegang, Office365, dataopslag, email, etc.) zijn bedoeld voor zakelijk gebruik in opdracht van ICTU; privé gebruik wordt gedoogd mits aan de beveiligingsrichtlijnen wordt voldaan en integer gehandeld wordt conform de ICTU sociale code.

- **Compliance controle:** ICTU heeft het recht om de gebruiker periodiek of steekproefsgewijs te vragen aan te tonen dat apparatuur voldoet aan de beveiligingsrichtlijnen.

B. Beveiligingsrichtlijnen

- **Minimaliseer lokale dataopslag:** Beperk lokale opslag van zakelijke informatie op een apparaat tot een noodzakelijk minimum. Randvoorwaarde voor lokale opslag is dat aan de andere beveiligingsrichtlijnen (patches en updates, malware scanning, disk/gegevensversleuteling, screenlock/schermbeveiliging en sterke wachtwoorden) is voldaan. Sla zakelijke informatie altijd minimaal op in de daarvoor beschikbaar gestelde ICTU-diensten (bijvoorbeeld SharePoint, OneDrive, Outlook). Daarmee zijn back-ups, versiebeheer en malware controle geborgd. Beperk lokale opslag van zakelijke informatie op verwijderbare media (DVD, USB, SD-card, etc.) tot een noodzakelijk minimum en gebruik daarbij altijd versleutelde opslag.

- **Versleutel gegevens:** Ondanks de minimale lokale dataopslag eis, zullen er altijd (tijdelijke) bestanden worden opgeslagen op een apparaat tijdens werkzaamheden. Daarom is aanvullend daarop volledige versleuteling van het opslagmedium van het apparaat (harddisk/SSD, usb-stick, SD-card, telefoon storage) vereist. Hiermee is de

informatie die toch aanwezig is op het apparaat alsnog beschermd in geval van bijvoorbeeld verlies of diefstal.
Indien volledige disk-encryptie niet realiseerbaar is, dient alle niet-openbare /geclassificeerde informatie te worden versleuteld, waarbij gebruik wordt gemaakt van sterke versleuteling (bijvoorbeeld AES-256). Indien er structureel wordt gewerkt met niet-openbare/geclassificeerde informatie, dan moet bij het opstarten/activeren van het apparaat altijd een handmatige ontsleuteling (pre-boot) worden gebruikt.

- **Legale software:** de medewerker is ervoor verantwoordelijk dat uitsluitend gebruik wordt gemaakt van geldige en legale (software)licenties op het betreffende apparaat. Ingehuurde ICTU-medewerkers dienen zelf te zorgen voor een geldige software licentie voor het werken met Microsoft Office documenten. ICTU stelt wel een basislicentie ter beschikking (Microsoft Office E1) om online te kunnen samenwerken met de ICTU-collega's.

  Tooling – Hackinghulpmiddelen: Standaard is het gebruik van software die als kwaadaardige software (bijvoorbeeld hack-tooling, pen-test software) kan worden aangemerkt op het netwerk NIET toegestaan. De monitoring op het netwerk en diensten van ICTU slaan aan op het gebruik hiervan en ongeoorloofd gebruik van dergelijke tooling zal worden gezien als inbreuk op de integriteit van de data- en of netwerkvoorziening. Voor bepaalde werkzaamheden in opdracht van ICTU kan het wel noodzakelijk en legitiem zijn dergelijke software te gebruiken. In die gevallen dient voor aanvang van de werkzaamheden te worden vermeld (en geregistreerd) bij de Servicedesk dat deze software gebruikt gaat worden door de verantwoordelijk projectmanager.

- **Hardening**: Wanneer een device (laptop, tablet, smartphone) verbonden is met de netwrkinfrastructuur van ICTU, is op het device uitsluitend functionaliteit actief, die noozakelijk is voor de normale werking van het device zelf of het doel waarvoor het device voor ICTU wordt gebruikt. Dit betekent dat gebruik van programmatuur die niet bijdraagt aan de werkzaamheden ten behoeve van ICTU niet is toegestaan. ICTU kan besluiten het netwerkverkeer van deze programmatuur te blokkeren.

- **Malware:** afdoende maatregelen zijn aanwezig tegen malware en virussen, zoals een geactiveerde firewall en een actieve en actuele bijgewerkte malware/virusscanner, waarbij routinematig alle aanwezige en gewijzigde bestanden worden gescand.

- **Patches en updates:** alle apparatuur die bij ICTU in een zakelijke context wort gebruikt, wordt periodiek en waar mogelijk geautomatiseerd voorzien van patches en updates (patchmanagement). Overige services en software zijn toegestaan, mits deze het functioneren van de ICTU-diensten niet nadelig beïnvloeden.
  Beveiligingsupdates en software updates worden minimaal maandelijks (automatisch) gecontroleerd en bijgewerkt. ICTU communiceert beveiligingsrichtlijnen en aanwijzingen over noodzakelijke updates of hotfixes via het ICTU Portaal, e-maill en/of Yammer. Deze aanwijzingen dienen te worden opgevolgd.
  Hier geldt een zogenaamd N-1-beleid: de software loopt maximaal een versie achter bij de meest actuele versie. Voorwaarde is dan wel dat de leverancier van de software op de gebruikte versie beveiligingsupdates levert. Wanneer het niet mogelijk is om aan dit beleid te voldoen, dan dit met redenen bij de Servicedesk geregistreerd te worden en door (een gemandateerd vertegenwoordiger van) de CISO te worden geaccepteerd.

- **Vernietigen van informatie bij uitdiensttreding:** Bij uitdiensttreding bij ICTU worden ICTU zakelijke accounts geblokkeerd en blijven afspraken over geheimhouding geldig. Alle ICTU zakelijke informatie dient voorafgaand aan uitdiensttreding te worden opgeslagen op de daarvoor bestemde ICT-diensten (ICTU SharePoint) of in digitale vorm te worden aangeleverd aan direct leidinggevende of projectleider. Vervolgens dient de

betreffende medewerker alle kopieën (lokale opslag op apparatuur, of in niet-ICTU diensten) onherstelbaar te wissen.

- **Opslag van data buiten ICTU ICT-diensten:** Zakelijke ICTU-informatie dient alleen te worden opgeslagen op de door ICTU aangeboden diensten voor veilige en beheerde opslag. Mocht er een noodzaak zijn om hiervan af te wijken, dan dient hier vooraf toestemming voor te worden gevraagd (en vastgelegd) bij de projectmanager of het afdelingshoofd. Bij opslag van informatie bij derden (zijnde niet ICTU) blijven de beveiligingsrichtlijnen op de zakelijke ICTU informatie van toepassing (versleutelde dataopslag, ook van back-ups, overeenkomstig account- en wachtwoordeisen, etc.). Daarnaast is opslag binnen de EU verplicht.

- **Gebruik veilige wachtwoorden**: Een gebruiker moet zich altijd authentiseren voordat hij een apparaat kan gebruiken (bijvoorbeeld de combinatie van een gebruikersnaam met een wachtwoord, vingerafdruk, pincode, beveiligingstoken). Gebruikte wachtwoorden horen altijd minimaal te voldoen aan de geldende wachtwoordeisen van ICTU op dat moment. Wachtwoorden van niet-ICTU diensten die wel worden gebruikt bij werkzaamheden voor ICTU voldoen aan dezelfde wachtwoord eisen.

- **Multi Factor Authenticatie**: Indien beschikbaar wordt altijd gebruik gemaakt van multifactor authenticatie(MFA) naast een gebruikersnaam en wachtwoord is bijvoorbeeld nog een code nodig. ICTU maakt voor toegang tot haar ICTU bedrijfsapplicaties en ICT-diensten gebruik van MFA. Daarvoor dient een medewerker een Microsoft Authenticator app te installeren op de mobiele telefoon die wordt gebruikt tijdens het werken bij ICTU. Alleen met behulp van deze applicatie, kan toegang worden verkregen tot data en systemen die geclassificeerde en/of niet-openbare informatie bevatten.

- **Automatische schermbeveiliging:** Onbeheerde werkplekken zijn altijd vergrendeld. Bij laptops wordt na maximaal 5 minuten inactiviteit de schermbeveiliging en/of screenlock geactiveerd. Voor mobiele telefoons is de richtlijn van een screentime-out (incl. lock) maximaal 2 minuten. Er dient altijd een wachtwoord, pincode of biometrische oplossing (vingerafdruk) gebruikt te worden om deze beveiliging op te heffen. Zorg ervoor dat de scherminhoud altijd wordt afgeschermd voor inzage door onbevoegden.

- **Veilige (wifi) netwerkverbinding:** Gebruik GOVROAM voor wifi-verbindingen indien beschikbaar. Voorkom gebruik van onbeveiligde of open wifi-verbindingen. Gebruik indien nodig 4G of een VPN-verbinding.

- **Veilige netwerkdiensten:** Gebruik zoveel mogelijk beveiligde netwerkdiensten, zoals websites met HTTPS in plaats van HTTP.
  ICTU biedt een beveiligde DNS-dienst, waarmee het bezoek aan bekend onveilige of voor ICTU-werkzaamheden onwenselijke websites wordt voorkomen. Via het Serviceplein van het ICTU-portaal en bij de ICTU ServiceDesk is meer informatie over deze dienst te krijgen.

- **Direct melden bij verlies of diefstal**: Verlies of diefstal van apparatuur, data of detectie van (digitale) inbreuk dient altijd onmiddellijk (uiterlijk binnen 24 uur) te worden gemeld bij de Servicedesk en aan je leidinggevende. Let op: dit geldt ook voor BYOD-apparaten.

- **Melden veiligheidsincidenten en/of datalekken**: meld (vermoedens van) beveiligingsincidenten en/of datalekken altijd onmiddellijk, (uiterlijk binnen 24 uur) bij de Servicedesk en aan je leidinggevende. Let op: dit geldt ook voor BYOD-apparaten.

Toetsing

Alle medewerkers van ICTU ondertekenen een akkoordverklaring op het voldoen aan de voorschriften. De administratie van de akkoordverklaringen wordt periodiek gecontroleerd. De naleving van de akkoordverklaring kan steekproefsgewijs worden getoetst door een gebruiker device te controleren.
In geval van een incident kan ICTU overgaan tot een systematische controle van devices van gebruikers.

Privacyverklaring

In verband met de beveiliging en het kunnen garanderen van de beschikbaarheid van diensten wordt het gebruik van ICTU-infrastructuur en ICT-Diensten gelogd en actief gemonitord. ICTU neemt de bescherming van jouw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. ICTU verstrekt geen verzamelde informatie aan derden, alleen indien zij daar wettelijk toe verplicht is.

Wijzigingen aan dit document

De CISO bewaakt dat jaarlijks dit document opnieuw wordt beoordeeld, waar nodig bijgesteld, om het vervolgens opnieuw te laten vaststellen. Elke nieuwe gewijzigde versie vervangt alle voorgaande documenten met betrekking tot gebruik van persoonlijke mobiele apparaten (laptop/tablet/telefoon). ICTU kondigt wijzigingen of aanvullingen aan via het ICTU Portaal / Yammer / e-mail.