Deze Richtlijn is vastgesteld door het MT IM&ICT op 11 januari 2021.

Cyberwijzer (voorheen HU-gedragsregels)

Auteur
Marcel van de Kolk

Inlichtingen
HU Dienst IM&ICT

Datum
7 oktober 2020

Versie
2.0

Versiebeheer

Versie	Datum	Auteur	Verwerking
1.0	15-07-2019	Ed de Vries	Publicatie
2.0	07-10-2020	Marcel van de Kolk (IT Security Manager)	Publicatie

Vaststelling

Versie	Versiedatum	Vastgesteld door	Rol	Vastgesteld op datum
1.0	15-07-2019	CvB	Goedkeuring en bekrachtiging	15-07-2019
2.0	07-10-2020	MT IM&ICT	Goedkeuring en bekrachtiging	11-01-2021

Inhoud

1 Inleiding

Iedereen die voor onderwijs, onderzoek of algemene bedrijfsvoering gebruik maakt van faciliteiten van de Hogeschool Utrecht, waaronder de netwerken en (ICT-)apparatuur, moet zich houden aan de door of namens het College van Bestuur gegeven gedragsregels zoals beschreven in deze Cyberwijzer, alsmede mondelinge dan wel schriftelijke aanwijzingen.

De ICT-voorzieningen worden aangeboden binnen het kader van het volgen van een opleiding of cursus, ter ondersteuning van onderzoek of ter ondersteuning van de bedrijfsvoering van de hogeschool. Het gebruik van deze voorzieningen is in principe alleen toegestaan als het ten dienste staat van deze activiteiten. Het incidenteel gebruikmaken van de ICT-voorzieningen voor privédoeleinden is toegestaan, zolang dit geen direct effect heeft op het onderwijs, onderzoek of bedrijfsvoering.

1.1 Onderhoud en ontsluiting gedragsregels

Deze gedragsregels zijn opgesteld en goedgekeurd door het MT IM&ICT en zijn een onderdeel van het InformatieBeveiligingsBeleid van de HU. Het document wordt onderhouden door de IT Security Manager als gedelegeerde van het MT IM&ICT. Deze Cyberwijzer wordt gepubliceerd op een centrale plaats (AskHU), die toegankelijk is voor iedereen voor wie deze gedragsregels van toepassing zijn.

2 Doel van deze cyberwijzer

Het instellen van deze cyberwijzer heeft tot doel om eenduidig kenbaar te maken welke regels van toepassing zijn bij het gebruik van de ICT-faciliteiten en daarmee de beschikbaarheid, stabiliteit en veiligheid van de ICT-faciliteiten te kunnen waarborgen.

Verder wordt beoogd te voorkomen dat:

- Misbruik en overbelasting van de computerfaciliteiten ontstaat;
- Onnodige vergissingen, incidenten of schade door het gebruik van de computerfaciliteiten optreedt;
- Schade aan de goede naam van de Hogeschool Utrecht wordt aangebracht.

2.1 Reikwijdte

Deze gedragsregels zijn van toepassing op iedereen die in het kader van werk of studie gebruik maakt van de ICT-voorzieningen die eigendom zijn van en ter beschikking gesteld worden door de hogeschool ten behoeve van werk of studie.

Indien de hogeschool ICT-voorzieningen ter beschikking stelt aan derden, dan zijn deze gedragsregels ook op dit gebruik van toepassing. De houder van de relatie dient deze derden op de gedragsregels te wijzen.

2.2 Goedkeuring, evaluatie en wijziging cyberwijzer

Het HU College van Bestuur accordeert de cyberwijzer dat door IM&ICT wordt voorgedragen. De cyberwijzer volgt de kaders van het HU-beleid en wordt iedere 3 jaar herzien, of tussentijds na substantiële verandering van het HU beleid of significante ontwikkelingen op ICT-vlak.

3 Controle op naleving

Als er een vermoeden is dat in strijd met deze gedragsregels wordt gehandeld dan wordt de leidinggevende van de medewerker daarover ingelicht, zodat deze de medewerker daarop kan aanspreken. Betreft het een student, dan kan de docentbegeleider of een medewerker van IM&ICT de student daarover aanspreken.

Indien er een vermoeden is van opzettelijk afwijken van de gedragsregels kan HU-CERT een onderzoek instellen naar het handelen van de medewerker/student. Indien opzet kan worden aangetoond kunnen disciplinaire maatregelen volgen.

4 ICT gedragsregels

Hogeschool Utrecht heeft de volgende gedragsregels gedefinieerd voor veilig gebruik van de HU ICT-voorzieningen.

4.1 Ga zorgvuldig en vertrouwelijk met je wachtwoord om

Wat	Je wachtwoord(en) zijn je toegang tot het netwerk, internet, diverse applicaties en data. Het verlies of diefstal hiervan kan zowel voor de HU als voor jou persoonlijk grote problemen opleveren.
Hoe	• Het HU account is persoonlijk en mag niet met iemand anders worden gedeeld. • Bewaar deze credentials zorgvuldig en deel ze met niemand. • Gebruik in plaats van moeilijk te onthouden wachtwoorden een wachtzin. Die zijn veel gemakkelijker te onthouden en moeilijker te kraken. • Binnen het HU domein gebruiken we Single-Sign-On voor een deel van de applicaties. Voor het overige deel van de applicatie wordt aangeraden om voor verschillende applicaties/website verschillende wachtwoorden te hanteren. Om ze gemakkelijker uit elkaar te kunnen houden kan je (een deel van) de naam van de applicatie/website in het wachtwoord opnemen. • Gebruik wachtwoorden/zinnen niet voor een tweede keer. • Maak gebruik van de door HU aangeboden wachtwoordmanager. • Leen je credentials nooit uit aan anderen. Ze zijn strikt persoonlijk uitgegeven en horen bij jouw rol. Collega's of medestudenten hebben hun eigen credentials, en je kunt niet weten wat iemand uit jouw naam van plan is. • Systeembeheerders en/of helpdeskmedewerkers zullen nooit om jouw credentials vragen. • Als je vermoedt dat er op welke wijze dan ook misbruikt gemaakt wordt van je account, meld dit dat z.s.m. bij de Centrale Service Desk (CSD) of HU-CERT. Die kunnen dan actie ondernemen om misbruik zoveel mogelijk te beperken. • Wachtwoorden mogen niet op memoblaadjes worden geschreven en op een monitor of onder het toetsenbord worden geplakt. Ook mogen deze niet worden bewaard in een algemeen toegankelijke locatie.

4.2 Voorkom misbruik en diefstal

Wat	Voorkom diefstal en misbruik van HU devices en ga er minimaal net zo voorzichtig mee om als met je persoonlijke eigendommen.
Hoe	• Zet minimaal een toegangscode op je (HU) telefoon en maak gebruik van sterke wachtwoorden.

	• Bewaar je gegevens niet op het device zelf maar op een share/schijfruimte die via de HU wordt aangeboden. Daar is je data veiliger en in geval van diefstal van je device is deze niet direct beschikbaar voor de dief. • Neem geen data/gegevens van de HU mee op papier of externe datadragers. De HU biedt een platform aan waarop je de data veilig kunt bewaren en deze kan via VPN worden benaderd. Het meenemen van deze data is dus niet nodig en kan alleen maar leiden tot verlies. • Laat HU devices niet in je auto achter. Criminelen rijden rond over de parkeerplaats en scannen op aanwezige apparatuur in geparkeerde auto's. Het kost ze echt slechts 1 minuut om je device te stelen. • Laptops die aan het einde van de werkdag niet mee naar huis worden meegenomen, dienen te worden opgeborgen in een afgesloten kast/lade.

4.3 Houd je devices up-to-date

Wat	Veel devices worden kwetsbaar voor cyberaanvallen doordat ze niet up-to-date zijn. In oudere software worden vaak kwetsbaarheden (ofwel 'gaten/lekken') gevonden waardoor een systeem gemakkelijker te hacken wordt.
Hoe	• Installeer altijd de laatste beveiligingsupdates en patches die verschijnen voor jouw devices. • Wees voorzichtig met het installeren van gedownloade software. Zorg in ieder geval dat je een licentie voor de software hebt. • Installeer zeker geen illegale software op je device. • Medewerker devices in beheer van de HU zijn voorzien van standaard software, en kunnen software uit de beschikbare catalogus installeren. Eigen downloads zijn daardoor niet nodig. Indien er software gewenst is die niet in de catalogus voorkomt kan deze via de CSD worden aangevraagd. • Denk goed na over het gebruik van online-tools. Zijn deze wel veilig, en wat gebeurt er met de data die je erin verwerkt? • Zorg voor een goede virusscanner op je device (op HU devices wordt hierin voorzien)

4.4 Houd je vertrouwelijke data veilig

Wat	Als je werkt met data die een vertrouwelijk karakter draagt (ook in het kader van privacy) is het zaak om die ook vertrouwelijk te houden, en ervoor te zorgen dat die niet 'op straat' komt te liggen.
Hoe	• Medewerkers zijn verplicht om te zorgen dat ALLE gevoelige/vertrouwelijke informatie in hardcopy of elektronische vorm in hun werkomgeving veilig is, en opgeruimd bij het verlaten van de werkplek en aan het einde van de werkdag. • Bewaar persoonsgegevens niet langer dan nodig voor het doel waarvoor je ze gekregen hebt. • Indien je in een openbare ruimte werkt met vertrouwelijke data en/of persoonsgegevens, voorkom dan dat mensen mee kunnen lezen op het scherm (gebruik een screenprotector). • Wanneer je buiten de HU werkt, maak dan altijd verbinding met het HU-netwerk via VPN (medewerkers). Op die manier kan je veilig met de HU applicaties werken en je data veilig opslaan zonder het risico van inbreuk. • Vergrendel altijd je scherm als je wegloopt van je device (in Windows ⊞ + L) • Als je vertrouwelijke data wilt opslaan, doe dat dan op de door de HU gefaciliteerde opslagruimte.

	• Verstuur vertrouwelijke data niet zomaar via email. Email is geen veilig medium, dus vertrouwelijke informatie die echt verstuurd moet worden kan je het best sturen via vertrouwelijke kanalen zoals via SURF-filesender. Daarbij heb je de optie om je data te versleutelen. Intern binnen de HU is het verstandiger de data niet te versturen maar op een plaats op te slaan waar je het bestand kunt delen. • Aan het einde van de werkdag dient alle gevoelige/vertrouwelijke informatie van de werkplek te worden verwijderd en opgeborgen in een afgesloten kast/lade. • Kasten en lades met opslag van gevoelige/vertrouwelijke dienen te allen tijde op slot te zijn. • Sleutels van afgesloten kasten/lades mogen niet onbeheerd op de werkplek liggen. • Documenten met gevoelige/vertrouwelijke informatie moeten worden weggegooid in een speciale afgesloten container die bedoeld is voor vernietiging of door een papierversnipperaar worden gehaald. • Documenten met gevoelige/vertrouwelijke informatie mogen niet op de printer achterblijven. • Whiteboards waarop gevoelige/vertrouwelijke informatie is geschreven dienen aan het einde van de meeting/vergadering te worden schoongeveegd. • Devices voor (massa)opslag van data zoals CD, DVD en USB-drives moeten altijd worden behandeld als vertrouwelijke informatie en worden opgeborgen in een afgesloten kast/lade.

4.5 Wees behoedzaam bij email-gebruik

Wat	Email is een krachtig medium, gebruik het verstandig.
Hoe	• Het aan jou verstrekte emailadres is persoonlijk en niet overdraagbaar. • Je bent zelf verantwoordelijk voor het beheer van je email box. • Het gebruik van het verstrekte HU emailadres is puur voor zakelijk gebruik, niet voor privédoeleinden. • Het is de gebruiker van de HU email faciliteiten niet toegestaan deze te gebruiken voor zaken die wettelijk niet zijn toegestaan • Het versturen van bulk-email (grote hoeveelheden email tegelijk) is standaard niet toegestaan, zonder voorafgaande toestemming vanuit IM&ICT.

4.6 Ga zorgvuldig om met social media

Wat	Voor het omgaan met social media gelden regels met betrekking tot de security & privacy.
Hoe	• Het is gebruikers van HU ICT-faciliteiten niet toegestaan ongevraagd vertrouwelijke- en/of persoonsgegevens of andere informatie over Hogeschool Utrecht en haar medewerkers, studenten, dienstverleners etc. te publiceren. • Gebruikers zijn persoonlijk verantwoordelijk voor de inhoud die ze, voor zover dat niet tot hun functie behoort, publiceren op blogs, fora en andere media. Zij zijn zich ervan bewust dat wat zij publiceren voor langere tijd openbaar zal zijn, en dat men de controle over de inhoud van de publicatie kwijt is. • Bij de geringste twijfel over een publicatie of over de raakvlakken met Hogeschool Utrecht is het verstandig hierover contact te zoeken met je leidinggevende of de Security Officer.

4.7 Surf discreet

Wat	Weet wat je doet op internet, en houdt het gebruik ervan zoveel mogelijk zakelijk of zover nodig voor studiedoeleinden.
Hoe	• Bekijk of verzamel geen informatie die in strijd is met de wet of de goede zeden (o.a. pornografisch materiaal) via HU ICT-faciliteiten (hieronder valt ook de internetverbinding van de HU). • Download en installeer geen software of andere zaken die auteursrechtelijk zijn beschermd en waarvoor je geen rechten/licentie hebt verkregen. • Verspreid op internet geen data of overige informatie die de goede naam van de HU kan aantasten. • Het is een gebruiker niet toegestaan zich toegang te verschaffen tot niet-openbare bronnen (bijv. hacken) of toegangsrechten van de HU te misbruiken en hierdoor deze bronnen aan anderen ter beschikking te stellen.

4.8 Meld incidenten direct

Wat	Als je vermoedt dat je account wordt misbruikt, je een phishingmail hebt ontvangen of iets anders verdachts gezien hebt, meld dit dan direct bij de CSD of HU-CERT.
Hoe	• Heb je een phishing mail gekregen en herkend? Stuur dan een mail naar HU-CERT met in de ***BIJLAGE*** de phishingmail die je hebt gekregen. (niet 'doorsturen' dus !) Op deze wijze kan het HU-CERT maatregelen nemen om (verdere) problemen voorkomen. • Heb je per ongeluk toch op een link geklikt waarvan je vermoedt dat dit uiteindelijk toch niet veilig was? Schroom niet en meld dit direct bij HU-CERT. Mogelijk kunnen zij de gevolgen nog beperken door snel maatregelen te treffen. • Vermoed je andere zaken die niet in de haak zijn? Meld ze bij de CSD of HU-CERT.

4.9 Gebruik je gezond verstand

Wat	Blijf gewoon nadenken bij wat je doet. Lijkt iets te mooi om waar te zijn? Dan is het dat meestal ook.
Hoe	• Wees terughoudend in het verstrekken van persoonlijke informatie. • (Dubbel) Check altijd de betrouwbaarheid van een persoon of website als je die niet kent. • Vertrouw je iets niet? Ga er dan niet op in of vraag advies.

Bijlage 1 Begrippenlijst

Begrip:	Uitleg:
HU-CERT	Het Computer Emergency Response Team van de HU, voor de eerste hulp bij incidenten op het gebied van CyberSecurity, bereikbaar via hu-cert@hu.nl of via een melding aan de CSD.
CSD	Centrale Service Desk van de HU, bereikbaar via helpdesk@hu.nl of 088 – 481 66 66
Device	Hieronder verstaan we elk apparaat waarop gebruik kan worden gemaakt van (door HU gefaciliteerde) ICT-componenten zoals software, internet etc.
Privacydesk	Het meldpunt voor je vragen over privacy gerelateerde zaken en het doen van (vermeende) datalekken. Mail naar askprivacy@hu.nl