

Bijlage 1 van het arbeidsreglement van Odisee vzw: Richtlijnen en toezicht inzake het gebruik van de ICT-middelen aan de hogeschool (versie 17 april 2023)

Situering

De hogeschool heeft de bevoegdheid om **richtlijnen** vast te stellen voor het gebruik en het toezicht erop van de ICT-middelen die zij ter beschikking stelt van haar personeelsleden en van andere gebruikers.

De stuurgroep informatieveiligheid (verder “de stuurgroep” genoemd) waakt over de uitvoering van deze richtlijnen: zo zal de stuurgroep samenkomen telkens een actualisering van de richtlijn zich opdringt of telkens er twijfel rijst over de uitvoering ervan.

De stuurgroep wordt als volgt samengesteld: De CISO¹ en de DPO², het diensthoofd Informatiebeheer, en een vaste vertegenwoordiger p r bedrijfsdomein.

Het toezicht op het gebruik van de ICT-middelen is geregeld in punt 10. Voor personeelsleden met een arbeiders- of bediendestatuut geldt hier in het bijzonder CAO nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online- communicatiegegevens. Omwille van de transparantie is het aangewezen om ook voor de andere personeelsleden deze CAO te volgen.

De CAO bepaalt dat controle door de werkgever op het gebruik van de online communicatiemiddelen door de werknemers toegestaan is. De controle moet wel gebeuren op een wijze die de inmenging in de persoonlijke levenssfeer tot een minimum beperkt.

De organisatie van het toezicht moet volgens CAO nr. 81 niet goedgekeurd worden op de Ondernemingsraad, maar deze moet wel geïnformeerd worden en vervolgens ook de individuele personeelsleden. Overeenkomstig artikel V.244. van de Codex Hoger Onderwijs moet het Hogeschoolonderhandelingscomité geïnformeerd worden over de werking en de organisatie van de hogeschool, en daaronder kan ook de organisatie van het toezicht begrepen worden.

Om een werkbaar instrument te cre ren, werd gekozen voor   n tekst die zowel de richtlijnen als het toezicht bevat en die geldt voor alle gebruikers, zowel personeelsleden, studenten als externen. De tekst vormt tevens de noodzakelijke uitwerking van de principes inzake gebruik en toezicht, zoals opgenomen in de geldende arbeidsreglementen.

¹ De CISO is verantwoordelijk voor het ontwikkelen, adviseren en handhaven van het informatieveiligheidsbeleid binnen de organisatie, inclusief het cre ren van bewustzijn bij medewerkers over het beleid.

² De DPO (Data Protection Officer) is de functionaris voor gegevensbescherming, belast met het toezicht houden op de naleving van de AVG-regelgeving binnen de organisatie.

Mogelijke sancties bij overtreding van de richtlijnen door personeelsleden zijn de sancties opgenomen in het arbeidsreglement (voor benoemde personeelsleden spreken we over tuchtmaatregelen). Voor studenten is er een koppeling met het onderwijs- en examenreglement en met het tuchtreglement dat de tuchtprocedure en de tuchtsancties bevat.

Dat betekent dat:

- De organen die daartoe in het tuchtreglement worden aangeduid, bevoegd zijn om ordemaatregelen op te leggen ten aanzien van de student, om met de student te spreken en om tuchtmaatregelen ten aanzien van de student op te leggen zoals voorzien in de tuchtprocedure;
- De personeelsdirecteur bevoegd is voor het gesprek met het personeelslid dat moet plaatsvinden vóór iedere beslissing die het personeelslid individueel kan raken, en dat de personeelsdirecteur of de algemeen directeur een sanctie of tuchtmaatregel kan nemen ten aanzien van het personeelslid;
- De directeur algemeen beheer of een ander lid van het directiecomité bevoegd is voor externe gebruikers (zowel voor het gesprek als voor de beslissing tenzij de beslissing behoort tot de bevoegdheid van de afgevaardigd bestuurder).

1 Doel en toepassingsgebied

De hogeschool stelt ICT-middelen ter beschikking voor educatieve, wetenschappelijke, administratieve en communicatieve doeleinden. Het gebruik ervan wordt sterk aangemoedigd voor het verbeteren van de kwaliteit van de kernactiviteiten van de instelling: onderwijs, onderzoek en maatschappelijke dienstverlening. De hogeschool beslist autonoom welke ICT-middelen ondersteund worden.

De naleving van de hiernavolgende regels waarborgt een waardig, gedisciplineerd en veilig gebruik van deze ICT-middelen.

Deze richtlijnen gelden voor alle personeelsleden, externen met ICT-faciliteiten van de hogeschool, en voor de studenten ingeschreven aan de hogeschool. Hierna worden zij gezamenlijk aangeduid als de gebruiker(s).

De gebruiker is er zich van bewust dat de hogeschool het netwerkgedrag van alle ICT-middelen logt en dat de hogeschool de goede werking van de netwerken kan controleren op basis van die logs. Deze controles gebeuren binnen de geldende wettelijke omgeving.

Personeelsleden die voor de uitoefening van hun professionele werkzaamheden aan de hogeschool geen ICT-middel voorhanden hebben, hebben het recht om hun e-mailadres van de hogeschool en het personeelsportaal van de hogeschool regelmatig te raadplegen op de werkplaats. Hierover worden afspraken gemaakt tussen deze personeelsleden en hun leidinggevende.

De richtlijnen gelden voor alle ICT-middelen, IT-infrastructuur en elektronische communicatiemiddelen en voor alle gegevens die door die systemen worden verzonden of erin worden opgeslagen. Ze gelden dus ook voor eigen ICT-middelen die in relatie / combinatie met de hogeschool gebruikt worden (bijvoorbeeld e-mailadres van de hogeschool, toegang tot het Wi-Fi netwerk op de campussen, ...).

De stuurgroep informatieveiligheid waakt over de uitvoering van de richtlijnen. Aangezien ICT-middelen en de wettelijke omgeving steeds evolueren, zal de stuurgroep samenkomen om de richtlijnen te toetsen en zo nodig aan te passen telkens de gewijzigde omstandigheden dit vereisen. Het aangepaste document zal aan de gebruikers worden meegedeeld via de URL: odisee.be/reglementering.

Vragen, opmerkingen en suggesties in verband met deze richtlijnen kunnen gericht worden aan de voorzitter van de stuurgroep informatieveiligheid via het e-mailadres: CISO@odisee.be.

2 Omgaan met informatie

De toegang tot de informatiebronnen van de hogeschool wordt verleend op een need-to-know basis, waarbij de gebruiker enkel toegang krijgt tot de informatie die noodzakelijk is voor de uitvoering van zijn functionele rol binnen de hogeschool. De toegangsrechten zijn individueel en niet overdraagbaar.

Het is de taak van de eigenaar van de informatie om er op toe te zien dat de toegangsrechten correct zijn ingesteld. Aan de eigenaar wordt gevraagd om op regelmatige basis een evaluatie te maken van de toegangsrechten waarvoor hij/zij verantwoordelijk is. Gebruikers die merken dat ze toegang hebben tot informatie waarvoor ze niet gemachtigd zouden moeten zijn, moeten dit melden aan de eigenaar en/of de dienst Information Management.

Elke gebruiker is verantwoordelijk voor het correct omgaan met de informatie die hij/zij beheert, verwerkt en opvraagt.

Bepaalde informatie van de hogeschool is vertrouwelijk en moet met bijzondere aandacht worden benaderd. Om te bepalen in welke mate informatie vertrouwelijk is, moet men zich afvragen wat het risico is voor de hogeschool bij een ongepaste verspreiding, zoals:

1. Het verlies van economische waarde, bijvoorbeeld informatie over de ontwikkeling van nieuwe diensten, onderzoeksgegevens of meer algemeen informatie, ongeacht de vorm waarin deze is opgeslagen, waarvan de hogeschool rechthebbende is;
2. De aantasting van het imago van de hogeschool, bijvoorbeeld door de verspreiding van gevoelige informatie die leidt tot negatieve publiciteit;
3. Een inbreuk op de wetgeving ter bescherming van de intellectuele eigendomsrechten, in het bijzonder de auteursrechten, octrooien, merkenrecht;
4. Een inbreuk op de verordening van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene Verordening Gegevensbescherming (AVG)).

- Salaris- en andere betalingsgegevens, gegevens betreffende personeels- en studentenadministratie, medische persoonsgegevens, toetsen / examenopgaven, examenresultaten, e.a. zijn persoonsgegevens in de zin van deze verordening;
5. Een inbreuk op een andere wetgeving;
 6. Overdracht van informatie afkomstig van derden waarmee een akkoord van niet-verspreiding werd afgesloten.

Vertrouwelijkheid van informatie geldt als uitgangspunt. Ook informatie die niet uitdrukkelijk als vertrouwelijk bestempeld wordt, mag niet zomaar openbaar of publiek gesteld worden. Bij twijfel kan advies worden ingewonnen bij de stuurgroep informatieveiligheid en/of de juristen van de hogeschool.

Vertrouwelijke informatie of andere informatie die essentieel is voor de werking van de hogeschool dient opgeslagen en verwerkt te worden in de Cloud van de hogeschool (de hogeschool maakt standaard gebruik van Office 365), en niet op de lokale harde schijf van de pc/werkstation, tenzij voor tijdelijk offline gebruik. Hierdoor kan er een back-up van de gegevens worden gemaakt, waardoor het risico op dataverlies beperkt blijft.

Informatie die is opgeslagen in de Cloud van de hogeschool kan en mag gedeeld worden, maar enkel met de gebruikers die recht hebben op de toegang tot de informatie.

Het is niet toegestaan om vertrouwelijke informatie of andere informatie die essentieel is voor de werking van de hogeschool op te slaan op een niet-ondersteunde opslagdienst, zoals bv. de Dropbox, Google Drive en Apple iCloud. Het is ook niet toegestaan om deze informatie te verzenden met behulp van een niet-ondersteunde instant messaging-technologie, zoals bv. WeTransfer, WhatsApp en Messenger, of te posten op sociale netwerken.

Het omgaan met vertrouwelijke informatie of andere informatie die essentieel is voor de werking van de hogeschool vanop een extern, niet door de hogeschool ondersteund, ICT-middel zoals een thuis-pc, laptop, tablet, smartphone of persoonlijk USB-apparaat (geheugenstick, mobiele harde schijf, enz.), ook wel “bring your own device” genoemd, is onderhevig aan gedragsregels. Deze regels worden in sectie 5 van dit document in detail beschreven. Gevoelige persoonsgegevens, meer bepaald ras of etnische afkomst; politieke opvattingen; religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond; genetische gegevens (DNA-analyse) ; biometrische gegevens met het oog op unieke identificatie; gezondheidsgegevens; gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid; persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, mogen nooit op een extern apparaat verwerkt worden. Bij vernietiging of hergebruik van een extern apparaat, moet erop gelet worden dat het geen informatie van de hogeschool meer bevat.

Bij het gedeeld gebruik van een pc/werkstation dient de gebruiker passende voorzorgmaatregelen te nemen om de informatie te beschermen waartoe de medegebruiker(s) mogelijk geen toegang heeft.

Afdrukken en kopieën van vertrouwelijke informatie moeten onmiddellijk worden opgehaald.

Op het internet (vb. sociale media), op persoonlijke webpagina's en blogs, mag geen informatie onderhevig aan copyright van de hogeschool of vertrouwelijke informatie over andere gebruikers of over de hogeschool worden vrijgegeven tenzij hiervoor een uitdrukkelijke, voorafgaande schriftelijke toelating is gegeven.

Indien informatie waarin persoonsgegevens vervat zitten, ongeoorloofd en onbedoeld bij derden terechtkomt, ongewenst wordt vernietigd, verloren, gewijzigd of verstrekt aan derden, dient de gebruiker onmiddellijk het datalek te melden via de URL: gdpr.odisee.be of het e-mailadres privacy@odisee.be.

3 Gebruikers-ID en wachtwoord

De toegang tot de ICT-faciliteiten, diensten en applicaties van de hogeschool verloopt via geautoriseerde kanalen. Er wordt hierbij gebruik gemaakt van een centraal toegewezen gebruikers-ID, die is gekoppeld aan de naam van de gebruiker, en authenticatiemethoden, inclusief een wachtwoord dat voldoet aan de beleidsvereisten en het gebruik van multifactor authenticatie.

Multifactor authenticatie is een methode die een extra beveiligingslaag creëert bovenop de gebruikers-ID en wachtwoord. Het werkt door een aanvullende verificatie te vereisen voordat er toegang tot gegevens en/of IT-bronnen wordt gegeven. De extra verificatie helpt om de account van de gebruiker te beschermen in het geval het wachtwoord gecompromitteerd is.

Het is de verantwoordelijkheid van de gebruiker om passende voorzieningen te treffen om multifactor bevestigingscodes te ontvangen via een authenticatie-app op de smartphone, sms, of uitzonderlijk via een hardware-token.

Wachtwoorden, inclusief persoonlijke identificatienummers (PIN's), hardware tokens of soortgelijke informatie of apparaten die worden gebruikt voor identificatie- en autorisatiedoeleinden mogen niet worden gedeeld en zijn niet overdraagbaar. De gebruikers zijn verantwoordelijk voor het gebruik van hun gebruikers-ID en wachtwoord. Wachtwoorden voor digitale certificaten die voor digitale handtekeningen worden gebruikt, mogen aan niemand worden bekendgemaakt. Wachtwoorden mogen niet in zichtbare (post-it, ...) vorm worden opgeslagen, en het ingeven van wachtwoorden moet met de nodige voorzichtigheid gebeuren (vb. niet als iemand toekijkt).

Alle ICT-systemen moeten worden beschermd met een opstart-wachtwoord en een schermbeveiliging om de inhoud van de gegevens zo optimaal mogelijk te beveiligen. Aan de gebruikers wordt gevraagd om het invoeren van hun wachtwoord niet te omzeilen door gebruik te maken van automatisch inloggen, ingesloten scripts of hard-code wachtwoorden in de programmatuur. Voor specifieke toepassingen, zoals bv. geautomatiseerde back-ups, kan er

door de dienst Information Management een uitzondering gemaakt worden. Elke uitzonderingssituatie moet voorzien worden van een procedure voor het wijzigen van de wachtwoorden en moet voldoen aan het beveiligingsbeleid voor het maken van wachtwoorden.

Voor sociale media en netwerken voor persoonlijke doeleinden moet de gebruiker een gebruikers-ID en wachtwoord gebruiken die verschillend is van de login en het wachtwoord van de hogeschool.

4 Verantwoordelijkheden van de gebruiker

De gebruiker verbindt er zich toe om elk slecht functioneren of misbruik van ICT-middelen, IT-infrastructuur en elektronische communicatiemiddelen, of lacunes in de beveiliging, onmiddellijk via de gekende kanalen te melden aan de dienst Information Management.

De gebruiker die merkt dat hij/zij toegang heeft tot informatie waarvoor hij/zij niet gemachtigd is, meldt dit onmiddellijk aan de dienst Information Management.

De gebruiker verbindt er zich toe om de door de hogeschool voorziene beveiligingsmiddelen te gebruiken en de opgelegde beveiligingsmaatregelen toe te passen (vb. wijziging van wachtwoord).

De gebruiker behandelt alle informatica-infrastructuur met de noodzakelijke zorg en voorzichtigheid. Alleen laptops en hun mobiele randapparatuur mogen door de gebruiker verplaatst worden, tenzij toelating wordt gegeven voor verplaatsing van andere infrastructuur. Het is verplicht om alle apparatuur van de hogeschool aan het einde van het dienstverband of gebruiksperiode te retourneren.

Van de gebruiker wordt verwacht dat hij/zij het juiste ICT-middel voor het juiste doel inzet, afhankelijk van de omstandigheden, bijvoorbeeld:

1. Interne Unified Communications-middelen (o.a. IP-telefonie, videoconferentie, Instant Messaging,...) te gebruiken als deze aanwezig zijn i.p.v. GSM's/Smartphones te gebruiken binnen de werkomgeving;
2. Enkel interne Unified Communications-middelen naar GSM's/Smartphones doorschakelen als dit noodzakelijk is;
3. Enkel inbellen op conferentienummers vanop GSM's/Smartphones wanneer er geen lokaal nummer aanwezig is om mee in te bellen;
4. Het interne netwerk gebruiken als dit mogelijk is i.p.v. dataverbindingen via mobiele netwerken (o.a. 4G-verbindingen,...).

De gebruiker dient voldoende veiligheidsmaatregelen te nemen om de mogelijkheid tot het inbreken op de systemen van de hogeschool en diefstal van informatie zo klein mogelijk te maken, bijvoorbeeld door:

1. Het veilig opbergen van de pc bij afwezigheid;

2. Het handmatig uitloggen van de pc/werkstation (door gebruik van de toetsencombinaties CTRL-ALT-DEL of WINDOWS-L) bij het verlaten van de werkplek;
3. In voorkomend geval het fysiek beveiligen van de ICT-middelen door ze te vergrendelen met een vergrendelingskabel, of op te bergen in een lade of kast wanneer de ruimte onbeheerd is.

De gebruiker dient de veiligheid van de gegevens die hij verwerkt en/of bewaart te vrijwaren van virussen en andere kwaadaardige programmatuur, in het bijzonder door:

1. De geïnstalleerde virusscanner niet uit te schakelen;
2. Voorzichtig om te gaan met e-mails waarin om inloggegevens of andere informatie wordt gevraagd, en ze desgevallend te rapporteren;
3. Verdachte bestanden of koppelingen niet te openen of aan te klikken, en ze desgevallend te rapporteren;
4. Programmatuur en gegevens verkregen via een extern netwerk of via draagbare media te controleren op virussen en andere kwaadaardige software;
5. Geen programmatuur van illegale of twijfelachtige oorsprong te installeren;
6. Enkel programmatuur te installeren of gebruiken op het ICT-middel waarvoor de nodige licenties of gebruiksafspraken aanwezig zijn.

Bij het vermoeden van een veiligheidsinbreuk dient het ICT-middel onmiddellijk van het netwerk verwijderd te worden. en dient de servicedesk verwittigd te worden.

Wanneer noodzakelijk (vb. bij diefstal of verlies) mag de hogeschool alle of gedeeltelijke toegangen van de ICT-middelen die aangesloten zijn op het netwerk van de hogeschool, blokkeren. Zo nodig mogen data en applicaties op deze ICT-middelen gewist worden vanop afstand en mogen de toestellen onbruikbaar gemaakt worden. Bij externe ICT-middelen (BYOD) die geen eigendom zijn van de hogeschool, gebeurt dit in samenspraak met de eigenaar van het ICT-middel.

Wanneer dit om organisatorische, technische of wettelijke redenen vereist is, kan de hogeschool de toegang tot bepaalde websites, apps, betaalnummers en (interne en externe) toegangen afsluiten, al dan niet tijdelijk.

5 Bring your own devices (BYOD)

Voor externe, niet door de hogeschool ondersteunde, ICT-middelen zoals thuis-pc's, laptops, tablets, smartphones of persoonlijke USB-apparaten (geheugenstick, mobiele harde schijf, enz.), hierna "bring your own devices" of BYOD genoemd, is de eigenaar/gebruiker volledig en uitsluitend verantwoordelijk. Deze verantwoordelijkheid geldt voor de implementatie van de noodzakelijke beveiliging, back-up en restore, verlies en diefstal, het onderhoud en het beheer van het apparaat en de informatie opgeslagen op het apparaat.

Gebruikers die vertrouwelijke informatie of andere informatie die essentieel is voor de werking van de hogeschool raadplegen of verwerken op een BYOD dienen volgende

gedragsregels in acht te nemen. Gebruikers die deze gedragsregels niet kunnen implementeren, vermijden het gebruik van BYOD voor vertrouwelijke informatie of andere informatie die essentieel is voor de werking van de hogeschool.

1. Algemene gedragsregels voor het omgaan met informatie op een BYOD:
 - a. Gevoelige persoonsgegevens zoals hoger vermeld mogen nooit worden verwerkt op een BYOD;
 - b. Beperk zoveel mogelijk het bewaren van vertrouwelijke of essentiële informatie op deze apparaten, zowel in volume als in tijd;
 - c. Beperk zo veel mogelijk de opname van vertrouwelijke of essentiële informatie in e-mails;
 - d. Maak uzelf vertrouwd met de beveiligingsmogelijkheden van het apparaat en configureer adequate beveiligingsfuncties op het apparaat;
 - e. Beveilig de toegang tot het apparaat met een toegangscode, wachtwoord of biometrische toegangsbeveiliging;
 - f. Houd de software van het apparaat actueel en installeer steeds de laatst beschikbare software updates;
 - g. Gebruik enkel officiële software op het apparaat en vermijd software van dubieuze herkomst;
 - h. Neem maatregelen om verlies of diefstal van het apparaat zoveel mogelijk te voorkomen en verwittig de servicedesk bij effectief verlies of diefstal;
 - i. Doe een fabrieksreset³, ook wel harde reset of masterreset genoemd, van het apparaat wanneer het overgedragen wordt aan een ander gezinslid of een derde partij waardoor alle informatie op het apparaat gewist wordt.
2. Specifieke gedragsregels voor het omgaan met informatie op een BYOD van het type pc/workstation of laptop:
 - a. Installeer steeds een virusscanner en houd de virusdefinities actueel;
 - b. Maak er een gewoonte van om het apparaat handmatig te vergrendelen of uit te loggen bij het verlaten van de werkplek;
 - c. Encrypteer alle vertrouwelijke en essentiële informatie afkomstig van de hogeschool die wordt opgeslagen op het externe apparaat (bv. door het activeren van BitLocker op een Windows computer).
3. Specifieke gedragsregels voor het omgaan met informatie op een BYOD van het type tablet of smartphone:
 - a. Configureer het apparaat zodat slechts een beperkt aantal verkeerde toegangscode's of paswoorden kunnen worden ingegeven voordat het gebruik van het apparaat (minstens tijdelijk) wordt geblokkeerd;
 - b. Zorg ervoor dat het apparaat is uitgerust met een door de fabrikant ondersteund besturingssysteem dat regelmatig wordt gepatcht en bijgewerkt;
 - c. Encrypteer, waar mogelijk, de inhoud van het apparaat;

³ Een fabrieksreset van een apparaat betekent dat alle persoonlijke gegevens, instellingen en applicaties die op het apparaat zijn opgeslagen, worden verwijderd en het apparaat teruggezet wordt naar de fabrieksinstellingen.

- d. Verwijder vertrouwelijke e-mails zodra die niet meer nodig zijn op het apparaat;
 - e. Stel de e-mail applicatie van het apparaat zo in dat enkel Odisee e-mails van een beperkte periode worden gesynchroniseerd en opgeslagen op het apparaat;
 - f. Wijzig alle paswoorden van Odisee e-mail en andere Odisee diensten (Office 365 account, enz.) die het apparaat gebruikte ingeval het apparaat wordt gestolen of verloren gaat;
 - g. Configureer, waar mogelijk, het apparaat met een remote-wipe⁴ functionaliteit, zodat bedrijfs-gerelateerde informatie op afstand kan worden gewist in het geval dat het apparaat wordt gestolen of zoekraakt en verwittig de servicedesk bij effectief verlies of diefstal.
4. Specifieke gedragsregels voor het omgaan met informatie op persoonlijke USB-apparaten (memory sticks, mobiele harde schijven, enz.)
- a. USB apparaten waarop vertrouwelijke en essentiële gegevens worden opgeslagen, moeten integraal geëncrypteerd worden.

BYOD waarvan is vastgesteld dat ze niet voldoen aan de minimale IT-normen of anderszins een bedreiging vormen voor de informatiebeveiliging van de hogeschool, kunnen zonder voorafgaande kennisgeving van het netwerk losgekoppeld worden.

6 Persoonlijk gebruik van ICT-middelen van de hogeschool

Bij persoonlijk gebruik blijven de richtlijnen voor het gebruik van de ICT-middelen aan de hogeschool van kracht.

Enkel voor personeelsleden-gebruikers: de hogeschool laat het persoonlijke gebruik toe van haar ICT-middelen voor zover dit geen nadelige invloed heeft op de arbeidsprestaties die van de gebruiker worden verwacht. Het gebruik wordt fiscaal en sociaal aangegeven als een voordeel alle aard. Enkel wanneer een personeelslid zelf aangeeft de ICT-middelen absoluut niet ten persoonlijke titel te gebruiken worden ICT middelen niet als VAA aangegeven. Persoonlijk gebruik is in principe verboden tijdens de arbeidstijd.

Enkel voor studenten-gebruikers: er wordt altijd voorrang verleend aan studiedoeleinden in het gebruik van de gemeenschappelijk ter beschikking gestelde ICT-middelen.

Voor alle gebruikers: de andere gebruikers mogen door het persoonlijke gebruik niet gestoord worden, de IT-infrastructuur van de hogeschool mag niet overdreven belast worden en er mogen geen kosten aan verbonden zijn voor de hogeschool. Zo niet worden de gemaakte kosten voor persoonlijk gebruik op de gebruiker verhaald.

Gebruikers die persoonlijke gegevens op ICT-middelen van de hogeschool opslaan en verwerken, moeten er zich bewust van zijn dat de hogeschool de bevoegdheid heeft om in

⁴ Een remote-wipe van een apparaat betekent dat alle gegevens die op het apparaat staan op afstand worden verwijderd, waardoor het apparaat teruggezet wordt naar de fabrieksinstellingen.

uitzonderlijke gevallen kennis te nemen van informatie die door een gebruiker verwerkt wordt op ICT-middelen van de hogeschool. Ten aanzien van personeelsleden mogen leidinggevenden dit doen indien dit voor de opdracht van de hogeschool absoluut noodzakelijk is. Het directiecomité wordt in dat geval altijd op de hoogte gebracht. Tenzij dit onmogelijk is, wordt ook de betrokken gebruiker geïnformeerd. In elk geval wordt zoveel mogelijk de persoonlijke levenssfeer van de betrokken gebruiker beschermd.

Ter bescherming van persoonlijke gegevens die door de gebruiker worden opgeslagen op ICT-middelen van de hogeschool, is het aan te bevelen om deze gegevens in de Cloud van de hogeschool te bewaren met een referentie naar persoonlijk gebruik.

De hogeschool is niet verantwoordelijk voor eventueel verlies van persoonlijke data die op de ICT-middelen van de hogeschool worden bewaard.

7 Ongeoorloofd gebruik

Onder meer in de volgende situaties is er sprake van ongeoorloofd gebruik:

1. Informatie verspreiden, opslaan of invoeren die:
 - a. Het imago, de morele of economische belangen van de hogeschool kan schaden;
 - b. Beledigend, lasterlijk, aanstootgevend of discriminerend is;
 - c. Schade kan toebrengen aan derden;
2. Vertrouwelijke informatie (bedrijfsgeheimen etc.) doorgeven aan personen die niet gerechtigd zijn om deze informatie te ontvangen;
3. Vertrouwelijke informatie onbeschermd bewaren, zowel elektronisch als op papier;
4. Bedrijfsdata kopiëren voor andere doeleinden dan professionele – of studiedoeleinden naar locaties buiten het netwerk van de hogeschool zonder voorafgaandelijke, schriftelijke toestemming. Alle data moeten teruggegeven worden aan de hogeschool bij het beëindigen van de (medewerking aan de) opdracht waaraan de data gerelateerd zijn;
5. Persoonlijk verkregen gebruiksrechten en licenties van de hogeschool doorgeven aan derden;
6. Wachtwoorden en gebruikersgegevens van andere gebruikers proberen te verkrijgen;
7. Een valse identiteit aannemen op het netwerk;
8. De beveiliging van systemen of informatie in het gedrang brengen door:
 - a. Interne of externe netwerkbeveiliging te omzeilen, door bv. het aansluiten van niet-ondersteunde wifi access-points en/of internetmodems/-routers in labo omgevingen;
 - b. Programmatuur te installeren of te gebruiken waarvoor geen toestemming is verleend of geen licentie is;
 - c. De wetgeving over het auteursrecht en andere intellectuele rechten te schenden (vb. programmatuur kopiëren tenzij dit door de licentie van de leverancier of door de wet is toegestaan);
 - d. ICT-apparatuur die geen eigendom is van de hogeschool, aankoppelen zonder uitdrukkelijke toestemming van de dienst Information Management;

- e. De toegang te forceren tot systemen waartoe men niet gerechtigd is
 - f. Het netwerk af te luisteren.
9. Gebruikersgegevens en wachtwoorden van derden via ongeoorloofde manieren (zoals o.a. phishing, sniffing, ...) trachten te verkrijgen;
 10. Ongewenste of ongevraagde elektronische berichten of kettingbrieven verspreiden;
 11. ICT-infrastructuur die niet voldoet aan de beveiligingsregels in dit document, aan te koppelen zonder toestemming van de dienst Information Management;
 12. Andere gebruikers storen bij het uitoefenen van hun activiteiten of pogingen ondernemen om een dienst, netwerk of computer te verstoren vb. door een netwerk of computer te overbelasten;
 13. Systeeminformatie, systeemconfiguratie, toepassingsprogramma's of bestanden wijzigen, verwijderen of doorgeven aan derden, tenzij men daarvoor bevoegd is;
 14. Intern ontwikkelde programmatuur, die deel uitmaakt van het patrimonium van de hogeschool en die binnen het kader van de beroeps- of opleidingsactiviteit werd ontwikkeld, commercialiseren voor persoonlijke doeleinden of handelingen stellen die het verder gebruik of de exploitatie van de software kunnen hinderen tenzij het programmatuur betreft die specifiek ontwikkeld werd om onbeperkt verspreid te worden zoals bijvoorbeeld programmatuur met een open broncode licentie⁵.

Als één of meerdere vormen van gebruik, die hierboven als ongeoorloofd gebruik worden betiteld, onderwerp uitmaken van wetenschappelijk onderzoek en daarom een afwijking van deze richtlijnen gewenst wordt, moet er een aanvraag bij de voorzitter van de stuurgroep informatieveiligheid worden ingediend via het e-mailadres: CISO@odisee.be.

Elke gebruiker dient er zich bewust van te zijn dat de hogeschool in het kader van een gerechtelijk onderzoek verplicht is om met de gerechtelijke autoriteiten mee te werken.

⁵ Met externe medewerkers die in het kader van hun werkzaamheden binnen de hogeschool programmatuur ontwikkelen, worden contractuele afspraken gemaakt.

8 Toegangsrechten voor externen

Externen die toegangsrechten tot ICT-middelen, IT-infrastructuur of elektronische communicatiemiddelen van de hogeschool nodig hebben voor het uitvoeren van hun opdracht aan de hogeschool (vb. consultants, externe sprekers) verkrijgen deze slechts na het ondertekenen en dateren van een verklaring dat ze de richtlijnen voor het gebruik van ICT aan de hogeschool hebben ontvangen en zullen naleven. Op de verklaring vermelden zij hun volledige naam, adres en telefoonnummer.

De toegangsrechten worden zuiver ten persoonlijke titel toegekend en gelden slechts voor de periode noodzakelijk voor de uitvoering van de opdracht.

9 Uitdiensttreding van een gebruiker (enkel voor personeelsleden)

Het personeelslid dat uit dienst treedt, leeft de voorschriften na van het document "[ICT-gebruik bij en na uitdiensttreding](#)". Dit document kan worden geraadpleegd op het personeelsportaal of kan worden opgevraagd bij de personeelsdienst.

10 Toezicht op het gebruik van de ICT-middelen

De controle wordt uitgevoerd door personen die in het kader van hun functie belast zijn met het beheer van systemen, netwerken of onderdelen daarvan, met name de systeem- en netwerkbeheerders. De controle gebeurt op een wijze die de inmenging in de persoonlijke levenssfeer tot een minimum beperkt. Individuele controle kan gebeuren naar aanleiding van incidenten of een vraag om medewerking van de gerechtelijke autoriteiten.

Zo nodig kunnen bewarende maatregelen genomen worden om de veiligheid en integriteit van de ICT-systemen en de daarmee verwerkte informatie te waarborgen.

– Ten aanzien van gebruikers-personeelsleden

Voor de personeelsleden met een arbeiders- of bediendestatuut geldt CAO nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online communicatiegegevens (hierna genoemd de CAO)⁶. Ook voor de andere personeelsleden wordt deze CAO gevolgd.

De CAO bepaalt dat controle door de werkgever op het gebruik van de online communicatiemiddelen door de werknemers toegestaan is. De controle moet wel gebeuren op een wijze die de inmenging in de persoonlijke levenssfeer tot een minimum beperkt.

⁶ De CAO is van toepassing op de controle op elektronische online communicatiegegevens in de ruime zin. Hierbij is het niet belangrijk of het interne online communicatie betreft, dan wel of deze extern gaat. Ook het e-mailverkeer van werknemers onderling tijdens de arbeidsuren valt dus onder de toepassing van deze CAO. De CAO nr. 81 stelt uitdrukkelijk dat zij een aantal elementen *niet* wenst te regelen met name de regels voor de toegang tot en/of het gebruik van de elektronische online communicatiemiddelen van de onderneming; dit blijft het prerogatief van de werkgever.

Over het invoeren van de mogelijkheid van algemene controle worden de personeelsleden collectief (via het HOC) en individueel (via het personeelsportaal) geïnformeerd. Individuele controle kan gebeuren naar aanleiding van incidenten of een vraag om medewerking van de gerechtelijke autoriteiten.

De uitoefening van het toezicht gebeurt i.f.v. alle doelstellingen van de CAO, conform het geldende arbeidsreglement:

- Het voorkomen van ongeoorloofde feiten;
- De bescherming van de (vertrouwelijke) belangen van de onderneming;
- De veiligheid en de goede technische werking van de ICT-middelen, IT-infrastructuur of elektronische communicatiemiddelen;
- Het te goeder trouw naleven van de richtlijnen voor ICT-gebruik aan de hogeschool.

Indien het enkel gaat over niet-naleving van doelstelling 4, kan individuele controle slechts gebeuren nadat de richtlijnen opnieuw in herinnering zijn gebracht.

Een incident wordt onderzocht:

- Na vaststelling door de dienst Information Management van een technisch incident;
- Na interne melding van een incident, dit is door een andere gebruiker;
- Na externe melding van een incident door contractuele partners van de hogeschool (vb. stageplaats);
- Na officiële vraag om medewerking van de gerechtelijke autoriteiten.

Bij niet-naleving van doelstelling 1, 2 of 3 gebeurt het onderzoek van het incident door directe individualisering. Bij niet-naleving van doelstelling 4 gebeurt de individualisering pas nadat de richtlijnen eerst opnieuw in herinnering zijn gebracht.

Indien het onderzoek uitwijst dat één van de doelstellingen overtreden is, wordt de personeelsdirecteur op de hoogte gebracht van het resultaat van het onderzoek. De personeelsdirecteur voert een gesprek met het personeelslid. Dit gesprek heeft plaats voor iedere beslissing die het personeelslid kan raken. Het personeelslid krijgt de kans zijn/haar bezwaren met betrekking tot de voorgenomen beslissing uiteen te zetten. Het personeelslid kan zich desgewenst door zijn/haar vakbondsafgevaardigde laten bijstaan. Er kan een ordemaatregel worden genomen en/of een sanctie of tuchtmaatregel die is opgenomen in het arbeidsreglement. Mogelijks strafrechtelijke feiten worden gemeld aan de bevoegde instanties.

— Ten aanzien van gebruikers-studenten

Een incident wordt onderzocht:

- Na vaststelling door de dienst Information Management van een technisch incident;
- Na interne melding van een incident, dit is door een andere gebruiker;
- Na externe melding van een incident door contractuele partners van de hogeschool (vb. stageplaats);
- Na officiële vraag om medewerking van de gerechtelijke autoriteiten.

Indien het onderzoek uitwijst dat de ICT-gedraglijn of wetgeving overtreden is, wordt de clusterdirecteur op de hoogte gebracht van het resultaat van het onderzoek. De clusterdirecteur voert een gesprek met de student. Dit gesprek heeft plaats voor iedere beslissing die de student kan raken. De student krijgt de kans zijn/haar bezwaren met betrekking tot de voorgenomen beslissing uiteen te zetten. Er kan een tuchtprocedure gestart worden in overeenstemming met het onderwijs- en examenreglement. Strafrechtelijke feiten worden gemeld aan de bevoegde instanties.

– Ten aanzien van andere gebruikers (dan Odisee-studenten en -personeelsleden)

Een incident wordt onderzocht:

- Na vaststelling door de dienst Information Management van een technisch incident;
- Na interne melding van een incident, dit is door een andere gebruiker;
- Na externe melding van een incident door contractuele partners van de hogeschool (vb. stageplaats);
- Na officiële vraag om medewerking van de gerechtelijke autoriteiten.

Indien het onderzoek uitwijst dat de ICT-gedraglijn of wetgeving overtreden is, wordt de directeur algemeen beheer op de hoogte gebracht van het resultaat van het onderzoek. De directeur algemeen beheer of een ander lid van het directiecomité voert een gesprek met de gebruiker. Dit gesprek heeft plaats voor iedere beslissing die de gebruiker kan raken. De gebruiker krijgt de kans zijn/haar bezwaren met betrekking tot de voorgenomen beslissing uiteen te zetten. Strafrechtelijke feiten worden gemeld aan de bevoegde instanties.

Indien de gebruiker een personeelslid of student van KU Leuven is, meldt de directeur Algemeen Beheer het incident, het resultaat van het onderzoek en het verloop van het gesprek met de gebruiker aan de CISO van KU Leuven.