ICT-reglement voor studenten

Christelijke Hogeschool Windesheim

Inhoudsopgave

ICT-reglement voor studenten

De Christelijke Hogeschool Windesheim (hierna: Windesheim) biedt aan de eigen studenten en aan bezoekende studenten de mogelijkheid internet te gebruiken ten behoeve van de studie. Tevens worden aan studenten voor persoonlijk gebruik een instellingsgebonden mailbox en mogelijkheden tot opslag van bestanden en persoonlijke studiegegevens beschikbaar gesteld ten behoeve van de studie. Daarnaast wordt de mogelijkheid geboden om in het kader van de studie diverse programmatuur te gebruiken en worden er in beperkte mate computers beschikbaar gesteld.
Aan het gebruik van al deze ICT-faciliteiten zijn regels verbonden, in het kader van de goede gang van zaken in de gebouwen en op de terreinen van Windesheim. In aanvulling op de hiertoe in dit reglement opgenomen regels zijn de huisregels van Windesheim onverminderd van kracht. Consequenties van handelen in strijd met dit ICT-reglement zijn opgenomen in de huisregels.
Het ICT-reglement voor studenten van Windesheim is gebaseerd op de Model AUP reglementen voor het Hoger Onderwijs, een gezamenlijk product van SURFnet en SURFibo.

Begrippenlijst

Bedrijfsvoering:	De Dienst Bedrijfsvoering die binnen Windesheim belast is met het als beheerder verzorgen van de toegankelijkheid, configuratie, continuïteit en beveiliging van de ICT-faciliteiten. De bevoegdheid voor uitvoering van de bepalingen in dit reglement is binnen Windesheim belegd bij de directeur Bedrijfsvoering. Operationeel handelen is deels gedelegeerd aan medewerkers van het ICT-bedrijf.
Client apparatuur	Alle eindgebruiker apparatuur zoals laptop, desktop, usb apparaten, tablet of mobiele telefoon.
Datalek:	persoonsgegevens die in handen vallen van Derden die geen toegang tot die gegevens (mogen) hebben.
Gast	Degene die anders dan op grond van een overeenkomst met instemming van Windesheim gebruik maakt van ICT-faciliteiten van Windesheim.
Gebruiker	De medewerker, student of gast die rechtmatig toegang heeft verkregen tot of rechtmatig gebruik maakt van de ICT-faciliteiten van Windesheim.
ICT-faciliteiten	De door of namens Windesheim ter beschikking gestelde faciliteiten voor elektronische informatie uitwisseling, waaronder intranet, internet, elektronische leeromgeving, e-mail, e-mailadres, telefonie en alle faciliteiten al dan niet met een gebruikersnaam/wachtwoord beschikbaar, evenals (draadloze) aansluitfaciliteiten ten behoeve van mobiele apparatuur. Het betreft hier dus zowel apparatuur als programmatuur als verbindingen. De omschrijving van ICT-faciliteiten is niet limitatief en kan worden aangevuld met faciliteiten zoals die in de toekomst ter beschikking worden gesteld.
Mailbox	Ruimte, ingericht op een opslagmedium van een computer, die exclusief ter beschikking staat van de gebruiker voor ontvangst, opslag en verzending van elektronische post.
Responsible disclosure -policy	Richtlijn waaraan melder van een beveiligingslek zich dient te houden om door Windesheim gevrijwaard te worden van mogelijke juridische stappen.
Student	Een ieder die onderwijs volgt bij Windesheim, met inbegrip van extraneï en cursisten.
Verkeersgegevens	Gegevens die informatie geven over het gebruik van de digitale systemen, zoals bandbreedte gebruik en soort netwerkverkeer (http, ftp,..).

Artikel 1 Gebruik van ICT-faciliteiten

1.1 ICT-faciliteiten worden aan de student beschikbaar gesteld ten behoeve van de studie, onder meer voor het kunnen maken van opdrachten, verslagen en scripties, het bijhouden van de studievoortgang, het raadplegen van bronnen en het communiceren met docenten en medestudenten.

1.2 Het gebruik van eigen apparatuur en toepassingen op de netwerkfaciliteiten van Windesheim is toegestaan zolang dit gebruik voldoet aan de regels van dit reglement. Het veranderen van instellingen in apparatuur en toepassingen beschikbaar gesteld door Windesheim is alleen

toegestaan met aparte toestemming van het systeembeheer. Het aansluiten van eigen netwerkapparatuur waarmee de verbinding kan worden gedeeld met derden op de bedrade of draadloze netwerkaansluitingen (zoals routers, DHCP servers, switches en HUBs) is te allen tijde verboden. Het is niet toegestaan om Windesheim ICT-faciliteiten in gebruik te houden zonder dat de gebruiker daarbij lijfelijk aanwezig is.

1.3 ICT-faciliteiten die alleen toegankelijk zijn met behulp van een gebruikersnaam en wachtwoord zijn persoonsgebonden. Deze wachtwoorden mogen niet met anderen worden gedeeld. Windesheim kan nadere eisen stellen aan de kwaliteit van wachtwoorden en andere beveiligingsaspecten, zoals up-to-date zijn van virusscanner. Bij een vermoeden van misbruik van een wachtwoord kan Windesheim per direct het betreffende account ontoegankelijk maken.

Artikel 2 Intellectueel eigendom en vertrouwelijke informatie

2.1 De student maakt geen inbreuk op de intellectuele eigendomsrechten van Windesheim en derden en respecteert de licentie afspraken zoals die van toepassing zijn binnen Windesheim.

2.2 Indien de student in het kader van zijn studie of het uitvoeren van taken voor Windesheim toegang krijgt tot vertrouwelijke informatie of privacy gevoelige informatie waaronder persoonsgegevens, dient de student die informatie strikt vertrouwelijk te behandelen. De student besteedt bijzondere aandacht aan het treffen van maatregelen zoals in artikel 3 van dit reglement genoemd, indien in het kader van het uitvoeren van deze taken de verwerking van vertrouwelijke of privacy-gevoelige informatie buiten Windesheim noodzakelijk is. Denk daarbij o.a. ook aan het beveiligen van informatie op externe opslagmedia of eigen client apparatuur en in niet instellingsgebonden Cloud-toepassingen.

2.3 Indien Windesheim met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten voorschriften heeft opgesteld dient de student deze stipt op te volgen.

Artikel 3 Beveiliging door Windesheim én de student

3.1 Windesheim heeft beveiligingsbeleid en neemt adequate technische en organisatorische maatregelen om de infrastructuur te beveiligen tegen verlies, diefstal, criminele activiteiten, verlies van vertrouwelijkheid, schending van privacy-rechten en schending van intellectuele eigendomsrechten.

3.2 Studenten hebben ieder hun eigen verantwoordelijkheid ten aanzien van informatiebeveiliging. Windesheim verwacht van studenten een proactieve houding en serieuze stappen om de eigen client apparatuur adequaat te beveiligen. De student is te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens.

3.3 In ieder geval dient de student indien met zijn apparatuur gebruikt wordt gemaakt van Windesheimfaciliteiten in het kader van beveiliging:

a. deze apparatuur te voorzien van een adequate virusscanner en firewall;
b. regelmatig reservekopieën te maken van alle relevante data en kopieën van instellingsdata veilig op te slaan;
c. moeilijk te raden wachtwoorden te gebruiken en deze regelmatig te veranderen;
d. deze apparatuur up-to-date te houden wat betreft software-instellingen;

3.4 Wanneer Windesheim aan het gebruik van bepaalde diensten specifiek beveiligingseisen stelt dan zal de student hiervan op de hoogte gesteld worden voor hij de dienst gaat gebruiken. Tevens zal hij aan de eisen moeten voldoen om de dienst te mogen gebruiken.

Artikel 4 Privégebruik en overlast

4.1 Gebruik, privé of ten behoeve van studie, is niet toegestaan wanneer dit in strijd is met de wet, storend is voor de goede orde bij Windesheim, overlast veroorzaakt bij anderen, inbreuk maakt op rechten van Windesheim of derden of de integriteit en de veiligheid van het netwerk aantast.

4.2 Onder niet toegestaan gebruik als genoemd in het eerste lid wordt in ieder geval verstaan:

a. het raadplegen van internetdiensten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud - tenzij dit buiten de openbare ruimte gebeurt en hiervoor tevens instemming is verkregen van de directeur Bedrijfsvoering - of het verzenden van berichten met een dergelijke inhoud;
b. het verzenden van berichten met een (seksueel) intimiderende inhoud of van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;

c. het versturen van spam (ongewenste berichten aan grote aantallen ontvangers tegelijk), het versturen van kettingbrieven of het verspreiden van kwaadaardige software zoals virussen, wormen, Trojaanse paarden en spyware;
d. filesharing- of streamingdiensten (zoals internetradio of internetvideo) te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de ICT-faciliteiten in gevaar kan brengen;
e. films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de student weet/moet weten dat dit in strijd met auteursrechten is;
f. films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.

4.3 Het gebruik van ICT-faciliteiten ten behoeve van commerciële activiteiten is uitsluitend toegestaan wanneer Windesheim hiervoor schriftelijk toestemming heeft verleend.

Artikel 5 Monitoring door Windesheim

5.1 Controle van gebruik van de ICT-faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit dit reglement. Deze regels zijn erop gericht de goede orde op Windesheim te bewaren en de integriteit en de veiligheid van het netwerk en de computerfaciliteiten van Windesheim te bewaken. Gebruik van de ICT-faciliteiten dat op basis van wet- of regelgeving of dit reglement niet is toegestaan wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

5.2 Ten behoeve van deze controle worden geautomatiseerd gegevens verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor de direct verantwoordelijke systeembeheerders en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld. Deze kunnen tot nadere technische maatregelen besluiten, zoals een blokkade van de toegang tot een bepaalde dienst of het beperken van de mogelijkheden van het apparaat in kwestie om het netwerk te kunnen gebruiken.

5.3 Indien door het gebruik van apparatuur van studenten in strijd wordt gehandeld met het in artikel 4.1 bepaalde, kan door Windesheim worden overgegaan tot uitschakeling van de netwerktoegangsmogelijkheden. Indien mogelijk wordt de student vooraf gewaarschuwd, zodat hij de gelegenheid heeft de overlast te staken. Wanneer dit wegens de vereiste spoed niet voorafgaand aan het nemen van de maatregel mogelijk is, wordt de student zo snel mogelijk na het nemen van de maatregel geïnformeerd.

5.4 Bij vermoedens van overtreding van de regels kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het gebruik van de ICT-faciliteiten. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats. Dit kan bijvoorbeeld het geval zijn bij vordering door politie/justitie.

5.5 Windesheim houdt zich bij het controleren op het niveau van verkeersgegevens of de inhoud onverkort aan de Wet bescherming persoonsgegevens en andere relevante wet- en regelgeving. In het bijzonder beveiligt Windesheim de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang tot de gegevens contractueel verplicht tot geheimhouding.

5.6 Voor eigen client apparatuur die op welke wijze dan ook synchroniseert met de Windesheim omgeving geldt dat alle informatie en alle berichten (dus ook privé) die gemaakt, opgeslagen, ontvangen of verstuurd worden en meegaan in de synchronisatie beschouwd worden als Windesheimdata en als zodanig zijn deze data aan dezelfde controle maatregelen onderhevig als alle andere Windesheimdata.

Artikel 6 Procedure bij gericht onderzoek

6.1 Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens betreffende de student worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit reglement door die student.

6.2 Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur van een Domein. In deze opdracht staat de reden voor gericht onderzoek expliciet vermeld. Het College van Bestuur ontvangt een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek.

6.3 Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de ICT-faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan Windesheim na toestemming van

de Domein directeur overgaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

6.4 Gericht onderzoek naar de beveiliging of integriteit van ICT faciliteiten mag in afwijking van artikel 6.2 door de directeur Bedrijfsvoering worden uitgevoerd op basis van concrete aanwijzingen. De resultaten van dit onderzoek worden alleen gedeeld met de student met het doel de beveiliging of integriteit van de client apparatuur van de student te verbeteren. Bij herhaling zal de procedure uit artikel 5.3 worden gevolgd .

6.5 De student wordt zo spoedig mogelijk schriftelijk geïnformeerd door de Domeindirecteur over de aanleiding, de uitvoering en het resultaat van het gerichte onderzoek. De student wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als vooraf informeren het onderzoek daadwerkelijk zou kunnen schaden.

6.6 Systeembeheerders verschaffen zich slechts toegang tot accounts of computers van de student als de student daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in dringende gevallen, bijvoorbeeld wanneer andere gebruikers schade berokkend kan worden. De student zal in dat geval achteraf zo spoedig mogelijk worden geïnformeerd.

Artikel 7 Melden en afhandelen van kwetsbaarheden

7.1 Studenten zijn verantwoordelijk voor de beveiligingsaspecten binnen de eigen invloedssfeer en worden dan ook geacht (vermoedens van) misbruik of beveiligingsincidenten direct te melden bij CSIRT (CSIRT@windesheim.nl) of bij het ICT-loket (servicedesk@windesheim.nl; C0.72; tel 9070).

7.2 Iedere student wordt geacht een datalek of vermoeden daarvan te melden bij het ICT-loket (servicedesk@windesheim.nl).

7.3 Pogingen van de student tot inbraak in beveiligde informatiesystemen van Windesheim worden beschouwd als overtreding van dit reglement, tenzij hierbij de Windesheim responsible disclosure policy (zie bijlage 1) in acht wordt genomen.

Artikel 8 Slotbepalingen

8.1 Dit reglement is op 12 december 2017 door het College van Bestuur vastgesteld en treedt voor onbepaalde tijd in werking op 1 januari 2018. Dit ICT-reglement voor studenten treedt in de plaats van het reglement zoals vastgesteld bij besluit 719 op 9 december 2014.

8.2 Deze regeling kan door het College van bestuur worden herzien. Wijzigingen worden alleen bij het begin van een collegejaar doorgevoerd, behalve in dringende gevallen of wanneer Windesheim door omstandigheden van buitenaf gedwongen is tot een snellere invoering.

8.3 Dit reglement is aanvullend op de bepalingen van het vigerende Instellingsdeel van het Studentenstatuut van Windesheim en het wordt geacht van dat statuut onderdeel uit te maken.

8.4 In gevallen waarin deze regeling niet voorziet, beslist het College van Bestuur.

8.5 Dit reglement kan worden aangehaald als “ICT-reglement studenten”.

Bijlage 1: Responsible disclosure policy

Windesheim wil zorgvuldig omgaan met haar gegevens en daarom is veiligheid belangrijk. Ondanks alle inzet om onze systemen veilig te maken is het mogelijk dat er zwakke plekken in onze beveiliging zijn ontstaan.

Mocht je zo'n zwakke plek in één van onze systemen constateren dan willen we graag met je samenwerken om deze situatie zo spoedig mogelijk op te lossen. We verzoeken je dan ook deze informatie met ons te delen.

Om misbruik van het datalek te voorkomen vragen we jou om je aan deze richtlijnen te houden:

1. Meld het probleem door een email te sturen naar CSIRT@windesheim.nl.
2. Maak geen actief misbruik van het beveiligingslek.
3. Deel informatie over dit lek niet met anderen totdat het lek hersteld is en wis alle gegevens die eventueel door het lek verkregen zijn.
4. Maak geen gebruik van aanvallen op de fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden.
5. Geef voldoende informatie zodat wij het probleem kunnen reproduceren en het zo snel mogelijk kunnen oplossen.

Wanneer jij je aan de bovenstaande richtlijnen houdt zeggen wij toe:

1. Dat we er naar streven om binnen vijf werkdagen contact met je op te nemen met een inschatting van de herstelperiode.
2. Geen juridische stappen tegen jou te ondernemen betreffende de melding.
3. Jouw melding vertrouwelijk te behandelen en jouw persoonsgegevens niet zonder jouw toestemming met derden te delen, tenzij hiervoor een wettelijke verplichting geldt. Onder pseudoniem/anoniem melden is mogelijk.
4. Jou op de hoogte te houden over de voortgang van de oplossing van het probleem.
5. Indien je dat wenst, in eventuele berichtgeving over dit probleem jou als ontdekker ervan te noemen.

We streven ernaar geconstateerde beveiligingslekken zo spoedig mogelijk op te lossen. Mocht je nadat het probleem is opgelost hierover willen publiceren dan worden wij graag betrokken bij publicatie.