Reglement verantwoord gebruik ICT-faciliteiten

Basis voor het reglement

Het gebruik van internet en ICT-middelen[1] is voor studenten en medewerkers binnen Gilde Opleidingen noodzakelijk ten behoeve van hun studie dan wel om hun werk goed te kunnen doen. Aan het gebruik hiervan zijn risico's verbonden die het stellen van gedragsregels noodzakelijk maken. Tegen de achtergrond van deze risico's mag van de studenten en medewerkers verantwoord gebruik van internet en ICT worden verwacht.

Met dit reglement wil Gilde Opleidingen regels stellen omtrent het gewenst gebruik van deze bedrijfsmiddelen. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig ICT- en internetgebruik.

Afspraken in het kader van privacy worden in een apart reglement geregeld, het "**Privacyreglement voor studenten**", respectievelijk het "**Privacyreglement voor medewerkers**".

Het gebruik van social media zoals Facebook, LinkedIn en Twitter wordt steeds belangrijker maar kan ook zijn weerslag hebben op Gilde Opleidingen. Daarom wil Gilde Opleidingen ook hier bepaalde regels aan stellen (zie **Protocol social media voor medewerkers en studenten**).

Uitgangspunten

Gilde Opleidingen stelt aan studenten voor persoonlijk gebruik een instellingsgebonden mailbox en mogelijkheden tot opslag van bestanden en persoonlijke studiegegevens beschikbaar ten behoeve van de studie. Aan het gebruik van deze faciliteiten zijn regels verbonden.

Gilde Opleidingen stelt regels ten aanzien van het gebruik van de bedrijfsmiddelen ICT en internet door medewerkers. Doel van deze regels is de goede orde te bepalen ten aanzien van:

- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
- bescherming van privacygevoelige informatie waaronder persoonsgegevens van Gilde Opleidingen en haar medewerkers en van studenten en ouders;
- bescherming van vertrouwelijke informatie van Gilde Opleidingen en haar medewerkers en van studenten en ouders;
- bescherming van de intellectuele eigendomsrechten van Gilde Opleidingen en derden waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen de instelling;

Dit reglement geldt voor eenieder die voor Gilde Opleidingen werkzaam is, dus ook voor uitzendkrachten en tijdelijke medewerkers.

Gilde Opleidingen streeft in het kader van handhaving van dit reglement naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele medewerkers zo veel mogelijk beperken. Zij zal waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen.

1.1 Aanvaardbaar gebruik van faciliteiten

Computer- en netwerkfaciliteiten (zoals openbare computers, draadloze en bedrade netwerkaansluitingen, e-mail en internettoegang, opslagcapaciteit, printers en elektronische leeromgevingen) worden aan de student beschikbaar gesteld, onder meer voor het kunnen maken van

[1] Onder ICT-middelen wordt onder meer verstaan: pc's (computers), laptops, tablets, smartphones, usb-sticks, randapparatuur, smartboards, netwerk en netwerkcomponenten.

opdrachten, verslagen en werkstukken, het bijhouden van de studievoortgang, het raadplegen van bronnen en het communiceren met docenten en medestudenten.

Computer- en netwerkfaciliteiten worden beschikbaar gesteld aan de medewerker voor gebruik in het kader van zijn functie. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.

De medewerker dient te allen tijde zorgvuldig om te gaan met de aan hem toegekende device(s) en de aan hem persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen. Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld. Bij een vermoeden van misbruik van een wachtwoord kan de ict-beheerder per direct het betrokken account ontoegankelijk maken.

Bepaalde faciliteiten zijn alleen toegankelijk met behulp van een gebruikersnaam en wachtwoord. Deze zijn persoonsgebonden en mogen niet met anderen worden gedeeld. Ook is het niet toegestaan om namens of voor iemand anders in te loggen. ICT kan nadere eisen stellen aan de kwaliteit van wachtwoorden en andere beveiligingsaspecten. Bij een vermoeden van misbruik van een wachtwoord kan ICT per direct het betreffende account ontoegankelijk maken.

Het e-mailsysteem en de bijbehorende mailbox en het e-mailadres wordt aan de medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie. E-mails blijven eigendom van de eindgebruiker.

Bij het gebruik van ICT-middelen dient te allen tijde dit reglement nageleefd te worden. Eindgebruikers zijn zelf verantwoordelijk de inhoud van het reglement te kennen en daarna te handelen. Het reglement is algemeen beschikbaar en eenvoudig vindbaar op het intranet. Bij significante wijzigingen is het de verantwoordelijkheid van Gilde Opleidingen dit bij de gebruikerspopulatie onder de aandacht te brengen.

Persoonlijk verstrekte ICT-middelen vallen onder de verantwoordelijkheid van de ontvanger. Goede zorg mag verwacht worden. Bij het signaleren van defecten dient dit door de verantwoordelijke gemeld te worden. Bij het signaleren van defecten, verstoringen of onjuist gedrag van algemene ICT-voorzieningen dient dit gemeld te worden bij ICT. Bij het signaleren van zwakke plekken in de informatiebeveiliging dient binnen een acceptabele periode een melding te worden gemaakt door het melden van een veiligheidsincident. Wat een acceptabele periode is varieert naargelang de ernst van het gesignaleerde edoch uiterlijk binnen een week.

Het is niet toegestaan misbruik te maken van gebreken aan de informatievoorziening en daarbij behorende bedrijfsmiddelen of zelf op onderzoek uit te gaan tot waar een gebrek geëxploiteerd kan worden.

Voor zaken die niet beschreven zijn wordt geacht in de geest van het reglement te handelen en het belang van Gilde Opleidingen met “gezond verstand” te behartigen.

1.2 Hergebruik en verwijderen van bedrijfsmiddelen

Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring. Een dergelijke goedkeuring dient schriftelijk overlegd te kunnen worden. Afgeschreven bedrijfsmiddelen worden niet ter beschikking gesteld voor privé gebruik.

Bedrijfsmiddelen die niet meer in gebruik zijn dienen ter inname te worden aangeboden bij ICT. Bij hergebruik zowel in- als extern zullen eventuele informatiedragers deskundig gewist alvorens te worden her ingezet. Bij vernietiging zal ICT de gegevens onomkeerbaar wissen of onbenaderbaar maken of wordt er gebruik gemaakt van een gecertificeerd vernietigingsproces.

1.3 Intellectueel eigendom en vertrouwelijke informatie

De medewerker dient vertrouwelijke informatie, privacygevoelige informatie waaronder persoonsgegevens waar hij in het kader van het werk toegang tot heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.

De student en medewerker maakt geen inbreuk op de intellectuele eigendomsrechten van Gilde Opleidingen en derden en respecteert de licentieafspraken zoals die van toepassing zijn binnen Gilde Opleidingen. De zeggenschap over de informatie van de instelling berust bij Gilde Opleidingen. De student en medewerker heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door Gilde Opleidingen.

Indien de student in het kader van zijn studie of het uitvoeren van taken voor Gilde Opleidingen toegang krijgt tot vertrouwelijke informatie of privacygevoelige informatie waaronder persoonsgegevens, dient de student die informatie strikt vertrouwelijk te behandelen.

De medewerker besteedt bijzondere aandacht aan het treffen van maatregelen zoals in dit reglement genoemd, indien in het kader van het uitvoeren van de werkzaamheden de verwerking van vertrouwelijke informatie buiten de instelling noodzakelijk is zoals via E-mail, in niet instellingsgebonden Cloud-toepassingen, op externe opslagmedia of eigen cliënt-apparatuur (USB-apparaten, tablets, et cetera). Indien Gilde Opleidingen met betrekking tot het waarborgen van de vertrouwelijkheid voorschriften heeft opgesteld zal medewerker deze strikt naleven.

1.4 Veilig opslaan van bedrijfsinformatie

Bedrijfsinformatie mag enkel op de daarvoor toegewezen (cloud)opslagmedia worden opgeslagen. Dit kan zowel de applicatie zijn waarin de informatie verwerkt wordt als een centrale opslaglocatie zoals netwerkschijven, SharePoint, OneDrive of een andere door ICT gefaciliteerde opslaglocatie. Het is alleen toegestaan om informatie op andere (cloud)locaties op te slaan met nadrukkelijke schriftelijke toestemming. Dit is ook van toepassing op transportmedia zoals USB-Sticks, geheugenkaarten of externe harde schijven. Ook wanneer het transportmedia het bedrijf niet verlaat. Wanneer wel goedkeuring is verleend voor het gebruik van dergelijke media en het betreft privacygevoelige informatie dan dient de drager voorzien te zijn van cryptografische beheersmaatregelen conform het daarvoor geldende beleid.

1.5 Cryptografische beheersmaatregelen

Privacygevoelige informatie die het bedrijf of aangesloten onderaannemers (zoals cloud leveranciers) verlaat dient versleuteld opgeslagen en/of verstuurd te worden. De sleutel en de informatie mogen niet bij elkaar worden opgeslagen. Voor het versturen van privacygevoelige informatie is SURFfilesender ter beschikking gesteld. De verstuurder is zelf verantwoordelijk voor het versleutelen van de gegevens en de keuze voor een moeilijk te herleiden sleutel. Bij gebruik van SURFfilesender kan dit door aan te geven dat de informatie versleuteld dient te worden en het opgeven van een wachtwoord wat voldoet aan de volgende eisen:

- Minimaal 8 karakters
- Gebruik van minimaal 1 hoofdletter (bij voorkeur niet alleen het eerste karakter)
- Gebruik van minimaal 1 cijfer (bij voorkeur niet alleen de laatste karakters)
- Gebruik van minimaal 1 leesteken
- Geen relatie tussen het wachtwoord en de betreffende informatie en/of de gebruiker ervan.

Wanneer het wachtwoord gedeeld moet worden met derden dan dient het wachtwoord separaat en bij voorkeur op een andere wijze naar de ontvanger gestuurd te worden.

Deze versleuteling moet ongedaan kunnen worden gemaakt als, bijvoorbeeld, de overheid op een wettelijke grondslag hiertoe een verzoek indient. De verantwoordelijkheid voor het bewaren en ter beschikking kunnen stellen van de sleutel ligt bij de versleutelaar.

1.6 Toegang tot informatie

Bedrijfsinformatie wordt enkel beschikbaar gesteld aan geautoriseerde personen. Hiervoor wordt het “least privilege” principe gehanteerd. Bij een ontdekking dat toegang gerealiseerd kan worden tot bedrijfskritische of privacygevoelige informatie waarvoor geen grondslag is vanuit de uit te voeren werkzaamheden dient dit per direct gemeld te worden als een veiligheidsincident.

Het is niet toegestaan om doelbewust afgeschermde bedrijfsinformatie te benaderen zonder eerstens de eigen identiteit kenbaar te maken (e.g. ethical hacking, man-in-the-middle, etc.) of zonder toestemming belangrijke of privacygevoelige bedrijfsinformatie beschikbaar te stellen zonder dat identificatie en authenticatie noodzakelijk is om de informatie te benaderen.

Identificatie en authenticatie gebeurt op basis van een of meerdere factoren.

Autorisatie wordt pas verleend na authenticatie van de afgegeven identificatiefactoren.

1.7 Beveiliging door de instelling én de student

Gilde Opleidingen neemt informatiebeveiliging serieus. Zij hanteert dan ook een streng 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.

Natuurlijk is een perfecte beveiliging onmogelijk. Daarom verwacht Gilde Opleidingen ook van studenten een proactieve houding en serieuze stappen om de eigen computer en andere apparatuur (zoals smartphones of tablets) adequaat te beveiligen. Zo is de student te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens. Als hier onvolkomenheden gezien worden, kan de ICT-beheerder de toegang ontzeggen.

In het bijzonder dient de student, indien met zijn apparatuur gebruikt wordt gemaakt van de instellingsfaciliteiten, in het kader van beveiliging:

- deze apparatuur te voorzien van een adequate virusscanner en firewall;
- goede wachtwoorden te gebruiken en deze regelmatig te veranderen;
- deze apparatuur up-to-date te houden wat betreft software-instellingen.

De student dient Gilde Opleidingen in staat te stellen geautomatiseerde controles (health check) uit te voeren aangaande de beveiliging of integriteit van eigen middelen. Ook wanneer daarvoor installatie van door Gilde Opleidingen beschikbaar gestelde (cliënt-) software benodigd is. De student is zelf verantwoordelijk voor de correcte werking van deze software op zijn of haar middelen. Gilde opleidingen heeft te allen tijde het recht toegang tot instellingssystemen te ontzeggen wanneer niet aan de gestelde voorwaden wordt voldaan, dit niet controleerbaar blijkt of wanneer er al dan niet bewust kwaadwillend handelen geconstateerd wordt.

1.8 Privégebruik en overlast

Privégebruik van de faciliteiten is toegestaan. Gebruik, privé of voor studie, mag niet storend zijn voor de goede orde bij Gilde Opleidingen en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van Gilde Opleidingen of derden of de integriteit en de veiligheid van het netwerk aantasten.

Het gebruik van computer- en netwerkfaciliteiten voor commerciële activiteiten is uitsluitend toegestaan wanneer Gilde Opleidingen hiervoor schriftelijk toestemming heeft verleend.

Het opslaan van privébestanden of -informatie op systemen van Gilde Opleidingen is toegestaan, mits dit niet leidt tot overbelasting van de opslagcapaciteit van deze systemen of een verstoring van de goede orde op de werkvloer. Gilde Opleidingen is echter niet verplicht van dergelijke bestanden of informatie reservekopieën te maken of kopieën beschikbaar te stellen bij vervanging of reparatie van de betreffende systemen.

Het gebruik van computer- en netwerkfaciliteiten door de medewerker ten behoeve van nevenwerkzaamheden is uitsluitend toegestaan als en voor zover Gilde Opleidingen hiervoor schriftelijk toestemming heeft verleend.

1.9 Specifiek gebruik van e-mail

In geval van ziekte, onverwacht langdurige afwezigheid of grove nalatigheid van de medewerker, doch uitsluitend als dit een zwaarwegende reden van bedrijfsbelang tot toegang oplevert, is Gilde Opleidingen gerechtigd een vervanger of leidinggevende toegang tot de bestanden of mailbox van de medewerker te verschaffen doch uitsluitend nadat hiertoe expliciet toestemming van de directeur P&O is verkregen en dit door de directeur kenbaar is gemaakt aan de betreffende medewerker. Deze mag zich echter geen toegang verschaffen tot als privé gemarkeerde mappen, als privé herkenbare mails, of mails verzonden naar dan wel afkomstig van een vertrouwenspersoon of bedrijfsarts. Indien de medewerker geen dergelijke markeringen heeft aangebracht, kan Gilde Opleidingen door inschakeling van een vertrouwenspersoon de betreffende informatie van de medewerker controleren om zo privéinformatie te herkennen en te separeren alvorens de vervanger of leidinggevende toegang krijgt. Dit Artikel 1.5 is ter goedkeuring voorgelegd aan de OR (WOR, artikel 27, lidd K).

E-mailberichten van leden van het medezeggenschapsorgaan onderling, van bedrijfsartsen en van eenieder die zich op grond van de wet op vertrouwelijkheid mag beroepen, worden niet gecontroleerd. Dit geldt niet voor geautomatiseerde controle op de veiligheid van het e-mailverkeer en netwerk.

1.10 Clear-desk & clear-screen

Wanneer de werkplek verlaten wordt dient de werkplek vrij te zijn gemaakt van belangrijke informatie. Dit betreft zowel fysieke als data dragers. Ook wanneer de datadrager slechts indirect toegang verschaft tot informatie (bijvoorbeeld een laptop). Wanneer er geen veilige opberglocatie beschikbaar is dient dit gemeld te worden bij de leidinggevende.

Wanneer de werkplek voor een kortere of langere tijd verlaten wordt dient tenminste het beeldscherm geblokkeerd te zijn (toets combinatie Windows + L). Wanneer een computer of laptop voor een langere tijd niet gebruikt wordt dient deze uitgeschakeld of in slaapstand gezet te worden. Dit voorkomt o.a. het gevaar om gehackt te worden, brandgevaar en nodeloos energie verbruik. Dit geldt voor zowel door Gilde Opleidingen verstrekte middelen als privé middelen (Bring Your Own Device).

Ook bij het werken vanaf externe locaties (e.g. thuiswerken) dient belangrijke bedrijfsinformatie beschermd te worden tegen toegang door derden middels bovenstaande richtlijn.

1.11 Monitoring door de instelling

Controle van gebruik van de faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit dit reglement ten behoeve van de goede orde op de instelling en de bewaking van de integriteit, continuïteit, beschikbaarheid en de veiligheid van het netwerk en de computerfaciliteiten van Gilde Opleidingen. Verboden gebruik van de faciliteiten wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

Voor deze controle worden geautomatiseerd gegevens verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor systeembeheerders t.b.v. analyses en worden alleen in geanonimiseerde vorm aan andere verantwoordelijken beschikbaar gesteld. De systeembeheerders kunnen na analyse 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.

In het bijzonder kan bij overlast, veroorzaakt door apparatuur van studenten, worden overgegaan tot uitschakeling van de netwerktoegangsmogelijkheden. Indien mogelijk wordt de student vooraf gewaarschuwd via een melding op zijn systeem (piepsysteem), zodat hij de gelegenheid heeft de overlast te staken.

Bij vermoedens van overtreding van de regels kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het gebruik van de faciliteiten. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.

Gilde Opleidingen houdt zich bij het controleren op het niveau van verkeersgegevens of de inhoud onverkort aan de Algemene Verordening Gegevensbescherming en andere relevante regelgeving. In het bijzonder beveiligt Gilde Opleidingen de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en worden personen met toegang daartoe contractueel verplicht tot geheimhouding.

1.12 Procedure bij gericht onderzoek

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

Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur P&O, waarbij de reden vermeld zal worden waarom tot dit gerichte onderzoek zal worden overgegaan. Het College van Bestuur ontvangt een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek.

Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan Gilde Opleidingen na voorafgaande aparte toestemming van College van Bestuur hiervoor, 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.

Nader onderzoek naar de beveiliging of integriteit van (rand)apparatuur mag in afwijking hiervan door de ict-beheerder worden uitgevoerd op basis van concrete aanwijzingen, zonder aparte toestemming.

De resultaten van dit onderzoek worden alleen gedeeld met de student of medewerker met het doel de beveiliging of integriteit van de (rand)apparatuur te verbeteren. Bij herhaling zal de procedure zoals hiervoor beschreven voor het gericht onderzoek worden gevolgd.

De student of medewerker wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou schaden.

Systeembeheerders verschaffen zich slechts toegang tot accounts of computers van student of medewerker, als de student of medewerker daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in dringende gevallen of bij een duidelijk vermoeden van schending van dit reglement, zoals nader bepaald in dit reglement en na akkoord van de directeur P&O. De student of medewerker zal in dat geval achteraf worden geïnformeerd.

1.13 Consequenties van overtreding

Bij handelen in strijd met dit reglement of algemeen geldende (wettelijke) regels, kan Gilde Opleidingen afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen. Hieronder vallen een waarschuwing, berisping, een tijdelijke afsluiting of beperking van de faciliteiten (maximaal een jaar) en in extreme gevallen een beëindiging van de inschrijving als student of beëindiging van de arbeidsovereenkomst.

Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet worden getroffen enkel op basis van een langs geautomatiseerde weg uitgevoerde verwerking van persoonsgegevens, zoals een constatering van een automatisch filter of blokkade. Voorts worden geen disciplinaire maatregelen getroffen zonder dat de student of medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

In afwijking van het voorgaande is het mogelijk dat Gilde Opleidingen bij (geautomatiseerde) constatering van overlast een tijdelijke blokkade van de betreffende faciliteit invoert. Deze blokkade zal zolang worden gehandhaafd tot aangetoond is dat de oorzaak tot tevredenheid van de ict-beheerder is weggenomen. Bij herhaling van de oorzaak kunnen alsnog disciplinaire maatregelen worden genomen.

1.14 Slotbepalingen

Dit reglement kan door Gilde Opleidingen worden herzien. Wijzigingen worden alleen bij het begin van een schooljaar doorgevoerd, behalve in dringende gevallen of wanneer Gilde Opleidingen door omstandigheden gedwongen is tot een snellere invoering. Wijzigingen worden alleen ingevoerd nadat de Medezeggenschapsraden om voorafgaand advies is gevraagd. Gilde Opleidingen zal feedback van studenten of medewerkers in overweging nemen alvorens de wijzigingen in te voeren. In gevallen waarin dit reglement niet voorziet, beslist het College van Bestuur.