

Reglement ICT, sociale media en internetgebruik

MARNIX ACADEMIE 2023 - 2024

29-06-2023

Gebruiksregels ICT en internet voor (externe) medewerkers, partners en studenten van de Marnix Academie.

Het gebruik van ICT-middelen, sociale media, en internet is voor (externe) medewerkers, partners en studenten van de Marnix Academie noodzakelijk om hun werk en/of studie goed te kunnen doen. Aan het gebruik hiervan zijn risico's verbonden die nopen tot het stellen van gedragsregels. Tegen de achtergrond van deze risico's mag van de (externe)medewerkers, partners of studenten verantwoord gebruik van internet en ICT worden verwacht.

Met dit reglement stelt de Marnix Academie (en onderliggende opleidingspartners waaronder MOC en Penta Nova) regels omtrent het gewenst gebruik van deze (organisatie)middelen. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig ICT en internetgebruik en de privacy van de (externe)medewerker, partner en student. Het gebruik van sociale media zoals whatsapp, Facebook, LinkedIn, Instagram, TikTok, Snapchat en Twitter wordt steeds belangrijker en kan ook zijn weerslag hebben op de Marnix Academie. Daarom stelt de Marnix Academie hier bepaalde regels aan. De Marnix Academie is bevoegd regels te stellen omtrent de uitvoering van het werk en de goede gang van zaken in gebouwen van de instelling, alsmede de thuiswerkplek. Omdat het Reglement voorziet in een verwerking van persoonsgegevens en/of controle op gedrag of prestaties van (externe)medewerkers, partner en/of studenten, is de Medezeggenschapsraad instemmingsgerechtigd.

1. Artikel 1. Uitgangspunten

- 1.1 De gebruikersregels richten zich op het gebruik van de bedrijfsmiddelen ICT en internet door (externe)medewerkers, partners of studenten. Doel van deze regels is de goede orde te bepalen ten aanzien van:
 - 1.1.1 *Systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;*
 - 1.1.2 *Tegengaan van seksuele intimidatie, discriminatie, pesten, kwetsen, stalken, bedreigen, schelden, laster of strafbare feiten;*
 - 1.1.3 *Bescherming van privacygevoelige informatie van haar (externe)medewerkers, partners, studenten en derden;*
 - 1.1.4 *Bescherming van vertrouwelijke informatie van haar (externe)medewerkers, partners, studenten en derden;*
 - 1.1.5 *Bescherming van de intellectuele eigendomsrechten van de Marnix Academie en derden waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen de Marnix Academie;*
 - 1.1.6 *Voorkomen van negatieve publiciteit en imagoschade;*
 - 1.1.7 *Kosten- en capaciteitsbeheersing;*
 - 1.1.8 *Voorkomen van ransomware, digitale gijzeling of ransomware aanvallen.*
- 1.2 Privégebruik van internet en ICT-middelen is beperkt toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden of het netwerk van de Marnix Academie of in conflict met andere artikelen in dit reglement.
- 1.3 Deze gebruiksregels gelden voor eenieder die bij de Marnix Academie gebruik maakt van ICT-middelen of internet.
- 1.4 Deze gebruiksregels gelden ook indien de (externe)medewerker, partner of student via Eduroam gebruik maakt van netwerkvoorzieningen van andere instellingen. Indien gebruikersregels van een andere instelling afwijken van deze gebruikersregeling, dan prevaleren de gebruikersregeling van de instelling waar de (externe)medewerker, partner of student zich bevindt.
- 1.5 De Marnix Academie streeft in het kader van handhaving van dit reglement naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele (externe)medewerkers, partners of studenten 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.

2. Artikel 2. Intellectueel eigendom en vertrouwelijke informatie

- 2.1 De (externe)medewerker, partner of student 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.
- 2.2 De (externe)medewerker, partner of student maakt geen inbreuk op de intellectuele eigendomsrechten van de Marnix Academie en derden en respecteert de licentie afspraken zoals die van toepassing zijn binnen de Marnix Academie.
- 2.3 De (externe)medewerker, partner of student 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 Marnix Academie noodzakelijk is zoals via E-mail, in niet instellingsgebonden Cloud-toepassingen, op externe opslagmedia of eigen client-apparatuur.
- 2.4 Het gebruik van opslagmethoden zoals USB-geheugen, externe harde schijven, geheugenkaarten, niet instellingsgebonden Cloud-toepassingen, niet instellingsgebonden diensten voor het uitwisselen van data (zoals iCloud, GoogleDrive, WeTransfer, Dropbox, of vergelijkbare diensten) zijn niet toegestaan.
- 2.5 Deze bepalingen gelden in het bijzonder voor systeembeheerders, voor wie schending van deze bepalingen als een zeer ernstig plichtsverzuim wordt aangemerkt, gezien hun bijzondere positie.

3. Artikel 3. Gebruik van computer- en netwerkfaciliteiten

- 3.1 Computer- en netwerkfaciliteiten worden aan de (externe)medewerker, partner of student voor gebruik in het kader van zijn functie resp. studie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie resp. opleiding. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.
- 3.2 De (externe)medewerker, partner of student dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen (zoals smartcards en tokens). Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld. De houder van een account kan worden verplicht om gebruik te maken van een meervoudige verificatie bij de inlogprocedure en stemt er mee in dat hiervoor dat het gebruik van een (privé) smarttelefoon benodigd is. Bij een vermoeden van misbruik van een wachtwoord kan het systeembeheer per direct het betrokken account ontoegankelijk maken.
- 3.3 De Marnix Academie kan voor onderwijs- en andere bedrijfsdoeleinden systemen of applicaties voorschrijven, zoals een Elektronische Leeromgeving, een e-mailsysteem, (mobiele) applicaties (apps), cloudvoorzieningen of multimediadiensten. De (externe)medewerker, partner of student zal voor het delen van lesmateriaal of het uitvoeren van onderzoek alleen deze systemen gebruiken en de daarbij gestelde beperkingen en eisen strikt naleven.
- 3.4 Het installeren van software op de computer- en netwerkfaciliteiten van de organisatie is niet toegestaan zonder aparte toestemming van het systeembeheer. Ook het aansluiten van servers en actieve netwerkcomponenten (zoals access points en routers) is niet toegestaan zonder toestemming van het systeembeheer. Het systeembeheer kan aan de toestemming regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners en wachtwoordbeveiliging.
- 3.5 Het aansluiten van eigen client-apparatuur (zoals, laptops, tablets en telefoons) is alleen toegestaan op de daarvoor beschikbaar gestelde (wireless) netwerkaansluitingen. Het systeembeheer kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners en wachtwoordbeveiliging.
- 3.6 Het opslaan van privébestanden of -informatie op systemen van de Marnix Academie is beperkt toegestaan, mits dit niet leidt tot overbelasting van de opslagcapaciteit van deze systemen of een verstoring van de goede orde op de werkvloer of operatie. De Marnix Academie 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.
- 3.7 Het gebruik van computer- en netwerkfaciliteiten ten behoeve van nevenwerkzaamheden is uitsluitend toegestaan als en voor zover de Marnix Academie hiervoor schriftelijk toestemming heeft verleend.

4. Artikel 4. Gebruik van e-mail en andere ICT-communicatiemiddelen

- 4.1 Het e-mailsysteem en de bijbehorende mailbox en e-mailadres worden beschikbaar gesteld voor gebruik in het kader van de functie resp. de opleiding. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie of opleiding.
- 4.2 Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.
- 4.3 Verboden bij elk gebruik (privé of niet) van ICT-communicatiemiddelen is echter:
 - 4.3.1 *Het verzenden van berichten met een pornografische, racistische, discriminerende, bedreigende, beledigende of aanstootgevende inhoud;*
 - 4.3.2 *Het verzenden van berichten met een (seksueel) intimiderende inhoud;*
 - 4.3.3 *Het verzenden van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;*
 - 4.3.4 *Het versturen van ongeverraagde berichten aan grote aantallen ontvangers, kettingbrieven te versturen of kwaadaardige software zoals virussen, Trojaanse paarden, malware, ransomware of spyware te versturen.*
 - 4.3.5 *Het geautomatiseerd doorsturen (bijvoorbeeld een mailbox in de forward zetten) naar systemen buiten de organisatie.*
 - 4.3.6 *De (externe)medewerker, partner of student gebruikt voor privémail bij voorkeur niet het door de Marnix Academie verstrekte e-mailadres, binnen de grenzen van artikel 1.2. De organisatie zal de toegang tot andere e-maildiensten niet blokkeren of specifiek monitoren.*
- 4.4 In geval van ziekte, onverwacht langdurige afwezigheid of grove nalatigheid van de (externe)medewerker, partner of student, doch uitsluitend als dit een zwaarwegende reden van bedrijfsbelang tot toegang oplevert, is de Marnix Academie gerechtigd een derde toegang tot de bestanden of mailbox van de (externe)medewerker, partner of student te verschaffen, doch uitsluitend nadat hiertoe aparte toestemming van de leidinggevende van de medewerker dan wel de opleidingsmanager van de student is verkregen. Deze derde mag zich echter geen toegang verschaffen tot als privé gemarkeerde mappen, als privé herkenbare mails, of mails verzonden naar of afkomstig van een vertrouwenspersoon/ bedrijfsarts. Indien de (externe)medewerker, partner of student geen dergelijke markeringen heeft aangebracht, kan de Marnix Academie door inschakeling van een vertrouwenspersoon de betreffende informatie van de (externe)medewerker, partner of student controleren om zo privéinformatie te herkennen en apart te plaatsen alvorens een derde toegang krijgt.
- 4.5 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.

5. Artikel 5. Gebruik van het netwerk en internet

- 5.1 De toegang tot internet en bijbehorende faciliteiten worden aan de (externe)medewerker, partner of student voor gebruik in het kader van zijn functie resp. studie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie resp. opleiding.
- 5.2 Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.
- 5.3 Verboden bij elk gebruik (privé of niet) is echter:
- 5.3.1 *Sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;*
 - 5.3.2 *Filesharing- of streamingdiensten (zoals internetradio of NPOstart, RTLXL, Youtube, Tiktok, ect) te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de faciliteiten in gevaar kan brengen. Beoordeling van de belasting op de faciliteiten door de systeemspecialist is hier bindend;*
 - 5.3.3 *Films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de medewerker daadwerkelijk weet of had behoren te weten dat dit in strijd met auteursrechten is;*
 - 5.3.4 *Films, muziek, software en overig auteursrechtelijk beschermd materiaal te verkrijgen (downloaden), verspreiden (uploaden) of verzamelen (opslaan) zonder toestemming van de rechthebbenden.*
 - 5.3.5 *Het creëren of faciliteren van ongevraagde berichten aan grote aantallen ontvangers, kettingbrieven te versturen of kwaadaardige software zoals virussen, Trojaanse paarden, malware, ransomware of spyware te versturen.*
 - 5.3.6 *On-gelegitimeerd toegang verschaffen, hacken, uitvoeren van penetratietesten zowel met als kwade of ethische doelstellingen. (mits hier voor onderzoeksdoelinden het CVB schriftelijk toestemming op heeft gegeven.)*

6. Artikel 6. Gebruik van sociale media

- 6.1 De Marnix Academie ondersteunt de open dialoog en de uitwisseling van ideeën en het delen van kennis van (externe)medewerkers, partners of studenten via sociale media. Indien dit werk- of studie gerelateerde onderwerpen betreft, dient de (externe)medewerker, partner of student ervoor te zorgen dat het profiel en de inhoud in overeenstemming is met hoe hij zich in tekst, beeld en geluid zou presenteren ten overstaan van (externe)collega's, partners en studenten. Uitwisseling of publicatie van gegevens, berichten, beeld en geluidsmateriaal via sociale media hebben de betrokkenen uitdrukkelijk toestemming gegeven. Alsmede artikel 1.1 en 5.3 zijn van toepassing bij het gebruik van sociale media.
- 6.2 Sociale media is een verzamelbegrip voor online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Hoofdkenmerken zijn interactie en dialoog tussen de gebruikers. De (externe)medewerker, partner of student is persoonlijk verantwoordelijk voor de inhoud welke hij of zij publiceert op de sociale media. De Marnix Academie heeft niet als taak hier redactie op uit te voeren en is niet bij machte redactionele werkzaamheden uit te voeren of verantwoordelijkheid voor de inhoud te dragen.
- 6.3 Het is toegestaan dat de (externe) medewerker, studenten als 'vrienden' of contacten op sociale media toevoegt waarbij de verbinding en het contact uitsluitend plaats vindt op basis van wederzijds goedvinden en het accountsprofiel herleidbaar is naar de natuurlijke persoon. Elke gebruiker is gerechtigd om zonder opgave van reden en op elk moment de verbinding te verbreken.
- 6.4 Wanneer een (externe)medewerker een sociale-media-account opzet dat direct werk gerelateerd is, terwijl het op naam van medewerker persoonlijk is gesteld, zullen de (externe)medewerker en de Marnix Academie bij beëindiging van het dienstverband een passende oplossing zoeken voor het overdragen van dit profiel of de informatie en contacten daarop. Persoonlijke sociale-media-accounts waarop incidenteel werk gerelateerde berichten worden geplaatst, ge-liked of doorgestuurd zonderen hierop uit.
- 6.5 Om te kunnen voldoen aan de AVG en inzageverzoeken vindt communicatie tussen of onderling met de (externe)medewerkers, partners of studenten plaats via de door de Marnix Academie gefaciliteerde middelen mits: De inhoud persoonsgegevens, studiegegevens, beeldmateriaal bedoeld voor studie of financiële gegevens van de organisatie bevat.

7. Artikel 7. Monitoring en controle

- 7.1 Controle van gebruik van de ICT-faciliteiten en internetgebruik vindt slechts plaats in het kader van handhaving van de regels uit dit reglement voor de doelen genoemd in artikel 1. Verboden gebruik van de bedrijfsmiddelen wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.
- 7.2 Ten behoeve van controle op de naleving van de regels worden gegevens geautomatiseerd 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.
- 7.3 Bij vermoedens van overtreding van de regels kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen en alleen na toestemming van het CvB vindt controle op de inhoud plaats.
- 7.4 De Marnix Academie houdt zich bij het controleren op het niveau van verkeersgegevens of persoonsgegevens onverkort aan de AVG en andere relevante wet- en regelgeving.
- 7.5 Enkele specifieke maatregelen ter controle die de Marnix Academie kan voeren, zijn:
- 7.5.1 *Controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van filtering van de inhoud op trefwoorden. Verdachte berichten worden automatisch teruggestuurd naar de afzender;*
 - 7.5.2 *Controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot het op basis van verkeersgegevens nagaan van de bronnen van kosten of capaciteitsvraag (zoals de adressen van internetradio en videosites). Als deze websites tot grote kosten of overlast leiden, worden zij geblokkeerd of afgeknepen, zonder daarbij de vertrouwelijkheid van de inhoud van de communicatie te schenden;*
 - 7.5.3 *Controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.*

8. Artikel 8. Procedure bij gericht onderzoek

- 8.1 Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens betreffende een specifieke (externe)medewerker, partner of student worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit reglement door die (externe)medewerker, partner of student.
- 8.2 Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de desbetreffende leidinggevende resp. opleidingsmanager of CVB. In geval het onderzoek (leden van) het College van Bestuur betreft, wordt een dergelijke opdracht gegeven door de Raad van Toezicht. Het College van Bestuur c.q. Raad van Toezicht ontvangt een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd binnen een door het College van Bestuur c.q. Raad van Toezicht te bepalen termijn.
- 8.3 In afwijking van het vorige lid vindt gericht onderzoek naar de beveiliging of integriteit van randapparatuur plaats door het systeembeheer op basis van concrete aanwijzingen. Aparte toestemming van de in lid 2 bedoelde instantie is niet nodig. De resultaten van dit onderzoek worden alleen gedeeld met de (externe)medewerker, partner of student met het doel de beveiliging of integriteit van de randapparatuur te verbeteren. Bij herhaling zal de procedure uit lid 2 worden gevolgd.
- 8.4 Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan de Marnix Academie overgaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Dit vereist schriftelijke toestemming van het College van Bestuur c.q. de Raad van Toezicht, welke toestemming de redenen zal noemen waarom deze wordt verleend.
- 8.5 Enkele specifieke persoonsgebonden maatregelen ter controle die de Marnix Academie kan voeren, zijn:
 - 8.5.1 *Controle op het uitlekken van vertrouwelijke informatie vindt plaats op basis van steekproefsgewijze controle op trefwoorden. Verdachte berichten worden apart gezet voor nader onderzoek in overleg met het bestuur;*
 - 8.5.2 *Controle op overtreding van het verbod uit artikel 4 lid 3 vindt plaats door twee personen op klacht [of steekproefsgewijs] e-mailberichten te openen en de inhoud te raadplegen. Deze personen zijn gebonden aan geheimhouding over de inhoud.*
- 8.6 De (externe)medewerker, partner of student wordt zo spoedig mogelijk schriftelijk geïnformeerd door de leidinggevende resp. opleidingsmanager over de aanleiding, de uitvoering en het resultaat van het onderzoek. De (externe)medewerker, partner of student 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.
- 8.7 Systeembeheerders verschaffen zich slechts toegang tot accounts of computers van een (externe)medewerker, partner of student als de deze daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts na toestemming van het College van Bestuur toegestaan in dringende gevallen of bij een duidelijk vermoeden van schending van dit reglement, zoals nader bepaald in dit artikel. De medewerker zal in dat geval achteraf worden geïnformeerd.
- 8.8 Tijdens gericht onderzoek kan worden besloten om de (externe) medewerkers, partners en studenten het gebruik van faciliteiten te verbieden, het account te blokkeren of de, in bruikleen gestelde middelen, terug te geven aan de Marnix Academie. Er mag gevraagd worden om vrijwillig privé faciliteiten voor gericht onderzoek ter beschikking te stellen mits deze aantoonbaar onderdeel uitmaken van de overtreding van dit document.
- 8.9 De opdrachtgever voor het gericht onderzoek kan beslissen om het onderzoek door een externe, daartoe bevoegde, partij uit te laten voeren. Ook voor deze partij is dit reglement van toepassing.

9. Artikel 9. Consequenties van overtreding

- 9.1 Dit reglement gelden voor (externe) medewerkers, partners en studenten van de Marnix Academie als voorschriften met betrekking tot de goede gang van zaken binnen de instelling.
- 9.2 In geval een student handelt in strijd met dit reglement kan het College van Bestuur op basis van art. 7.57H WHW maatregelen treffen. Tegen een dergelijk besluit staat bezwaar en beroep open.
- 9.3 In geval een medewerker handelt in strijd met dit reglement kan het College van Bestuur maatregelen treffen op grond van de cao of de wet.
- 9.4 In geval van een externe medewerker of partner zal in overleg met de leidinggevende van de overtreder naar een maatregel gezocht worden. Als tussen de betreffende organisaties geen uitkomst is, is Marnix Academie gerechtigd conform artikel 9.3 of 9.5 te handelen.
- 9.5 Daarnaast kan de Marnix Academie aangifte doen bij de politie bij (vermoeden van) handelen in strijd met enige wet.

10. Artikel 10. Gebruik van niet- Marnix Academie gefaciliteerde faciliteiten

- 10.1 Met niet- Marnix Academie gefaciliteerde faciliteiten wordt onder andere bedoeld: laptops, Mac Books, Smartphones, Tablets, smartwatches, scanners, printers, internetverbindingen thuis of elders.
- 10.2 Het gebruik van niet- Marnix Academie gefaciliteerde faciliteiten voor werk en studie doeleinden zijn toegestaan mits dit de informatiebeveiliging en privacy niet in gevaar brengt en in lijn met dit reglement wordt gehandeld.
- 10.3 De eigenaar en/of gebruiker van de faciliteit is verantwoordelijk dat deze voldoende beschermd wordt door tenminste:
 - 10.3.1 *Virusscanner en firewall te gebruiken (m.u.v. smartdevices);*
 - 10.3.2 *Een wachtwoord, pincode of biometrische verificatie te gebruiken om toegang te krijgen;*
 - 10.3.3 *De regelmatig de software en het besturingssysteem te updaten;*
- 10.4 De Marnix Academie kan technische beleidsmaatregelen op de accounts van de Marnix Academie activeren waarmee de onder artikel 10.3 benoemde zaken kunnen worden afgedwongen alvorens de faciliteit voor werk of studiedoeleinden kan worden gebruikt;
- 10.5 Het gebruik van openbare wifi punten zonder identificatie wordt sterk afgeraden en is voor werkdoeleinden niet toegestaan.

11. Artikel 11. Slotbepalingen

- 11.1 Dit reglement wordt periodiek geëvalueerd door het College van Bestuur of de personen die zijn belast met werkzaamheden op het gebied van informatiebeveiliging en privacy en kan door hen worden herzien. Wijzigingen worden alleen bij het begin van een collegejaar ingevoerd, behalve in dringende gevallen of wanneer de Marnix Academie door omstandigheden van buitenaf gedwongen is tot een snellere invoering. Wijzigingen worden alleen ingevoerd nadat de Medezeggenschapsraad daarmee heeft ingestemd. In gevallen waarin dit Reglement niet voorziet, beslist het College van Bestuur.
- 11.2 Dit reglement is voor iedereen vindbaar op de publieke website van de Marnix Academie. Voor (externe)medewerkers, partners of studenten met een account van de Marnix Academie ook vindbaar in de applicatiewijzer op het portaal. Bij de eerste keer inloggen met een nieuw account van de Marnix Academie, wordt dit reglement eenmalig weergegeven ter accordering. Bij ingrijpende aanpassingen van dit reglement, kan er voor bestaande accounts worden gekozen om bij inloggen dit reglement wederom eenmalig weer te geven ter accordering. Wijzigingen van dit reglement zullen op het intranetportaal worden gepubliceerd middels een nieuwsbericht.
- 11.3 Gezond verstand van de (externe)medewerker, partner of student wordt verwacht. Bij onduidelijkheid kan via het servicepunt ondersteuning gevraagd worden als er vragen op het gebied van ICT, internet, informatiebeveiliging of sociale media zijn. Op het gebied van informatiebeveiliging en privacy kan men zich ook direct richten tot de securityofficer of functionaris gegevens bescherming. Als een (externe)medewerker, partner of student vermoeden heeft van inbreuk op misbruik wordt deze geacht dit binnen 1 werkdag te melden bij het Servicepunt.

11.4 Historie van het reglement:

Initieel: Dit Reglement vervangt het Reglement ICT- en Internetgebruik 2018 en kan worden aangehaald als Reglement ICT- en Internetgebruik. Dit Reglement treedt in werking op de dag nadat de Medezeggenschapsraad heeft ingestemd met (de aanpassing van) het Reglement.
Op 03-04-2022 hebben het college van bestuur en de medezeggenschapsraad ingestemd met aanpassingen op het gebruik van sociale media en enkele tekstuele wijzigingen.
Dit Reglement is vastgesteld door het College van Bestuur op 16 mei 2022.
De Medezeggenschapsraad heeft ingestemd op 21 juni 2022.
Mei 2023 is uitgebreide feedback verzameld (bij: Juriste, Functionaris gegevensbescherming en projectleider ICT) welke in dit reglement is verwerkt. De aanpassingen houden in: - tekstuele wijzigingen ter verduidelijking van de inhoud. - Actualisatie op benoeming van technologieën. - Artikel 6.5, 8.8 en 8.9 toegevoegd. - Artikel 10 toegevoegd - Indeling van artikel 11 (eerder 10) is ter verbetering van de leesbaarheid aangepast en aangevuld.
Dit reglement is opnieuw vastgesteld op 22 juni 2023 door het CVB en de MR heeft ingestemd op 22 juni 2023.