Opdracht Basic Security IT-Management aspect: InfoSec Policy

Inhoud

[1. Acceptable Infrastructure Use Policy 0](#_Toc445279902)

[2. Email policy 0](#_Toc445279903)

[3. Netwerk: wired - wireless 0](#_Toc445279907)

[4. Teleworker Policy (Remote Access) 0](#_Toc445279904)

[5. BYOD Policy 0](#_Toc445279905)

[6. BYOA Policy 0](#_Toc445279906)

[7. Printer policy 0](#_Toc445279908)

[8. PingPing 0](#_Toc445279909)

[9. Password policy 0](#_Toc445279910)

# Acceptable Infrastructure Use Policy

* Elke werknemer krijgt één email toegewezen bij het begin van zijn job aan de PXL. De email maakt gebruik van de voor- en achternaam van de werknemer bv ([voornaam.achternaam@pxl.be](mailto:voornaam.achternaam@pxl.be)) Het wachtwoord blijft hetzelfde als de werknemer kreeg bij het begin van zijn job. (indien zelfde naam -> cijfer toevoegen)
* Je mag niemand anders zijn account gebruiken, of proberen iemand anders zijn wachtwoord te stelen.
* Je bent zelf verantwoordelijk voor je gegevens inclusief je computer, netwerk adres poort, software en hardware. Als lid van de PXL mag je geen gebruikers toegang geven die geen toegang hebben.
* De hogeschool is gebonden door haar contractuele en licentie overeenkomsten. Je wordt dan ook verwacht dergelijke overeenkomsten na te leven bij het gebruik van deze middelen.
* Je moet een redelijke inspanning leveren om je wachtwoorden en je bestanden te beschermen tegen gebruikers die geen toegang hebben voor gebruik of toegang.
* Je mag niet proberen om beperkte gedeelte van het netwerk, een os, security software of andere administratieve applicaties zonder toestemming van de eigenaar of de beheerder toegang te krijgen.
* Wanneer andere beleidsterreinen meer beperkend zijn dan dit beleid, heeft het meer beperkende beleid voorrang.
* Je mag geen gebruik maken van netwerktoestellen of software met de bedoeling om schade en/of storingen te veroorzaken die andere toestellen of personeel in het systeem kunnen hinderen in het uitvoeren van hun functie.
* Je mag geen gebruik maken van tools die het mogelijk maken om onbevoegde toegang te verschaffen tot het system of onderdelen hiervan ( netwerk sniffers, paswoord krakers, kwetsbaarheid scanner, … ) ,tenzij u hier toestemming voor hebt gekregen van een bevoegd personeelslid die verantwoordelijk is voor de veiligheid van het systeem.

# Email policy

## Personeel

* Elke werknemer krijgt 1 email toegewezen bij het begin van zijn job aan de PXL. De email maakt gebruik van de voor- en achternaam van de werknemer bv ([voornaam.achternaam@pxl.be](mailto:voornaam.achternaam@pxl.be)) Het wachtwoord blijft hetzelfde als de werknemer kreeg bij het begin van zijn job. (indien zelfde naam -> cijferke)
* Indien de werknemer ontslagen wordt, wordt hij verwijderd uit het systeem. Dan kan hij/zij het email adres dat hij gekregen heeft niet meer gebruiken.
* De school email kan in school of vanuit de werknemer zijn thuis gecontroleerd worden.
* Het gebruik van het email systeem volgt het reglement van de school. Hieruit volgt dat het reglement ook kan worden gebruikt om misbruik te bestraffen van het email systeem.
* Indien er problemen ontstaan, zal het departement dit rechtstreeks met de werknemer afhandelen.
* Het doel van het email systeem is als communicatie tussen de werknemers (lector / student) en voor eventuele administratieve zaken.
* De werknemer is verantwoordelijk voor zijn eigen email account en de berichten die hiervan worden verzonden. De werknemer moet, en mag, zijn wachtwoord NIET delen met anderen.

## Studenten

* Elke student krijgt 1 email toegewezen bij het begin van zijn studies aan de PXL. De email maakt gebruik van de voor- en achternaam van de student bv ([voornaam.achternaam@student.pxl.be](mailto:voornaam.achternaam@student.pxl.be)) Het wachtwoord blijft hetzelfde als de student kreeg bij het begin van zijn studies. (indien zelfde naam -> cijferke)
* Indien de student afstudeert of stopt met zijn schoolcarrière, wordt hij/zij verwijderd uit het systeem. Dan kan hij/zij het email adres dat hij/zij gekregen heeft niet meer gebruiken.
* De school email kan in school of vanuit de student zijn thuis gecontroleerd worden.
* Het gebruik van het email systeem volgt het reglement van de school. Hieruit volgt dat het reglement ook kan worden gebruikt om misbruik te bestraffen van het email systeem.
* Indien er problemen ontstaan, zal het departement dit rechtstreeks met de student afhandelen.
* Het doel van het email systeem is als communicatie tussen de werknemers (lector / student) en voor eventuele administratieve zaken.
* De student is verantwoordelijk voor zijn eigen email account en de berichten die hiervan worden verzonden. De student moet, en mag, zijn wachtwoord NIET delen met anderen.

## Algemeen

* Het email system van school mag niet gebruikt worden voor persoonlijk gebruik en kan indien het gebeurt worden teruggetrokken wanneer het reglement wordt overtreden.
* De systeem administrators kunnen filters opzetten die virussen of grote grafische files die niet met het school gebeuren te maken hebben (bv. gelukwensen bij feestdagen) verwijderen.
* De mails die verzonden worden via het email systeem kunnen gemonitord worden.
* De PXL zal de toegang tot andere emaildiensten niet blokkeren.

Deze richtlijnen zijn onder voorbehoud en kunnen onderhevig zijn aan veranderingen.

# Netwerk: wired - wireless

## Algemeen

* In geval van examens wordt het draadloze netwerk voor desbetreffende studenten afgesloten.
* Via bekabeld netwerk zal er steeds een verbinding tot het netwerk mogelijk zijn.
* Het bekabeld netwerk is niet beveiligd met een wachtwoord.
* VPN’s mogen opgezet worden onder begeleiding van de IT dienst of leerkrachten IT in alle andere gevallen mag dit niet.

## Beveiliging

* Draadloos netwerk is voor iedereen met een wachtwoord toegankelijk via de login.
  + Voor de studenten is dit hun studentennummer + hun privé wachtwoord dat ze van de PXL gekregen hebben. Voor de lectoren is dit hun lectoren nummer + hun privé wachtwoord dat ze van de PXL gekregen hebben.

Voor de veiligheid van de studenten en lectoren behouden ze best hetzelfde wachtwoord wat ze van de PXL gekregen hebben, omdat dit reeds voldoet aan het wachtwoord policy van de PXL.

# Teleworker Policy (Remote Access)

## Personeel

* Alleen als de hogeschool PXL dit wenst, en kan ondersteunen, mag de werknemer werken als een teleworker.
* De werknemer moet permissie krijgen van de directie, of als docent, permissie van zijn departementshoofd.
* De goedkeuring van de permissie moet gepaard gaan met informatie van het beveiligingsrisico zoals: de locatie van waar men werkt als teleworker, het gebruik van vertrouwde informatie.
* Het personeel moet zorgen dat de teleworker faciliteiten ondersteund kunnen worden.
* Elk apparaat dat door de teleworker gebruikt wordt, moet worden goedgekeurd door de IT-dienst van de PXL.
* Indien het geval dat een teleworker moet omgaan met vertrouwde informatie, moet hij een pc krijgen van de hogeschool uit die werkt met een full disk encryptie systeem.

# BYOD Policy

## Algemeen

* Men mag zijn eigen device gebruiken voor persoonlijk gebruik tijdens de werkuren, zolang dit niet storend is voor de werkomgeving en de vooruitgang van het werk.
* Inbreuk op dit reglement wordt gevolgd door sancties volgens dat zelfde reglement.
* Het gebruik van een eigen device volgt alle policies vermeldt in dit document.
* De devices mogen niet gebruikt worden voor het opslaan en versturen van vertrouwelijke informatie, tenzij er een uitzondering wordt gemaakt door de directie of het departement.

## Risico’s

* De gebruiker is verantwoordelijk voor het verlies van data, persoonlijke of vertrouwelijke van de hogeschool, en zal, indien er inbreuk is op het reglement, gestraft worden.
* De gebruiker is verantwoordelijk voor zijn eigen back-up.

## Beveiliging

* Personeel dat omgaat met vertrouwelijke informatie hun device moet na inactiviteit van 5 minuten in een password protected slaapstand gaan.
* Het eigen device moet password protected zijn volgens de Password Policy.
* De gebruiker krijgt alleen toegang tot het netwerk van de hogeschool met de login gegevens die verkregen werden met tewerkstelling of inschrijven bij de hogeschool.

## Devices en support

* De gebruiker wordt niet vergoed voor het gebruik van zijn eigen device.
* Connectie problemen met het schoolwerk worden ondersteund door de IT-dienst en men kan dus met zijn eigen device hier terecht.
* Problemen met software nodig voor de werkomgeving worden ondersteund door de IT-dienst en men kan dus met zijn eigen device hier terecht.
* Elk device heeft de nodige software nodig voor het gebruik in de werkomgeving. De gebruiker is hier zelf verantwoordelijk voor.

# BYOA Policy

## Algemeen

* De app die wordt gebruikt, moet beveiligd zijn.
* Personeel en studenten kunnen applicaties voorbrengen aan de directie of het departement die besluiten of de app op de “white-list” wordt toegelaten.
* De app die wordt gebruikt moet van een door de directie of het departement goedgekeurde verkoper komen of behoort tot een specifieke categorie die door hen is goedgekeurd.
* In het geval dat er een informatielek is van vertrouwelijke informatie, wordt de gebruiker verantwoordelijk gesteld en volgen sancties volgens het reglement.

# Printer policy

## Bedrijfsprinters

* PXL zorgt voor standaard papier.
* PXL zorgt voor nieuwe kleurpatronen.
* PXL houdt de software van de printer up-to-date.
* PXL zorgt voor het onderhouden van de printer.
* PXL lost problemen in verband met de printer op.

## 3D-printers

* Er mag niets geprint worden dat verboden wordt door de wet.
* Er mag niets geprint worden dat niet veilig, gevaarlijk of een bedreiging vormt voor het welzijn van anderen.
* Er mag niets geprint worden dat niet gepast is in voor een schoolomgeving.
* Er mag niets geprint worden dat in strijd is met andermans eigendomsrechten. Dit betekent dat de printer niet gebruikt mag worden voor het printen van producten die merk beschermt zijn.
* PXL bezit het recht om alle 3D-print aanvragen te weigeren.
* Alleen aangewezen PXL medewerkers krijgen toegang tot het gebruik van de 3D-printer.

# PingPing

## Algemeen

* Alle PXL-studenten en – personeel zijn in het bezit van een studentenkaart. Deze kaart fungeert eveneens als PingPing-kaart en zij houden deze kaart strikt persoonlijk.
* Kortingen worden enkel verkregen indien met PingPing betaald
* Voor het vernieuwen van de PingPing-kaart bij het begin van een nieuw schooljaar is de student / het personeel zelf verantwoordelijk.
* Voor het opladen en het herladen van de PingPing-kaart is de student / het personeel zelf verantwoordelijk. Dit kan aan de 2 oplaadtoestellen in gebouw B en gebouw D.

## Printers

* Printers kunnen door iedereen met een PingPing-kaartje binnen het PXL-netwerk gebruikt worden. Het verschuldigde bedrag wordt dan getoond op de printer en betaald via je PingPing kaart.

## Automaten

* De automaten kunnen door iedereen met een pingping-kaartje binnen het PXL-netwerk gebruikt worden. Dit kan ook cash. Het verschuldigde bedrag wordt getoond op de automaat en betaald via je pingping kaart.

# Password policy

## Algemeen

* Alle werknemers en studenten hebben toegang tot het netwerk van de PXL. Hun logingegevens zijn strikt persoonlijk om het netwerk zo optimaal mogelijk te kunnen beveiligen, om data te beschermen en om andere computers op het netwerk te beschermen.
* Deze password policy is ontworpen om de bronnen op het netwerk te beschermen met sterke paswoorden.

## Paswoord lengte en formatie

* Het paswoord moet minstens 1 hoofdletter, 1 kleine letter, 1 getal en 1 speciaal teken ($, #, %, ...) bevatten.
* Het paswoord moet 8 tekens of langer zijn.
* Uw eigen naam/delen van uw eigen naam mogen niet voorkomen in het wachtwoord.
* Het wachtwoord mag niet hetzelfde zijn als één van de afgelopen 20 wachtwoorden.
* het wachtwoord mag niet starten met een '!'.
* Verboden karakters: ", é, è, à, ç, §, ù, °.

## Paswoord beveiliging

* Bewaar je paswoorden niet in de Cloud, op openbare plaatsen of lokaal op de computer.
* Schrijf je paswoord nooit op.
* Omvat nooit je paswoord in een niet-geëncrypteerd document.
* Vertel nooit je paswoord aan iemand.
* Geef je paswoord niet door via telefoon of e-mail.
* Geef je paswoord nooit vrij via een forum of via het internet.
* Als iemand achter je paswoord vraagt, verwijs dan door naar de IT-dienst.
* Wees voorzichtig bij het intypen van je wachtwoord.
* Verander je paswoord meteen wanneer je denkt dat andere je paswoord weten.
* Sinds paswoordbeveiliging kritiek is voor de veiligheid van de PXL en iedereen op het netwerk, mogen werknemers die zich niet houden aan deze policy een disciplinaire actie verwachten en in zeer ernstige gevallen eventueel ontslag.
* De PXL heeft elk account 1 gecompliceerd paswoord gegeven en dit kan gebruikt worden over het hele PXL netwerk.