

TOESTELBELEID

vzw Onderwijsinrichting van de Ursulinen te Onze-Lieve-Vrouw-Waver

voor:

Sint-Ursula-Instituut (instellingsnummers 126946, 126953, 126961)

Bosstraat 9

2861 Onze-Lieve-Vrouw-Waver

Deze nota maakt deel uit van het informatieveiligheids- en privacybeleid (IVPB).

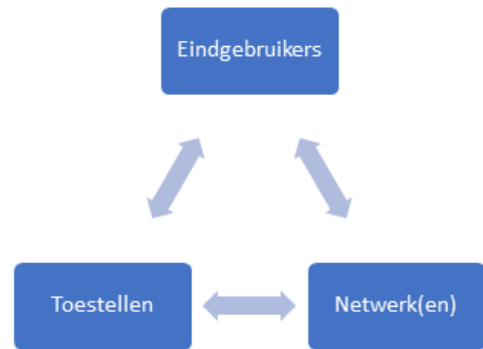
Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-05-25	GELDIG	A. Vanhaeren, AIV	

1. Inleiding

1.1 Algemeen

In een eenvoudige interpretatie zijn er drie aspecten van een modern ICT-netwerk om rekening mee te houden inzake beschikbaarheid, integriteit en vertrouwelijkheid:

- **(Eind)gebruikers** = *personen*
- **Toestellen** = *desktops, laptops, maar ook tablets, ... en ook: servers*
- **Netwerk(en)** = *de verbinding(en) tussen gebruikers en toestellen*



In deze nota wil het Sint-Ursula-Instituut enerzijds regels bepalen om de bijdrage van elk van deze drie aspecten in het IVP (Informatieveiligheid en privacy)-beleid te maximaliseren, en anderzijds wordt toegelicht hoe op het Sint-Ursula-Instituut **controle** op elk van deze aspecten gevoerd wordt.

Deze nota valt onder de eindverantwoordelijkheid van vzw Onderwijsinrichting van de Ursulinen te O.-L.-V.-Waver.

1.2 Algemene bepalingen

Ongeacht het "type" toestel of netwerk, zijn er een aantal maatregelen die het Sint-Ursula-Instituut steeds toepast. Hieronder worden deze opgesomd. In wat volgt, worden de specifieke maatregelen toegelicht.

- Het voorzien van manieren om te herkennen wanneer het "gewone" verkeer gemonitord, onderschept, nagebootst of gewijzigd wordt.
- Het combineren met een aantal monitoring tools en/of logboeken, d.w.z. manieren om de handelingen bij te houden voor analyse of eventueel naar bewijslast toe.
- In deze logboeken worden een aantal **identificatieparameters** geregistreerd. Er vinden geen ongeoorloofde inzages of systematische analyses plaats op deze gegevens. Enkel bij gegronde vermoedens van inbreuken kunnen hierop gerichte en/of willekeurige controles uitgevoerd worden. Alle informatie hier aangaande wordt strikt vertrouwelijk behandeld.

2. Netwerkbeveiliging en -controle

2.1 Bekabeld netwerk en servers

Met het “bekabelde netwerk” bedoelen we het geheel van componenten die de netwerkverbindingen maken en beheren, zoals: routers, switchen, hubs, kabels, servers, modems, ...

De algemene maatregelen (zie § 1.2) worden toegepast, met in het bijzonder logging van: tijdsregistratie, MAC- en IP-adressen, toestelnamen, gebruikersnamen.

Wachtwoorden op de netwerkcomponenten worden systematisch gewijzigd t.o.v. de “default” waarden, of te gemakkelijke combinaties. De gekozen wachtwoorden voldoen in het bijzonder aan alle afspraken uit het **wachtwoordbeleid**.

2.2 Wifi-netwerk

Voor personeel, leerlingen en gasten is wifi voorzien in het Sint-Ursula-Instituut. Deze dienst is gratis voor de eindgebruikers, maar heeft voor de school wel een zekere kostprijs (in aanschaf, onderhoud en beveiliging).

Daarom wordt de aard en hoeveelheid van het netwerkverkeer gemonitord.

De algemene maatregelen (zie § 1.2) worden toegepast, met in het bijzonder logging van: tijdsregistratie, MAC- en IP-adressen, toestelnamen, gebruikersnamen.

Het datagebruik via het draadloze netwerk wordt bijgehouden in logboeken en kan desgevallend wel geanalyseerd worden, als het globale verbruik dit rechtvaardigt. Alle informatie hier aangaande wordt strikt vertrouwelijk behandeld.

Het netwerkverkeer dat via het draadloze netwerk verloopt, wordt versleuteld.

3. Beveiliging en controle op internetverkeer

In het Sint-Ursula-Instituut is er, zowel voor de toestellen die eigendom zijn van de school als op bepaalde andere toestellen (zie ook § 2.2, § 4 en § 5), een internetverbinding mogelijk.

Als organisatie is het Sint-Ursula-Instituut verantwoordelijk voor het algehele dataverbruik, en voor alles dat er met / via deze internetverbinding gebeurt. Daarom hanteert men ook hier een aantal regels en controles daarop.

De beheerders, noch de elektronische controlesystemen en de logboeken, hebben op geen enkele manier toegang tot de inhoud van persoonlijke berichten (zoals messaging, e-mail, intern communicatiesysteem, ...).

4. Beveiliging en controle op toestellen van de school

Onder “toestellen” van de school rekenen we zowel desktop computers, laptops als tablets.

4.1 Algemeen

De volgende beveiligingsregels resp. -controles kunnen hierop (tegelijkertijd) toegepast worden:

- Het internetverkeer en de gebruikte toepassingen worden, op verscheidene niveaus, gecontroleerd inzake bv. uitgaand verkeer, capaciteit maar ook veiligheid van de toepassing, het al dan niet veranderen van systeeminstellingen (gerelateerd aan beveiliging resp. prestaties, enz.)
- De beheerders steken veel tijd en geld in het zo vlot mogelijk “draaiend” houden van alle hardware en het netwerk. Dit is onmogelijk als gebruikers de systeem- of beveiligingsinstellingen veranderen. Er worden in het Sint-Ursula-Instituut dan ook verschillende maatregelen genomen om dit te verhinderen. Het doelbewust veranderen van systeem- of beveiligingsinstellingen is verboden.

Dit beleid wordt gecombineerd met een aantal monitoring tools en/of (lokale) logboeken, d.w.z. manieren om de handelingen bij te houden voor analyse of eventueel naar bewijslast toe. De algemene maatregelen (zie § 1.2)

worden toegepast, met in het bijzonder logging van: tijdsregistratie, MAC- en IP-adressen, gebruikersnamen, toestelnamen, logintijd, gebruikte toepassingen, wijzigingen in systeeminstellingen.

- In het Sint-Ursula-Instituut kunnen er, in het kader van support, bepaalde tools gebruikt worden die de actieve vensters en/of het realtime beeldscherm van de eigen toestellen kunnen monitoren. De doeleinden hiervan zijn louter en alleen pedagogisch. Het is in het bijzonder leraren en ondersteunend personeel *niet* toegestaan om zonder concreet vermoeden van doelbewuste en ernstige inbreuken, schermafdrucken te bewaren, een scherm op te nemen of een scherm over te nemen zonder toestemming van de betrokkene.
- Leraren en ondersteunend personeel kunnen, in het kader van hun uit te oefenen taak, de actieve vensters, geopende websites en/of het beeldscherm zien. Het is niet uitgesloten dat de inhoud van **persoonlijke berichten** (ontvangen en/of verzonden) leesbaar is, alhoewel dit nooit het doel op zich zal zijn. Al deze medewerkers behandelen de informatie strikt vertrouwelijk, en bewaren deze niet.
- Het is, met dezelfde tools, wel toegestaan dat de beheerders de schermen bewaren (als een schermafdruck of als een opname). Zij doen dit enkel bij een concreet vermoeden van doelbewuste en ernstige inbreuken, en alle informatie wordt strikt vertrouwelijk behandeld. Onbevoegde medewerkers hebben geen toegang tot de schermafdrucken of opnames.

4.2 Vergrendeling, encryptie en wissen van op afstand

De mobiele toestellen (d.w.z. laptops, tablets, smartphones) die bepaalde personeelsleden gebruiken maar die eigendom zijn van het Sint-Ursula-Instituut, dienen extra beveiligd te worden indien er persoonsgegevens op bewaard, bekeken of verwerkt worden.

In het bijzonder wordt er een vergrendeling aan de hand van wachtwoord, pincode, swipe code, vingerafdruk of andere authenticatie toegepast.

Voor directie, ondersteunend personeel dat toegang heeft tot gevoelige persoonsgegevens op het toestel in kwestie, zorgverantwoordelijken en CLB geldt bovendien:

- Encryptie van opslagmedia (indien mogelijk);
- Optie om te lokaliseren of te wissen van op afstand, in geval van diefstal of verlies (indien mogelijk). Dit laatste is enkel mogelijk voor tablets (meer bepaald iPad) en niet voor laptops.

5. Beveiliging en controle op toestellen van eindgebruikers zelf



In het Sint-Ursula-Instituut is het mogelijk om, via het netwerk of wifi van de school (zie ook § 2.2), gebruik te maken van eigen toestellen. Het is de bedoeling dat deze maximaal gebruikt worden om taken uit te voeren, gerelateerd aan de onderwijsinstelling.

5.1 Algemeen

Inzake een eigen toestel zijn een aantal beveiligings- en beheerdersaspecten anders dan in § 4. Desalniettemin gelden alle principes van deze paragraaf evenzeer voor handelingen gerelateerd aan het Sint-Ursula-Instituut, die uitgevoerd worden op een eigen toestel. Zie, naast § 4 uit deze nota, ook het algemene **communicatiebeleid**. De bijzondere regels en afspraken inzake het BYOD¹-beleid, zijn:

Het internetverkeer en gebruikte toepassingen wordt, op verscheidene niveau's, gecontroleerd inzake bv. uitgaand verkeer, capaciteit maar ook veiligheid van de toepassing, het al dan niet veranderen van systeeminstellingen (gerelateerd aan beveiliging resp. prestaties, enz.).

De algemene maatregelen (zie § 1.2) worden toegepast, met in het bijzonder logging van: MAC- en IP-adressen, gebruikersnamen, toestelnamen, logintijd, gebruikte toepassingen, wijzigingen in systeeminstellingen, enz.

5.2 Vergrendeling, encryptie, antivirusbeveiliging, backups en wissen van op afstand

De mobiele toestellen (d.w.z. laptops, tablets, smartphones) van medewerkers, waarop persoonsgegevens van het Sint-Ursula-Instituut bewaard, bekeken of verwerkt worden, dienen extra beveiligd te worden. De school vraagt die medewerkers dan ook om de volgende maatregelen op deze toestellen in acht te nemen:

- Er wordt een vergrendeling aan de hand van wachtwoord, pincode, swipe code, vingerafdruk of andere authenticatie gevraagd.
- Er wordt gevraagd om een ten allen tijde up-to-date antivirusprogramma te gebruiken.
- Backups dienen genomen, bewaard en beheerd te worden.

Voor directie, ondersteunend personeel dat toegang heeft tot gevoelige persoonsgegevens op het toestel in kwestie, zorgverantwoordelijken en CLB wordt daarenboven het volgende gevraagd:

- Encryptie van opslagmedia (indien mogelijk);
- Optie om te lokaliseren of te wissen van op afstand, in geval van diefstal of verlies (indien mogelijk). Dit laatste is enkel mogelijk voor tablets (meer bepaald iPad) en niet voor laptops.

¹ BYOD = "bring your own device". Het gebruik van eigen toestellen voor schoolgerelateerde processen.