

TOESTELBELEID

Don Bosco Onderwijscentrum VZW

voor:

Don Bosco Halle Technisch Instituut / Centrum Leren & Werken

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

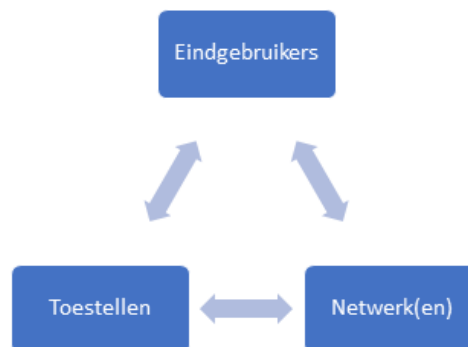
Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-05-26	GELDIG		

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, smartphones, ... en ook: servers*
- **Netwerk(en)** = *de verbinding(en) tussen gebruikers en toestellen*



In deze nota wil Don Bosco Halle Technisch Instituut / Centrum Leren & Werken enerzijds regels bepalen om de bijdrage van elk van deze drie aspecten in het IVP-beleid te maximaliseren, en anderzijds wordt toegelicht hoe op Don Bosco Halle Technisch Instituut / Centrum Leren & Werken **controle** op elk van deze aspecten gevoerd wordt.

Deze nota valt onder de eindverantwoordelijkheid van Don Bosco Onderwijscentrum VZW.

1.2 Algemene bepalingen

Ongeacht het "type" toestel of netwerk, zijn er een aantal maatregelen die Don Bosco Halle Technisch Instituut / Centrum Leren & Werken kan toepassen. 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) kunnen worden toegepast, met i.h.b. logging van: MAC- en IP-adressen, gebruikersnamen, toestelnamen, logintijd, gebruikte toepassingen, wijzigingen in systeeminstellingen, enz.

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

2.2 Wifi-netwerk

Voor personeel, leerlingen en gasten is wifi voorzien op Don Bosco Halle Technisch Instituut / Centrum Leren & Werken. 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) kunnen worden toegepast, met in het bijzonder logging van: MAC- en IP-adressen, gebruikersnamen, toestelnamen, logintijd, gebruikte toepassingen, wijzigingen in systeeminstellingen, enz.

Ook de bezochte websites of applicaties, en het datagebruik via het draadloze netwerk, kunnen bijgehouden worden in logboeken en kunnen 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 *niet* versleuteld. Het raadplegen, bewerken enz. van persoonsgegevens wordt dan ook ten stelligste afgeraden, tenzij er een andere vorm van versleuteling gehanteerd wordt (bv. *https* i.p.v. *http*).

Dit wifi-netwerk is onbeveiligd

Telkens wanneer u zich aanmeldt bij een onbeveiligd netwerk, kan iedereen zien wat u online uitspookt.

3 Beveiliging en controle op internetverkeer

Op Don Bosco Halle Technisch Instituut / Centrum Leren & Werken is er, zowel voor de toestellen die eigendom zijn van de school als op andere toestellen (zie ook § 2.2, § 4 en § 5), een internetverbinding mogelijk.

Als organisatie kan Don Bosco Halle Technisch Instituut / Centrum Leren & Werken het dataverbruik, en alles dat er met / via deze internetverbinding gebeurt, loggen.

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

4 Beveiliging en controle op toestellen van de school

Onder “toestellen” van de school rekenen we zowel desktop computers, laptops, tablets als (eventuele) werk-smartphones die eigendom zijn van de school.

4.1 Algemeen

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

- Het internetverkeer en gebruikte toepassingen kunnen op verscheidene niveaus gecontroleerd worden inzake bv. bezochte doelsites, 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 op Don Bosco Halle Technisch Instituut / Centrum Leren & Werken dan ook verschillende maatregelen genomen om dit te verhinderen.

Dit beleid kan gecombineerd worden 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) die toegepast kunnen worden, met in het bijzonder naar logging toe, zijn: tijdsregistratie, MAC- en IP-adressen, gebruikersnamen, toestelnamen, logintijd, gebruikte toepassingen, wijzigingen in systeeminstellingen.

- Op Don Bosco Halle Technisch Instituut / Centrum Leren & Werken kunnen 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 leerkrachten 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.
- Leerkrachten 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, directie en eventueel andere personeelsleden die hiervoor bevoegd geacht worden, 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, pda's, tablets, smartphones) die bepaalde personeelsleden gebruiken maar die eigendom zijn van Don Bosco Halle Technisch Instituut / Centrum Leren & Werken, dienen extra beveiligd te worden indien er persoonsgegevens op bewaard, bekeken of verwerkt worden.

In het bijzonder wordt er een vergrendeling a.d.h.v. wachtwoord, pincode, swipe code, vingerafdruk of andere authenticatie toegepast.

Voor directie, ondersteunend personeel en iedereen die toegang heeft tot gevoelige persoonsgegevens op het toestel in kwestie 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)

5 Beveiliging en controle op toestellen van eindgebruikers zelf

Op Don Bosco Halle Technisch Instituut / Centrum Leren & Werken is het mogelijk om, via het netwerk of wifi van de school (zie ook § 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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken, 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 kunnen op verscheidene niveaus gecontroleerd worden inzake bezochte doelsites, uitgaand verkeer, capaciteit, maar ook de veiligheid van de toepassing en het al dan niet veranderen van systeeminstellingen (gerelateerd aan beveiliging).

De algemene maatregelen (zie § 1.2) kunnen 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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken bewaard, bekeken of verwerkt worden, dienen extra beveiligd te worden. Dit beleid vraagt die medewerkers dan ook om de volgende maatregelen op deze toestellen in acht te nemen:

- Er wordt een vergrendeling a.d.h.v. 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 zoals in het respectievelijke beleid vastgelegd.

Voor directie, ondersteunend personeel en iedereen die toegang heeft tot gevoelige persoonsgegevens op het toestel in kwestie 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)

¹ BYOD = “bring your own device”. Het gebruik van eigen toestellen op en voor schoolgerelateerde processen.

bring your own device
BYOD
device
security
governance
network security
consumerization
manage
applications
configure
security policy
corporate network
smartphone
connectivity
tablet
encryption
laptop
passwords