



TOESTELBELEID

Voor:

- 104571 Vrije Basisschool Sjabi, Begijnhofstraat 8, 2870 Puurs-Sint-Amands (Puurs),
- 025817 Vrije Basisschool voor Buitengewoon Onderwijs De Wissel, Kleine Amer 20, 2870 Puurs-Sint-Amands (Kalfort),
- 010645 Vrije Basisschool Klavertjevier, Breendonk-Dorp 94, 2870 Puurs-Sint-Amands (Breendonk),
- 010793 Vrije Kleuterschool De Regenboog, Coolhemveldstraat 3, 2870 Puurs-Sint-Amands (Kalfort),
- 010769 Vrije Lagere School Twinkelveld, Winkelveld 1, 2870 Puurs-Sint-Amands (Kalfort),
- 104174 SJABI Eerste Graadschool, Kerkplein 15, 2870 Puurs-Sint-Amands (Puurs),
- 104166 SJABI Bovenbouw ASO-TSO-BSO, Begijnhofstraat 3-5, 2870 Puurs-Sint-Amands (Puurs),
- 027664 SJABI BuSO, Hof-Ten-Berglaan 8, 2870 Puurs-Sint-Amands (Puurs),
- 010629 Vrije Basisschool De Krinkel, Ruisbroek-Dorp 38, 2870 Puurs-Sint-Amands (Ruisbroek),
- 010637 Vrije Basisschool Sint-Carolus, Kloosterstraat 1, 2870 Puurs-Sint-Amands (Ruisbroek),
- 010819 Vrije Basisschool Liezele, Turkenhofdreef 2, 2870 Puurs-Sint-Amands (Liezele),
- 010827 Vrije Basisschool Libos, Lippelodorp 48, 2890 Puurs-Sint-Amands (Lippelo),
- 010835 Vrije Basisschool De Kameleon, Oppuursdorp 41, 2890 Puurs-Sint-Amands (Oppuurs),
- 010892 Vrije Kleuterschool Zonnebloem, Hekkestraat 1, 2890 Puurs-Sint-Amands (Sint-Amands),
- 010884 Vrije Lagere School Zonnebloem, Hekkestraat 1, 2890 Puurs-Sint-Amands (Sint-Amands).

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

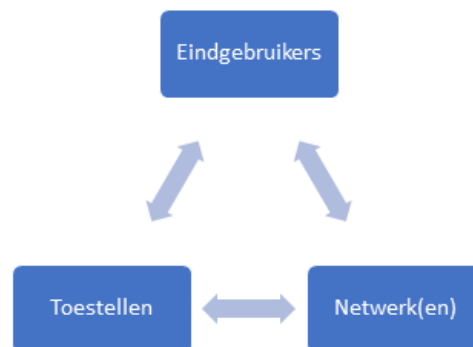
Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-12-18	GELDIG	Gunter Aerts Hilde Claes	
1.1	2022 03 10	GELDIG	Gunter Aerts Erik Van De Voorde	

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



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

Deze nota valt onder de eindverantwoordelijkheid van Sint-Jan Berchmansinstituut VZW.

1.2 Algemene bepalingen

Ongeacht het “type” toestel of netwerk, zijn er een aantal maatregelen die de instelling 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 inzagen 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 i.h.b. 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 i.h.b. aan afspraken uit het **wachtwoordbeleid**.

2.2 Wifi-netwerk

Voor personeel, leerlingen en gasten is wifi voorzien op de instelling. 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 i.h.b. logging van: tijdsregistratie, MAC- en IP-adressen, toestelnamen, gebruikersnamen.

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

3 Beveiliging en controle op internetverkeer

Op de instelling 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 de instelling 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 algemene maatregelen (zie § 1.2) worden toegepast, met i.h.b. logging van: tijdsregistratie, MAC- en IP-adressen, toestelnamen, gebruikersnamen.

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

4 Beveiliging en controle op toestellen van de school

Onder "toestellen" van de school rekenen we zowel desktopcomputers, 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 de gebruikte toepassingen worden, op verscheidene niveaus, gecontroleerd 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 de instelling 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 i.h.b. logging van: tijdsregistratie, MAC- en IP-adressen, gebruikersnamen, toestelnamen, logintijd, gebruikte toepassingen, wijzigingen in systeeminstellingen.

- Op de instelling worden er (op sommige toestellen) bepaalde tools gebruikt die de actieve vensters en/of het realtime beeldscherm van de eigen toestellen kunnen monitoren. Dit gebeurt echter enkel mits voorafgaande toestemming van de gebruiker.
- Personeelsleden 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 zijn. Al deze personeelsleden behandelen de informatie strikt vertrouwelijk, en bewaren deze niet.
- Het is wel toegestaan dat de beheerders, directie en eventueel andere personeelsleden die hiervoor bevoegd geacht worden de schermen bewaren (als een schermafdruk 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 personeelsleden 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 de instelling, dienen extra beveiligd te worden indien er persoonsgegevens op bewaard, bekeken of verwerkt worden.

I.h.b. wordt er een vergrendeling a.d.h.v. 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)

5 Beveiliging en controle op toestellen van eindgebruikers zelf



Op de instelling 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 de instelling, 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 niveaus, gecontroleerd 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 algemene maatregelen (zie § 1.2) worden toegepast, met i.h.b. logging van: MAC- en IP-adressen, gebruikersnamen, toestelnamen, logintijd, gebruikte toepassingen.

5.2 Vergrendeling, encryptie, antivirusbeveiliging, back-ups en wissen van op afstand

De mobiele toestellen (d.w.z. laptops, pda's, tablets, smartphones) van medewerkers, waarop persoonsgegevens van de instelling 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 te allen tijde up-to-date antivirusprogramma te gebruiken.
- Back-ups dienen genomen, bewaard en beheerd te worden zoals in het respectievelijke beleid vastgelegd.

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);

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

- Optie om te lokaliseren of te wissen van op afstand, in geval van diefstal of verlies (via Intune of via de domeinadministratieve accounts)