

TOESTELBELEID



CKSA

School De Brug

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

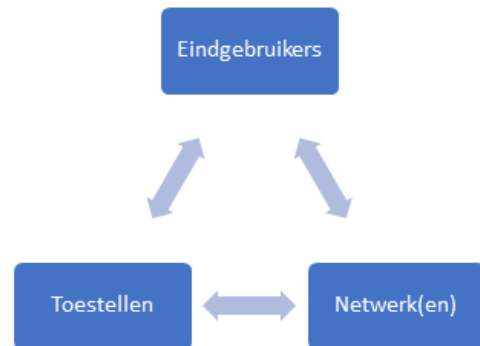
| Datum | Auteur(s) | Opmerking |
|------------|----------------|--|
| 2018-05-26 | | sjabloon Katholiek Onderwijs Vlaanderen wordt terbeschikking gesteld |
| 2018-12-04 | CIV | aangepast sjabloon schoolbestuur wordt overhandigd aan directies |
| 2020-01-10 | School De Brug | finalisering schooleigen document |
| | | |
| | | |

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

Deze nota valt onder de eindverantwoordelijkheid van schoolbestuur CKSA.

1.2 Algemene bepalingen

Ongeacht het "type" toestel of netwerk, zijn er een aantal maatregelen die CKSA 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 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 aan alle afspraken uit het document ivm wachtwoordbeleid.

2.2 Wifi-netwerk

Voor personeel, leerlingen en gasten is wifi voorzien op CKSA en op alle CKSA-scholen. 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.

Ook de bezochte websites of applicaties, en het datagebruik via het draadloze netwerk, 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 *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*).

3 Beveiliging en controle op internetverkeer

Op alle CKSA-scholen 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 CKSA 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.

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 de gebruikte toepassingen worden, op verscheidene niveau's, 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 CKSA 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.

- Binnen CKSA 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 i.h.b. 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, tablets, smartphones) die bepaalde personeelsleden gebruiken maar die eigendom zijn van CKSA, 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)

4.3 Leasingtoestellen en/of huurkooptoestellen

Dezelfde beveiligingsregels als in § 4.1 en § 4.2 gelden hiervoor.

Indien het toestel op het einde van de looptijd van de leasing terug aan CKSA en/of aan de school overgemaakt wordt, dan zullen alle gegevens op de interne opslag verwijderd worden, zonder inzage of controle op de inhoud.

Pas na het wissingsproces zal het toestel terug in gebruik genomen worden.

5 Beveiliging en controle op toestellen van eindgebruikers zelf



Op CKSA-scholen 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 werkgerelateerde handelingen 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. 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.

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 CKSA-scholen worden bewaard, bekeken of verwerkt, 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 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)

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