Hellingstraat 44
1800 Vilvoorde
Tel 02 257 10 49
info@kov.be www.kov.be

Toestelbeleid

KOV vzw

Met volgende instellingen:

Basisonderwijs:

- **De Biekorf**
- **De Knipoog**
- **De Lampion**
- **Heilig-Hartschool**
- **Sint-Jozef Groenstraat**
- **De Windroos**
- **Parochiale Basisschool Diegem**

Buitengewoon lager onderwijs:

- **Klavertje Vier**

Secundair onderwijs:

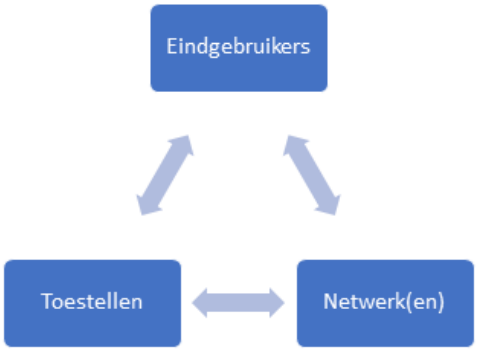
- **Het College**
- **TechnOV**
- **Virgo Plus**
- **Topsportinternaat volleybal**

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

Aangemaakt: 10/09/2021 - Laatst aangepast: 9/10/2023 - Document revisienummer: 11

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

Deze nota valt onder de eindverantwoordelijkheid van KOV vzw.

1.2 Algemene bepalingen

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

2.2 Wifi-netwerk

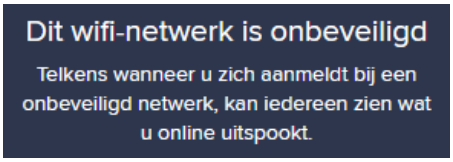
Voor personeel, leerlingen en gasten is wifi voorzien op KOV vzw. Deze dienst is gratis voor de eindgebruikers, maar heeft voor de school wel een zekere kostprijs (in aanschaf, onderhoud en beveiliging).

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.

De bezochte websites of applicaties, en het datagebruik op het bedraad en/of draadloze netwerk wordt 7 dagen 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 is 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 KOV vzw 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 KOV vzw 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, 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.

Zie ook Artikel 6 uit addendum aan de arbeidsovereenkomst over het ter beschikking stellen van een laptop

4.1 Algemeen

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

- 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 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 KOV vzw 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.

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 KOV vzw, 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 en zorgverantwoordelijken geldt bovendien:

- 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 KOV vzw 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 KOV vzw, die uitgevoerd worden op een eigen toestel. Zie, naast § 4 uit deze nota, ook het algemene ***communicatiebeleid***. De bijzondere regels en afspraken inzake het BYOD[1]-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, wijzigingen in systeeminstellingen, enz.

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

De mobiele toestellen (d.w.z. laptops, pda's, tablets, smartphones) van medewerkers, waarop persoonsgegevens van KOV vzw 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.
- Werkdocumenten dienen op de juiste plaats bewaard te worden zodat de nodige backups kunnen genomen en beheerd worden zoals in het respectievelijke beleid vastgelegd.

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

- Encryptie van lokale opslagmedia wordt aanbevolen wordt voorbereid
- 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.


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