Databeveiligingsmaatregelen

Fysieke toegang

- De toegang tot het kantoor is fysiek beperkt tot personen die daartoe bevoegd zijn (door middel van een sleutel) tenzij de beheerder en/of de administratief medewerker en/of kerkenraadsleden aanwezig zijn.
- Er is een adequaat sleutel*b*eheer.
- Op papier gedrukte gevoelige en/of bijzondere persoonsgegevens staan in een afgesloten kast.
- Er geldt een clean desk en clear screen policy.

Toegangsrechten/autorisatie

- Toegang tot mappen op de harde schijf/server is beperkt op een need to know basis.
- Toegang tot IT-platformen en onderdelen daarvan is beperkt op een need to know basis.
- Toegang tot (bijzondere en/of gevoelige) personeelsgegevens is beperkt op een need to know basis.
- Toegangsrechten worden aangepast bij een functiewissel/taakwissel.
- Toegangsrechten worden op de dag dat de arbeidsovereenkomst c.q. de actieve arbeid van een medewerker of vrijwilliger eindigt ingetrokken.

Netwerkbeveiliging

- Er is adequate beveiliging bij toegang tot het netwerk waaronder identificatie van vertrouwde apparaten.

IT-middelen

- Er is een overzicht van IT-middelen waarop persoonsgegevens worden verwerkt. (computers, laptops, tablets, telefoons, printer met dataopslag, USB-sticks)
- De toegang tot desktopcomputers is beveiligd met een adequaat wachtwoord.

Wachtwoorden

- Er zijn afspraken over wachtwoorden en wachtwoordbeheer.
- Er worden geen eenvoudig te raden wachtwoorden gebruikt.
- De wachtwoorden worden niet opschreven, tenzij dit geschiedt in een beveiligde wachtwoordkluis.
- Wachtwoorden/inloggegevens worden niet automatisch opgeslagen.
- Wachtwoorden worden niet gedeeld.
- Wachtwoorden worden jaarlijks veranderd.
- Er zijn automatische controles/procedures die leiden tot het instellen van een sterk wachtwoord.
- Een sterk wachtwoord bestaat uit minimaal 8 tekens, waarvan, 1 hoofdletter, een kleine letter, een cijfer en een speciaal teken. (stand 2017/2018)
- Bij meer dan 3 inlogpogingen wordt de toegang – gedurende een periode – ontzegd.
- Bij een foute inlogpoging wordt enkel vermeld dat er sprake is van een foutieve combinatie van inloggegevens. Er wordt niet vermeld of de gebruikersnaam actief is.
- Het bovenstaande geldt voor alle inlogprocedures.

Opslag

- Persoonsgegevens worden beveiligd opgeslagen.
- Er zijn heldere afspraken met medewerkers en vrijwilligers over de plaats waarop persoonsgegevens worden opgeslagen. (netwerkmappen, lokale mappen, e-mails, andere plaatsen).
- Gebruik beveiliging op netwerkmappen en waar nodig ook beveiliging op bestanden op het netwerk.

Beveiligingsmaatregelen

- Er is overzicht op welke plaatsen de data fysiek staat opgeslagen.
- De server is adequaat beveiligd.

Verwijdering van persoonsgegevens

- Wettelijke termijnen worden toegepast
- IT-hardware en USB sticks worden op adequate wijze gewist of vernietigd, wanneer zij niet meer worden gebruik.
- De papieren versies van (gevoelige of bijzondere) persoonsgegevens worden adequaat vernietigd.

Dataverkeer

- Bij het verkrijgen van persoonsgegevens via het internet wordt gebruik gemaakt van beveiligde protocollen zoals een ssl-certificaat (https).
- Lijsten met ledengegevens worden beveiligd verstuurd mbv een wachtwoord.

Software

- De laatste versie van het besturingsprogramma is geïnstalleerd op *de* apparaten.
- Gebruikte software is voorzien van de laatste updates.

Malware/virussen

- Er is een up to date firewall en virusscanner op alle IT-middelen geïnstalleerd.
- Medewerkers zijn verplicht USB sticks en andere verwijderbare media die worden aangesloten op het netwerk eerst te scannen op virussen of dit gebeurt (bij voorkeur) automatisch.

Back-up

- Er is een regelmatige back-up van de gegevens (dagelijks/wekelijks).
- De back-up omvat alle persoonsgegevens. Niet alleen netwerkmappen op de server en e-mails, maar ook lokale mappen voor zover daar persoonsgegevens staan opgeslagen die niet ook op de server staan.
- De back-up wordt jaarlijks getest.
- De back-up is beveiligd.

Mobiele apparaten (laptops/tablets/telefoons)

- Mobiele apparaten zijn fysiek beveiligd indien niet in gebruik. (achter slot en grendel)
- Mobiele apparaten zijn technisch beveiligd (wachtwoord, firewall, antivirus, automatisch sessie beëindigen, etc.).
- Er worden zo min mogelijk persoonsgegevens opgeslagen op mobiele apparaten.
- Opslag geschiedt bij voorkeur centraal via een virtuele desktoptoegang en niet op het apparaat.

Printer

- Het is mogelijk om gevoelige gegevens c.q. personeelsgegevens op een beveiligde of apart toegankelijke printer te printen.

Webapplicaties

- Verwerking door verwerkers gebeurt alleen op basis van verwerkersovereenkomsten.

Kennis en bewustwording

- Bij medewerkers is de nodige kennis aanwezig om adequaat met persoonsgegevens en IT-middelen om te gaan.
- Bij vrijwilligers is de nodige kennis aanwezig om adequaat met persoonsgegevens en IT-middelen om te gaan.

Evaluatie en ontwikkeling

- Test en evalueer jaarlijks de effectiviteit van het beleid, de maatregelen en de beveiliging.
- Blijft up to date van actuele (technische) beveiligingsmaatregelen.
- Voer de nodige verbeteringen door op basis van de evaluatie en externe ontwikkelingen.