Databeveiligingsmaatregelen voor verenigingen

Beveiligingsmaatregelen

Fysieke toegang

- De toegang tot het kantoor is fysiek beperkt tot personen die daartoe bevoegd zijn. (bijvoorbeeld door middel van een sleutel/pasje/code, al dan niet aangevuld met toegangsregistratie.)
- Er is een adequaat sleutel-, toegangscode- en alarmcodebeheer.
- De toegang tot de ruimtes waar persoonsgegevens staan opgeslagen is fysiek beperkt tot personen die daartoe bevoegd zijn. (bijvoorbeeld door middel van slot&sleutel.)
- Op papier gedrukte gevoelige of bijzondere persoonsgegevens (zoals personeelsgegevens) staan in een afgesloten kast. Overige persoonsgegevens staan in een ruimte die kan worden afgesloten en is afgesloten indien er niemand aanwezig is.
- 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 personeelsgegevens is beperkt op een need to know basis.
- Toegang tot bijzondere of gevoelige persoonsgegevens is beperkt op een need to know basis (denk aan medische gegevens).
- Toegangsrechten van gebruikers worden adequaat beheerd en geactualiseerd.
- 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.
- Er is adequate beveiliging bij toegang tot het netwerk waaronder een lijst van ‘geblokkeerde’ landen van waaruit geen toegang tot het netwerk mogelijk is of een lijst van landen van waaruit wel toegang mogelijk is. Voor veel verenigingen zal ‘alleen Nederland’ volstaan.

Verenigingswifi-netwerk

- Bestuur, medewerkers en eventueel commissieleden hebben een apart wifikanaal gescheiden van het wifikanaal voor leden/gasten. (I.v.m. toegang tot het netwerk en de server.)
- Het wifi-wachtwoord van het hoofdkanaal is enkel bekend bij de bevoegde personen en het wordt niet gedeeld met leden/gasten?
- Voor leden en gasten is er een ‘gast-wifi’

Beheer van IT-middelen

- Er is een overzicht van IT-middelen waarop persoonsgegevens worden verwerkt. (computers, laptops, tablets, telefoons, printer met dataopslag, USB-sticks)
- Er is een overzicht van de IT-middelen van de vereniging waarop persoonsgegevens worden verwerkt. (computers, laptops, tablets, telefoons, printer met dataopslag, USB-sticks)
- Er is adequaat beheer van de IT-middelen.
- Verenigingsmiddelen met persoonsgegevens mogen enkel worden meegenomen buiten het verenigingsterrein indien hier goedkeuring van de beheerder van de IT-middelen voor is.

Beveiligingsmaatregelen

Toegang tot IT

- De toegang tot desktopcomputers is beveiligd met een adequaat wachtwoord of ander beveiligingsmechanisme.
- De toegang tot laptops is beveiligd met een adequaat wachtwoord of ander beveiligingsmechanisme.
- De toegang tot andere apparaten (in het bijzonder tablets/telefoons) is beveiligd met een adequaat wachtwoord of ander beveiligingsmechanisme.
- Er is een session time out/automatische schermblokkering ingesteld bij niet-gebruik van de apparaten (3-5 minuten).
- Het beeldscherm wordt bij verlaten van de werkplek geblokkeerd. Sneltoets: “Windowstoets + L” (L van lunch).

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. Ook niet met familie/collega’s.
- 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.
- Inlogactiviteiten worden gelogd.
- Wachtwoorden (in het bijzonder voor externe toegang tot het netwerk) worden gecodeerd verstuurd.
- Het bovenstaande geldt voor alle inlogprocedures.

Twee factoren authenticatie

- Voor de beveiliging van zeer gevoelige data is meervoudige authenticatie gewenst (naast een gebruikersnaam en een wachtwoord moet dan bijvoorbeeld ook een code ingevoerd worden, die je via SMS of via een bijbehorende smartphone-app ontvangt).

Logging

- Er is een log per IT-platform van gebruikersactiviteiten.

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

- Bijzondere en gevoelige persoonsgegevens worden ‘versleuteld’ opgeslagen.
- Bijzondere en gevoelige persoonsgegevens worden waar mogelijk ‘gepseudonimiseerd’ opgeslagen.
- Er is overzicht op welke plaatsen de data fysiek staat opgeslagen.
- De server is adequaat beveiligd.
- Indien de server wordt gedeeld met een andere organisatie dan zijn er heldere afspraken over servergebruik en veilige toegang tot de server.

Verwijdering van persoonsgegevens

Er zijn bewaartermijnen bepaald en er zijn – al dan niet geautomatiseerde - procedures waardoor de persoonsgegevens die de bewaartermijn overschrijden worden verwijderd.

- 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. (bijvoorbeeld met een papierversnipperaar met DIN vernietigingsnorm categorie 3 of 4)

Dataverkeer

- Bij het verkrijgen van persoonsgegevens via het internet wordt gebruik gemaakt van beveiligde protocollen zoals een ssl-certificaat (https). (check ook alle online inschrijfformulieren).
- Lijsten met leden- of deelnemersgegevens worden beveiligd verstuurd. (In Ms Excel en Ms Word kan je eenvoudig een bestand beveiligen met een wachtwoord.)
- Bijzondere of gevoelige persoonsgegevens worden beveiligd en bij voorkeur versleuteld verzonden.
- Bij gebruik van USB sticks worden de persoonsgegevens versleuteld opgeslagen en de toegang is beveiligd met een sterk wachtwoord. (alle onbeveiligde USB sticks worden ingeleverd en vervangen)
- Bij het gebruik van Dropbox, WeTransfer, GoogleDocs, etc dient de gebruiker te controleren of dit gebruik conform de AVG is. Vermijd het versturen van gevoelige of bijzondere persoonsgegevens.

Software

- De laatste versie van het besturingsprogramma is geïnstalleerd op apparaten van de vereniging.
- Gebruikte software is voorzien van de laatste updates.
- Er kan geen software op verenigingscomputers worden opgeslagen zonder toestemming van de IT-beheerder. Op verenigingsmiddelen mag enkel de IT-beheerder software downloaden of installeren. Voor andere gebruikers dient dit technisch onmogelijk te zijn.

Malware/virussen

- Er is een up to date firewall en virusscanner op alle IT-middelen geïnstalleerd.
- Er is een adequate firewall en virusbescherming op het verenigingsnetwerk 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.

- Inkomende e-mails worden automatisch gecontroleerd op virussen, trojans en andere malware.

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. (Dit is enkel haalbaar indien er heldere afspraken zijn over waar data wordt opgeslagen).
- 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 is VPN geïnstalleerd op mobiele apparaten.
- Er worden zo min mogelijk persoonsgegevens opgeslagen op mobiele apparaten.
- Opslag geschiedt bij voorkeur centraal via een virtuele desktoptoegang en niet op het apparaat.
- Mobiele apparaten kunnen op afstand onbruikbaar worden gemaakt of de gegevens kunnen op afstand worden verwijderd.
- De harde schijf, SSD of andere opslag van mobiele apparaten is beveiligd/versleuteld zodat deze bij verlies niet toegankelijk is. (beveiliging van het mobiele apparaat is onvoldoende)
- Indien persoonsgegevens op mobiele apparaten worden opgeslagen wordt er ook een back-up van de harde schijf/SSD gemaakt.
- Er is een effectief beleid hoe medewerkers en vrijwilligers met mobiele apparaten van de vereniging dienen om te gaan.

Telewerken (alle werkzaamheden buiten kantoor)

- Inloggegevens/wachtwoorden worden gecodeerd verstuurd.
- Er wordt geen gebruik gemaakt van openbare wifi, tenzij adequate beveiligingsmaatregelen zijn genomen. (Een alternatief is een eigen mobiele hotspot)
- Er is een beleid voor telewerken.

Printer

- Het is mogelijk om gevoelige gegevens c.q. personeelsgegevens op een beveiligde of apart toegankelijke printer te printen.
- Het is beleid om gevoelige gegevens die zijn geprint van het printergeheugen te verwijderen.

Webapplicaties

- Zorg dat webapplicaties adequaat beveiligd zijn. Richtlijnen zijn onder meer de OWASP top 10 en de uitgave beveiliging webapplicaties van het National Cyber Security Centrum.

- Doorgaans worden webapplicaties van derden gebruik. Zorg dat bij verwerking door deze verwerkers ook adequate beveiligingsmaatregelen worden genomen door de verwerkers. (De afspraken hierover liggen vast in de verwerkersovereenkomst).

Gebruik privéapparatuur

- Er zijn heldere afspraken over gebruik van privéapparatuur en hier wordt voor getekend.
- Het gebruikte apparaat wordt aangemeld.
- Bij gebruik van privéapparatuur is het besturingsprogramma, gebruikte software en antivirussoftware volledig geupdate.
- Er is antivirus software geïnstalleerd
- Er is een firewall geïnstalleerd
- Enkel de noodzakelijke persoonsgegevens worden opgeslagen.
- Deze persoonsgegevens worden zo spoedig mogelijk – duurzaam – verwijderd (prullenbak legen)
- Er worden geen bijzondere of gevoelige persoonsgegevens opgeslagen.
- Opslag geschiedt in een met een wachtwoord beveiligde map.

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.
- Laat alle medewerkers en vrijwilligers een geheimhoudingsverklaring tekenen, zodat men zich bewust is van de risico's en hun rol daarin.

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.