Notitie informatieveiligheid H.E.M.A.-bond Nederland

Achtergrond
De Veiligheidscommissie van de H.E.M.A.-bond Nederland (HBN) heeft met de "Notitie gegevensbescherming HEMA Bond" een belangrijke eerste aanzet gegeven tot het inrichten van informatiebeveiligingsbeleidbinnen de HBN. In deze notitie zijn een aantal basisstandaarden opgenomen waaraan de HBN en geassocieerde clubs zouden moeten voldoen om tot een acceptabel niveau van informatiebeveiliging te komen. De standaarden hebben betrekking op de verantwoordelijkheid van het Bondsbestuur énde aangesloten clubs op de volgende gebieden: wachtwoordbeleid, autorisatiebeleid en gegevensbescherming (specifiek: verantwoorde omgang met email en ledengegevens). Ook wordt gewezen op het belang van een veilige webserver en (administratie)software en een aantal aanvullende maatregelen benoemd die kunnen helpen om de informatiebeveiliging naar een hoger plan te tillen.

Doelstelling
Het Bondsbestuur vindt het belangrijk om nader invulling te geven aan de lijn die de Veiligheidscommissie heeft uitgezet op gebied van informatieveiligheid. De HBN beheert persoons- en privacy gevoelige gegevens en behoort veilig en zorgvuldig om te gaan met informatie en het uitwisselen van informatie. Leden en aangesloten clubs kunnen schade ondervinden wanneer er sprake is van het verlies van gegevens, of het door onbevoegden kennisnemen of manipuleren van informatie. In deze bestuursnotitie informatieveiligheid wil het Bondsbestuur het begrip informatiebeveiliging nader definiëren, een aantal belangrijke uitgangspunten benoemen en strategische doelen stellen voor de komende twee jaar. Aan de hand van de praktische handreiking die de notitie van de Veiligheidscommissie biedt zal het bestuur vervolgens een aantal concrete maatregelen benoemen waarmee zij aan de slag gaat om de gestelde doelen te verwezenlijken.

Voor de clubs die aangesloten zijn is deze notitie bedoeld als advies. Daarbij dient echter te worden opgemerkt dat dit een uitvloeisel is van wet- en regelgeving. De Bond meent dat zij van aangesloten clubs mag verwachten dat zij eenadequate administratie voeren. Informatieveiligheid is daaraan onlosmakelijk verbonden.

Definitie
Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket aan maatregelen om de betrouwbaarheid van de informatievoorziening te waarborgen. Het draait daarbij om beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.

- Beschikbaarheid: Gegevens en functionaliteit dienen voor gebruikers zodanig beschikbaar te zijn dat zij hun taken optimaal kunnen uitvoeren.
- Integriteit: De juistheid van gegevens en functionaliteit dient te voldoen aan de daarvoor gestelde normen, wet- en regelgeving.
- Vertrouwelijkheid:Toegang tot (persoons)gegevens en functionaliteit is beperkt tot degenen die daartoe door de eigenaar hiervan is vastgesteld.

Het informatiebeveiligingsbeleid geldt voor het gehele proces van informatievoorziening binnen de HBN en beperkt zich niet alleen tot de ICT. Het beleid beperkt zich niet alleen tot het bestuur, maar heeft ook betrekking opde geassocieerde clubs en de leden.

Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm et cetera) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekortschietende organisatie.

Uitgangspunten
Ten aanzien van informatiebeveiligingsbeleid hanteert het Bondsbestuur de volgende uitgangspunten:

- Het Bondsbestuur is eindverantwoordelijk voor informatiebeveiliging van de Bond en stelt het informatiebeveiligingsbeleid vast.
- Van aangesloten clubs/verenigingen is het bestuur verantwoordelijk voor informatiebeveiliging van de betreffende club/vereniging.

- Binnen het Bondsbestuur is de secretaris (?) verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid.
- Het Bondsbestuur bevordert en borgt kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de HBN.

De strategische doelen van het informatiebeveiligingsbeleid 2018 – 2020 zijn:
Voor de komende periode (2018-2020) heeft het bestuur de volgende strategische doelen gedefinieerd:

- Het managen van de informatiebeveiliging van de Bond: het bestuur en haar andere organen.
- Het voorkomen van ongeautoriseerde toegang tot informatie van de Bond.
- Het beheersen van de toegang tot informatiesystemen van de Bond.
- Het publiceren van richtlijnen voor de aangesloten clubs/verenigingen op de website van de Bond
- Het adequaat reageren op incidenten.
- Het beschermen en correct verwerken van persoonsgegevens van leden.
- Het minimaliseren van risico's van menselijk gedrag.
- Het opnemen van informatieveiligheid als onderdeel van de audit van clubs.

Uiteindelijk heeft hetinformatiebeveiligingsbeleidals doel de continuïteit van de informatiesystemen te waarborgen en schade en eventuele gevolgen te minimaliseren. Hierin hanteert het Bondsbestuur een pragmatische aanpak.

Maatregelen

1. Het Bondsbestuur zal regels en verantwoordelijkheden voor het beveiligingsbeleid vastleggen en vaststellen. Het Bondsbestuur doet hiervoor een voorstel dat aan de Veiligheidscommissie ter toetsing wordt voorgelegd en ter vaststelling wordt voorgelegd aan de ALV.
2. Het Bondsbestuur zal periodiek aandacht besteden aan bewustwording over informatieveiligheid. Dit realiseert het Bondsbestuur door praktische richtlijnen (bv de notitie bescherming gegevens Hemabond) te publiceren op de website en aan de ALV terugkoppeling te geven op lopende acties.
3. Het Bondsbestuur wordt verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken. Als startpunt wil het Bondsbestuur de richtlijnen voor authenticatie en autorisatie uit de notitie gegevensbescherming van de Veiligheidscommissie implementeren. Daarnaast wil het Bondsbestuur eenprotocol meldplicht datalekken opstellen en een protocol wijzigen wachtwoorden bij bestuurswissels.
4. Het Bondsbestuur ondertekent een integriteitsverklaring inzake de omgang met vertrouwelijke gegevens.
5. Van aangesloten clubs wordt verwacht dat zij kunnen tonen dat zij zich houden aan de geldende wet- en regelgevingaangaande informatieveiligheid. Tijdens een audit kan dit worden bekeken, uiteraard zonder dat ledengegevens of passwords zelf worden gedeeld.

Bijlage: Praktische richtlijnen voor informatiebeveiliging (uit notitie gegevensbescherming HEMA Bond)

Wachtwoordbeleid

- Wachtwoorden moeten langer zijn dan 12 tekens.
- Tip bij aanmaken nieuwe wachtwoorden: gebruik de handleiding uit de notitie gegevensbescherming HEMA Bond.
  Voorstel: bij aanmaken nieuwe wachtwoorden gebruik maken van de tips uit de notitie gegevensbescherming HEMA Bond.
- Wachtwoorden mogen niet digitaal gedeeld worden.
- Van alle wachtwoorden die toegang geven tot persoonsgegevens moet bekend zijn wie ze heeft.
  Voorstel: vastleggen in protocol bestuurswissel dat de penningmeester degene is die de wachtwoorden inzake de ledengegevens heeft en beheert.
  Voorstel: Protocol wijzigen wachtwoorden olv veiligheidscommissie opnemen in stappen/protocol voor bestuurswissel.

Gegevensbescherming

- Gebruik ook voor Excel spreadsheets een wachtwoord.
- Verzamel niet meer gegevens dan je nodig hebt. Gegevens van oud-leden,personen die geen lid meer zijn van een club, mogen nog maximaal tot een maand na het einde van het boekjaar waarin zij hun lidmaatschap hebben opgezegd bewaard worden. Na afloop van het boekjaar moeten de gegevens zo snel mogelijk verwijderd worden.
  Voorstel: draag zorg voor periodiek opschonen oude ledenlijsten.
- Gebruik mailchimpof een soortgelijk programma voor mailings.
- Verstuur zo min mogelijk ledenadministratie exportsper mail. Gebruik zipbestanden met wachtwoordbeveiliging.

Betrouwbarewebserver en up-to-date administratie software

- Sla ledengegevens alleen op een beveiligde server op via up-to-date administratie software en een veilige hosting partij.
- Vergroot de beveiliging zo mogelijk via een certificaat voor https.

Verklaring omgang met vertrouwelijke gegevens

- Stel een verklaring op voor de Bondsbestuursleden en de clubbesturen ten aanzien van de vertrouwelijke omgang met gegevens. Betrokken verklaren hierin de gegevens waartoe zij toegang hebben geheim te houden en naar hun vermogen zullen beveiligen. En na vertrek uit het bestuur alle ledengegevens van hun digitale apparaten te verwijderen. (Emailservers, smartphones en servers).
- Streef ernaar de hoeveelheid gegevens op persoonlijke apparaten te verminderen en zo snel mogelijk overbodig te maken.