Informatiebeveiligingsbeleid Stichting Armoedefonds

1. ***Organisatie van de informatiebeveiliging***

1.1 Taken en Rollen
Het bestuur van Stichting Armoedefonds stelt formeel het IB-beleid op.
De Privacy Officer geeft namens het bestuur op dagelijkse basis invulling aan de sturende rol door besluitvorming in het bestuur voor te bereiden en toe te zien op de uitvoering hiervan.

De coördinatie van informatiebeveiliging is belegd bij de Privacy Officer. De uitvoerende taken zijn zoveel mogelijk belegd bij de relevante personen. De personen rapporteren aan de Privacy Officer. Jaarlijks wordt het functioneren van de IB gerapporteerd.

2. ***Beveiliging van apparatuur en informatie***

2.1 Beheersmaatregelen
In het beginsel mag niemand binnen Stichting Armoedefonds autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd.

Er is een scheiding gemaakt tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.

2.2 Beheer van de dienstverlening door een derde partij
De beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de (bewerkers)overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd.

De diensten, rapporten en registraties, die door de derde partij worden geleverd, worden gecontroleerd en beoordeeld en er worden periodiek audits uitgevoerd.

Wijzigingen in de dienstverlening door derden, in bijvoorbeeld bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, worden beheerd.

In de basis-SLA voor dienstverlening is aandacht besteed aan informatiebeveiliging.

2.3 Behandeling van de media
Er zijn procedures voor het beheer van verwijderbare media en voor het veilig verwijderen of hergebruiken van ICT-apparatuur.

Harde schijven en andere media worden adequaat gewist of vernietigd bij afstoting of hergebruik. In ieder geval indien er vertrouwelijke informatie is opgeslagen en/of licentie plichtige programmatuur op is geïnstalleerd.

Er zijn richtlijnen voor het opbergen van papieren en computermedia. In ieder geval voor gevoelige of kritieke bedrijfsinformatie.

Tevens is er een innamebeleid voor mobiele apparatuur , zoals laptops, pda's, iPads, voor wanneer deze niet meer worden gebruikt.

Er wordt een encryptie op informatie met het classificatielabel vertrouwelijk en zeer geheim gezet.

2.4 Uitwisseling van informatie
Vaststellen formeel beleid, formele procedures en formele beheersmaatregelen om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen. Geformaliseerde situatie rondom het transport van de back-ups en de mogelijkheden van leveranciers om toegang tot het netwerk te verkrijgen.

De uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen wordt in een overeenkomst vastgelegd dit ter bescherming van informatie, die een rol speelt bij elektronische berichtuitwisseling.

Beschermingsmaatregelen voor media die informatie bevatten tegen onbevoegde toegang, misbruik of het corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie. Door middel van een vaste procedure voorwaarden voor gegevensuitwisseling met derden.

3. ***Logische toegangsbeveiliging***

3.1 Authenticatie en autorisatie

Wachtwoorden worden voor een beperkte periode toegekend (3 tot maximaal 6 maanden). Wachtwoorden dienen aan eisen te voldoen, deze worden afgedwongen door het systeem.

De gebruiker is verantwoordelijk voor het geheim blijven van zijn wachtwoord.

Authenticatiemiddelen zoals wachtwoorden worden beschermd tegen inzage en wijziging door onbevoegden tijdens transport en opslag (door middel van encryptie).

Autorisatie is rol gebaseerd. Autorisaties worden toegekend via functie(s) en organisatie onderdelen.

3.2 Externe toegang
Stichting Armoedefonds kan een externe partij toegang verlenen tot het netwerk. Hiervoor dient een procedure gemaakt en gevolgd te worden. Externe partijen kunnen niet op eigen initiatief verbinding maken met het besloten netwerk van Stichting Armoedefonds, tenzij uitdrukkelijk overeengekomen.

De externe partij is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. Stichting Armoedefonds heeft het recht hierop te controleren en doet dat aan de hand van de audit-trail en interne logging.

3.3 Mobiel en thuiswerken
Voor werken op afstand is een thuiswerkomgeving beschikbaar. Toegang tot vertrouwelijke informatie wordt verleend op basis van multifactorauthenticatie. Onbeheerde apparatuur (privé-apparaten of de 'open laptop') kan gebruik maken van draadloze toegangspunten (WiFi). Deze zijn logisch gescheiden van het netwerk van Stichting Armoedefonds.

Mobiele bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen bedrijfsinformatie wordt opgeslagen op het mobiele apparaat (zero footprint'). Bedrijfsinformatie dient te worden versleuteld bij transport en opslag conform classificatie eisen. Voorzieningen als webmail, als ook sociale netwerk en clouddiensten (Dropbox, Gmail, etc.) zijn door het lage beschermingsniveau (veelal alleen naam en wachtwoord, het ontbreken van versleuteling) niet geschikt voor het delen van vertrouwelijke en geheime informatie.

3.4 Overige maatregelen
Het fysieke (bekabelde) netwerk is niet toegankelijk voor onbeheerde apparatuur. Het netwerk van Stichting Armoedefonds is waar mogelijk gesegmenteerd (afdelingen, gebruikers en systemen zijn logisch gescheiden). Tussen segmenten met Verschillende beschermingsniveaus worden access control lists (ACL's) geïmplementeerd.

3.5 Beveiliging van informatiesystemen (software)
Applicaties en Software worden regulier met een minimum van 4 keer per jaar gerepareerd door 'patchen' van software, of 'ad hoc' bij acute dreiging. Welke software wordt geüpdatet wordt mede bepaald door de risico's.

4. ***Beveiligingsincidenten en registratie***

De medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten direct te melden bij de Privacy Officer van Stichting Armoedefonds. Voor afhandeling geldt de reguliere rapportage en escalatielijn. Afhankelijk van de ernst van een incident is er een meldplicht bij het College Bescherming Persoonsgegevens.

5. *Bedrijfscontinuïteit*

Elk afdeling binnen Stichting Armoedefonds heeft voor de belangrijkste processen en systemen continuïteits-/uitwijkplannen welke door middel van een beheerst proces tot stand komen. Continuïteitsplannen worden regelmatig getest en actueel gehouden.

6. *Naleving*

6.1 Organisatorische aspecten
Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van de processen binnen Stichting Armoedefonds, waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elke afdeling stuurt.

Versie: 1.0
Datum: juli 2019