Voor u ligt de algemene beleidsverklaring voor informatiebeveiliging. Dit document is openbaar gesteld door Nobralux voor al haar belanghebbenden. De inhoud hiervan is een zorgvuldige opgestelde samenvatting van het totale managementsysteem voor informatiebeveiliging van Nobralux.

Algemene beleidsverklaring voor informatiebeveiliging

We streven ernaar aantoonbaar te voldoen aan de wensen en eisen van de markt en de eisen vanuit wet- en regelgeving. Om dit aantoonbaar te maken verplichten wij onszelf om te voldoen aan de norm ISO 27001.

Beveiliging van informatie is een onderdeel van de integrale managementverantwoordelijkheid. De directie is verantwoordelijk voor het beleid en de procedures. Vragen en wijzigingen m.b.t. beleid worden vooraf met de directie besproken en enkel door de directie geaccordeerd.

Het informatiebeveiligingsbeleid is passend voor het doel van Nobralux.

Bij het aangaan van samenwerkingsverbanden met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatievoorziening, wordt nadrukkelijk aandacht besteed aan informatiebeveiliging. Afspraken hierover worden schriftelijk vastgelegd en op de naleving hiervan wordt toegezien.

De bedrijfsprocessen, informatiesystemen en gegevensverzamelingen van alle onderdelen van onze organisatie zijn volgens een gestructureerde methode geclassificeerd naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid. Hier wordt overeenkomstig mee omgegaan.

Bij de aanname, tijdens het dienstverband en in geval van ontslag van medewerkers wordt nadrukkelijk aandacht besteed aan de betrouwbaarheid van medewerkers en aan de waarborging van de vertrouwelijkheid van informatie.

Wij voeren een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren. Wij beschikken over gedragsregels voor het gebruik van (algemene) informatievoorzieningen. Deze zijn verwoord in onze gebruikersverklaring voor personeel alsmede het informatiebeveiliging beleid. Op de naleving van deze gedragsregels wordt toegezien.

Bij overtreding van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen kan de directie een sanctie opleggen zoals bijvoorbeeld op non-actiefstelling zetten, disciplinaire straffen, en/of beëindiging van het dienstverband.

Wij hebben maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.

Wij hebben maatregelen getroffen voor de beveiliging en het beheer van de operationele informatie- en communicatievoorzieningen. Maatregelen tegen allerlei vormen van kwaadaardige programmatuur (computervirussen, ransomware, spyware, etc.) vormen hiervan een belangrijk onderdeel.

Wij hebben maatregelen getroffen waardoor is gewaarborgd dat alleen geautoriseerde medewerkers gebruik kunnen maken van de informatie- en communicatievoorzieningen.

Bij de aanschaf van informatiesystemen wordt in alle fasen nadrukkelijk aandacht besteed aan informatiebeveiliging en toegang op basis van taken, rollen en verantwoordelijkheden.

Wij hebben adequate maatregelen getroffen waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) is gewaarborgd, zowel in normale als in buitengewone omstandigheden.

Als onderdeel van het beleidsproces voor informatiebeveiliging wordt door interne en externe partijen toegezien op de naleving van het informatiebeveiliging beleid.

Er is een information security officer aangewezen. Tevens is voor deze rol een back-up aangewezen. In verscheidene beleidsdocumenten wordt gesproken over de security officer. Er mag overal vanuit worden gegaan dat de back-up security officer gelijkwaardig is aan de security officer en bij afwezigheid van de security officer bevoegd is om namens hen te handelen.

Informatiebeveiligingsincidenten worden gemeld bij de security officer. De evaluatie van de afhandeling van deze incidenten wordt benut voor de verbetering van informatiebeveiliging.

Wij hanteren een aantal basisprincipes voor informatiebeveiliging, die als leidraad dienen voor management en medewerkers. Op deze basisprincipes kan worden teruggevallen, wanneer zich vraagstukken voordoen die niet zijn uitgewerkt in het beleid. Onze 7 basisprincipes voor informatiebeveiliging zijn:

1. Informatie van klanten, medewerkers en overige belanghebbenden wordt te allen tijde zorgvuldig behandeld.
2. Informatiebeveiliging is onderdeel van de integrale risicobeheersing en wordt waar mogelijk gecombineerd met andere risicomanagement disciplines om de efficiëntie te verhogen.
3. Bij het treffen van beveiligingsmaatregelen is wet- en regelgeving altijd leidend.

4. Bij externe uitbesteding/samenwerking is het belangrijk dat interne eisen worden vertaald in contractuele overeenkomsten. Uitgangspunt is dat de informatiebeveiliging bij de uitbestede/samenwerkende partij minimaal gelijkwaardig is aan het eigen niveau van informatiebeveiliging.
5. Van alle medewerkers wordt een alerte houding verwacht op het gebied van informatiebeveiliging. Risico's, verdachte situaties en (potentiële) beveiligingsincidenten worden direct gemeld.
6. Iedere medewerker is zelf verantwoordelijk voor het naleven van beveiligingsmaatregelen, waardoor sprake is van individuele aansprakelijkheid. De directie stelt medewerkers in staat die verantwoordelijkheid te nemen.
7. Maatregelen zijn in balans met de te beschermen waarde. Er moeten argumenten zijn om beveiligingsmaatregelen te treffen. Dit betekent dat onderzoek, inclusief risicoanalyse structureel moet plaatsvinden naar de noodzaak van maatregelen.

We verplichten onszelf om continue te verbeteren. Dit borgen we middels onze Plan-Do-Check-Act cyclus van onze processen en tevens in periodieke doelstellingen, een cultuur van bewustzijn en organisatorische inrichting.