LUMEN GROUP privacy & data

Overzicht technische en organisatorische maatregelen (informatiebeveiligingsbeleid)

In verband met het toenemende belang van informatiebeveiliging hebben hieronder een aantal wij specifieke controls opgenomen. Deze zijn uitgesplitst in de belangrijkste en overige controls. Dit overzicht dient als input voor het informatiebeveiligingsbeleid.

Belangrijkste controls	
1.	Is er een wachtwoordenbeleid?
2.	Worden er sterke authenticatie-methoden gehanteerd?
3.	Worden rollen en rechten (autorisaties) per applicatie/programma toegekend op basis van een autorisatiematrix?
4.	Is er een toegangs- en toekenningsprocedure voor autorisaties?
5.	Is de autorisatiematrix nog actueel?
6.	Worden de autorisaties nog correct ingedeeld?
7.	Worden toegangspogingen (incl. uitzonderingen en fouten) in de systemen gelogd?
8.	Wordt toegang gebruikersactiviteiten (zoals inzage) in de diverse dossiers gelogd?
9.	Vindt er (automatische) controle van de logging plaats?
10.	Worden persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?
11.	Is de website versleuteld door middel van *Transport Layer Security* (TLS)?
12.	Worden bijzondere persoonsgegevens via een versleuteld communicatiekanaal gedeeld?
13.	Is er een overzicht van de IT-/ICT-infrastructuur waarin alle applicaties en programma's zijn weergegeven met bijbehorende autorisatieniveaus?
14.	Worden van de diensten, rapporten en registraties van IT-/ICT-leveranciers en -beheerders opgevraagd, geconcludeerd en opgevolgd? (bijv. door middel van PEN-testen en auditverklaringen)

Overige controls	
15.	Worden software- en beveiligingsupdates automatisch- geïnstalleerd op de computers en apparaten?
16.	Is er bescherming tegen malware?
17.	Worden beveiligingsupdates en -patches tijdig geïmplementeerd?
18.	Worden er (tijdig) back-ups gemaakt?
19.	Worden de back-ups ook op een voldoende afgescheiden plek bewaard?
20.	Worden de back-ups regelmatig getest?
21.	Wordt gebruik gemaakt van een Virtual Private Networks (VPN)?
22.	Is het netwerk beveiligd met een firewall?
23.	Zijn systemen uitgerust met een *data leakage detection* mechanisme?
24.	Wordt er gebruik gemaakt van USB-sticks?
25.	Zijn de harde schijven van de computers of andere gegevensdragers versleuteld (bijv. Bitlocker/FireVault)?
26.	Worden er geheimhoudingsverklaringen gesloten met medewerkers en overige natuurlijke personen die onder de verantwoordelijkheid van de organisatie persoonsgegevens verwerken?
27.	Worden de downloadmap en prullenbak op de computer automatisch geleegd?
28.	Worden computers vergrendeld als medewerkers weglopen van hun computer?
29.	Is sprake van een *clean desk policy*?
30.	Worden papieren documenten met persoonsgegevens bewaard in een gesloten kast en ruimtes?