Vragenlijst risicobeoordeling

Ethias
Commerciële dienst Collectiviteiten
Prins-Bisschopssingel 73, 3500 Hasselt
Tel. 011 28 20 15
E-mail: publiekesector@ethias.be

ETHIAS CYBER PROTECTION

Algemene informatie

Naam van de organisatie:

Adres:

Postcode: Gemeente:

Activiteitensector:

Contactpersoon (persoon die deze vragenlijst ondertekent)

Aanspreking:

Naam: Voornaam:

Functie:

Tel.: E-mailadres:

1. Betrokkenheid van het Top Management

- **Heeft u een verantwoordelijke voor de gegevensverwerking en informatiebeveiliging aangesteld?** ◯ Ja ◯ Neen
- **Heeft u uw ICT-risico geïdentificeerd en uw organisatie beschermd voor de toekomst?** ◯ Ja ◯ Neen
- **Voldoet u aan de wettelijke vereisten inzake privacy, gegevensverwerking en veiligheid?** ◯ Ja ◯ Neen
- Bent u zich bewust van de cyberdreigingen en kwetsbaarheden op uw netwerken? ◯ Ja ◯ Neen

2. Uitwerking van een veiligheidsbeleid en een gedragscode

- Beschikt u over een schriftelijk beveiligingsbeleid voor uw IT-systeem en heeft u de gebruikers hiervan op de hoogte gebracht? ◯ Ja ◯ Neen
- **Past u procedures toe voor de intreding en uittreding van gebruikers (personeel, stagiairs, enz.)?** ◯ Ja ◯ Neen
- **Heeft u de rollen en verantwoordelijkheden voor de beveiliging (fysiek, personeel en ICT) beschreven?** ◯ Ja ◯ Neen
- **Heeft u intern een gedragscode voor het gebruik van IT-middelen verspreid?** ◯ Ja ◯ Neen
- Plant u of voert u veiligheidsaudits uit? ◯ Ja ◯ Neen

3. Bewustmaking van het personeel voor Cyberrisico's

- Moedigt u de gebruikers aan om uw gedragscode alsook het wachtwoordbeheer na te leven? ◯ Ja ◯ Neen
- **Herinnert u de gebruikers regelmatig aan het belang van waakzaamheid op het gebied van IT-beveiliging?** ◯ Ja ◯ Neen
- **Herinnert u gebruikers er regelmatig aan dat de informatie als gevoelig moet worden beschouwd en in overeenstemming met de privacyregels moet worden verwerkt?** ◯ Ja ◯ Neen
- **Informeert u gebruikers over hoe ze phishing (e-mailfraude) kunnen herkennen en hoe ze moeten reageren?** ◯ Ja ◯ Neen
- **Heeft u het personeel van de afdeling boekhouding geïnformeerd over het fenomeen «CEO-fraude» en voorziet u in controleprocedures voor de uitvoering van betalingen?** ◯ Ja ◯ Neen

4. Beheer van belangrijke IT-middelen

- Houdt u een inventaris bij van alle ICT-uitrustingen en softwarelicenties? ◯ Ja ◯ Neen
- Houdt u een gedetailleerde en actuele kaart bij van al uw netwerken en interconnecties? ◯ Ja ◯ Neen

5. Update van de programma's

- **Installeert u regelmatig updates (Patches) van de software op uw werkstations, mobiele toestellen, servers en netwerkcomponenten...)?** ◯ Ja ◯ Neen
- Voert u de beveiligingsupdates voor alle software zo snel mogelijk uit? ◯ Ja ◯ Neen
- Heeft u het updateproces geautomatiseerd en controleert u de efficiëntie ervan? ◯ Ja ◯ Neen

6. Installatie van antivirusbescherming

- **Heeft u antivirussoftware op alle werkstations en servers geïnstalleerd?** ◯ Ja ◯ Neen
- **Wordt uw antivirus minstens wekelijks geüpdatet?** ◯ Ja ◯ Neen
- Worden uw antivirusupdates automatisch uitgevoerd? ◯ Ja ◯ Neen
- Weten de gebruikers hoe het antivirus waarschuwt bij een virusinfectie? ◯ Ja ◯ Neen
- **Heeft u een firewall die uw systeem beschermt en die minstens wekelijks wordt geüpdatet?** ◯ Ja ◯ Neen

7. Back-up van alle informatie

- **Voert u wekelijks back-ups uit?** ◯ Ja ◯ Neen
- **Worden de back-ups minstens jaarlijks getest?** ◯ Ja ◯ Neen
- Host u back-upoplossingen op uw eigen servers? ◯ Ja ◯ Neen
- Maakt u gebruik van cloudopslagoplossingen? ◯ Ja ◯ Neen
- Worden de back-ups opgeslagen op een andere site dan het IT-systeem? ◯ Ja ◯ Neen
- Zo ja, worden ze uitbesteed aan een gespecialiseerd bedrijf? ◯ Ja ◯ Neen
- Versleutelt u de gegevens? ◯ Ja ◯ Neen

  Zo ja, welke gegevens?

8. Beheer van de computer- en netwerktoegang

- **Verplicht u het gebruik van persoonlijke en sterke wachtwoorden (met een mix van cijfers, speciale tekens, hoofdletters, enz.) van minstens 6 tekens?** ◯ Ja ◯ Neen
- **Verandert u deze wachtwoorden minstens driemaandelijks en automatisch (of opgelegd door het systeem)?** ◯ Ja ◯ Neen
- **Worden de wachtwoorden gewijzigd bij een vermoeden van hacking?** ◯ Ja ◯ Neen
- **Verandert u standaard alle wachtwoorden?** ◯ Ja ◯ Neen
- Heeft iemand beheerrechten voor de dagelijkse taken? ◯ Ja ◯ Neen
- **Houdt u een beperkte en actuele lijst van systeembeheerders bij?** ◯ Ja ◯ Neen
- **Gebruikt u alleen individuele accounts?** ◯ Ja ◯ Neen
- **Deactiveert u ongebruikte accounts onmiddellijk?** ◯ Ja ◯ Neen
- Worden de rechten en voorrechten beheerd door gebruikersgroepen? ◯ Ja ◯ Neen
- Worden de toegangsrechten van het personeel bepaald op basis van het verantwoordelijkheidsniveau van de gebruiker? ◯ Ja ◯ Neen
- Past u een specifiek beleid inzake toegang tot het IT-systeem toe voor onderaannemers of leveranciers? ◯ Ja ◯ Neen

9. Beveiliging van werkstations en mobiele apparaten

- **Worden ongebruikte werkstations en mobiele apparaten automatisch vergrendeld?** ◯ Ja ◯ Neen
- Worden laptops, tablets en smartphones soms onbeheerd achtergelaten? ◯ Ja ◯ Neen
- **Deactiveert u de Autorun-functie voor externe media?** ◯ Ja ◯ Neen
- Bewaart of kopieert u alle gegevens op een server of een NAS (Network Area Storage)? ◯ Ja ◯ Neen
- Staat u het gebruik van privétoestellen toe (PC, GSM...)? ◯ Ja ◯ Neen

10. Beveiliging van servers en netwerkcomponenten

- **Zijn de lokalen van de onderneming beveiligd om de toegang tot de server(s) te verhinderen?** ◯ Ja ◯ Neen
- **Is het openbare WiFi-netwerk gescheiden van het bedrijfsnetwerk?** ◯ Ja ◯ Neen
- Beschermt u de WiFi met een WPA2-encryptie? ◯ Ja ◯ Neen
- Sluit u ongebruikte poorten en diensten? ◯ Ja ◯ Neen
- **Vermijdt u een verbinding op afstand met de servers (RPC-protocol)?** ◯ Ja ◯ Neen
- Gebruikt u beveiligde toepassingen en protocollen? ◯ Ja ◯ Neen
- Worden de beveiligingslogs op de servers en firewalls minstens 1 maand bewaard? ◯ Ja ◯ Neen

11. Beveiliging van toegangen op afstand

- Wordt de toegang op afstand automatisch gesloten als er gedurende een bepaalde periode geen activiteit is? ◯ Ja ◯ Neen
- **Beperkt u de toegang op afstand tot wat strikt noodzakelijk is?** ◯ Ja ◯ Neen
- Zijn alle verbindingen met het bedrijfsnetwerk beveiligd en versleuteld? ◯ Ja ◯ Neen
- **Beveiligt u de internetverbindingen met het IT-systeem (laptops, mobiele telefoons, tablets...) met behulp van de VPN-tool?** ◯ Ja ◯ Neen

12. Terbeschikkingstelling van een bedrijfscontinuïteitsplan & incidentmanagementplan

- **Heeft u een incidentmanagementplan om te reageren op een incident?** ◯ Ja ◯ Neen
- Verspreidt en actualiseert u de informatie over het aanspreekpunt (interne en externe contacten, technische directie en contacten...)? ◯ Ja ◯ Neen
- **Meldt u alle incidenten aan het management?** ◯ Ja ◯ Neen
- Heeft u een continuïteitsplan opgesteld, getest en geüpdatet in het geval van een cyberaanval? ◯ Ja ◯ Neen
- Heeft u reeds een gebeurtenis gemeld die onder het toepassingsgebied van de GDPR valt? ◯ Ja ◯ Neen
- Bent u reeds het slachtoffer geweest van een cyberaanval? ◯ Ja ◯ Neen

  Zo ja, van welke aard?

- Vanaf welke onderbrekingsduur van uw informatiesysteem is er een aanzienlijke impact op uw activiteiten?

  ◯ Minder dan 12 uur ◯ Tussen 12 en 24 uur ◯ Tussen 1 en 2 dagen

  ◯ Tussen 2 en 5 dagen ◯ Meer dan 5 dagen

13. Type van gebruikte gegevens

- Gebruikt u persoonsgegevens van particulieren (andere dan die van uw werknemers of agenten)? ◯ Ja ◯ Neen
- Is het mogelijk om online te betalen op de website van de ondernemingen? ◯ Ja ◯ Neen

Opgemaakt te op

Naam en voornaam van de contactpersoon