Digital Security
Progress. Protected.

ESET FOR GOVERNMENT

Digital security voor de overheid op elk niveau

DIT ZIJN DE BELANGRIJKSTE WETGEVINGEN VOOR OVERHEIDSINSTELLINGEN:

AVG

Algemene verordening gegevensbescherming (AVG):

Dit is een Europese privacywetgeving die sinds mei 2018 van kracht is en geldt voor alle organisaties die persoonsgegevens verwerken. Overheidsinstellingen zijn hier dus ook aan gebonden.

WBNI

Wet beveiliging netwerk- en informatiesystemen (Wbni):

Dit is een Nederlandse wetgeving die gericht is op de beveiliging van netwerk- en informatiesystemen van organisaties die actief zijn in vitale sectoren, waaronder de overheid.

DIT IS HET BELANGRIJKSTE NORMENKADER VOOR OVERHEIDSINSTELLINGEN:

BIO

Baseline Informatiebeveiliging Overheid (BIO):

Dit is een normenkader voor informatiebeveiliging dat specifiek is ontwikkeld voor overheidsinstellingen. De BIO richt zich op de bescherming van vertrouwelijke informatie en persoonsgegevens.

AVG

Om te voldoen aan de Algemene Verordening Gegevensbescherming (AVG) kan een overheidsinstelling de volgende stappen nemen:

1. **Bewustwording:** zorg dat alle medewerkers op de hoogte zijn van de AVG en de gevolgen daarvan voor de organisatie.
2. **Data-inventarisatie:** breng in kaart welke persoonsgegevens de organisatie verwerkt, waar deze gegevens vandaan komen en met wie deze worden gedeeld.
3. **Risicoanalyse:** voer een risicoanalyse uit om de risico's voor de verwerking van persoonsgegevens te identificeren en te evalueren.
4. **Beleid en procedures:** stel een privacybeleid en bijbehorende procedures op die in lijn zijn met de AVG, zodat duidelijk is hoe de organisatie persoonsgegevens verwerkt en beschermt.
5. **Technische en organisatorische maatregelen:** implementeer de nodige technische en organisatorische maatregelen om persoonsgegevens te beschermen, zoals versleuteling, toegangscontrole en bewustwordingstrainingen voor medewerkers.
6. **Data protection impact assessment (DPIA):** voer een DPIA uit bij verwerkingen waarbij een hoog risico voor de rechten en vrijheden van betrokkenen bestaat.
7. **Incident management:** zorg voor een plan om datalekken en andere privacy-incidenten te managen en te melden aan de betrokkenen en de Autoriteit Persoonsgegevens.
8. **Documentatie:** documenteer alle stappen die worden genomen om aan de AVG te voldoen, zodat kan worden aangetoond dat de organisatie zich aan de wetgeving houdt.

Het is aan te bevelen om een functionaris gegevensbescherming (FG) aan te stellen, die verantwoordelijk is voor de privacybescherming binnen de organisatie en fungeert als contactpersoon voor de Autoriteit Persoonsgegevens en betrokkenen. Daarnaast kan het nuttig zijn om externe expertise in te huren om de organisatie te helpen bij het implementeren van de nodige maatregelen en bij het naleven van de AVG.

WBNI

Om te voldoen aan de Wet beveiliging netwerk- en informatiesystemen (Wbni) kan een overheidsinstelling de volgende stappen nemen:

1. **Identificeer de systemen:** identificeer de netwerk- en informatiesystemen die van belang zijn voor de continuïteit van de dienstverlening en/of de nationale veiligheid.
2. **Classificeer de systemen:** classificeer de netwerk- en informatiesystemen aan de hand van de eisen die de Wbni stelt, in de categorieën basis, normaal en hoog.
3. **Beveiligingsmaatregelen:** implementeer de nodige beveiligingsmaatregelen om de netwerk- en informatiesystemen te beschermen. De maatregelen moeten passen bij de classificatie van de systemen en kunnen onder meer bestaan uit toegangscontrole, versleuteling, detectie van kwetsbaarheden en beveiliging tegen malware.
4. **Incident management:** zorg voor een plan om cybersecurity-incidenten te managen en te melden aan het Nationaal Cyber Security Centrum (NCSC). Dit plan moet passen bij de classificatie van de systemen.
5. **Certificering:** het is mogelijk om als overheidsinstelling gecertificeerd te worden volgens de Wbni. Hiervoor moet de organisatie een assessment uitvoeren waarbij een onafhankelijke derde partij beoordeelt of de organisatie voldoet aan de eisen van de Wbni.
6. **Monitoring en evaluatie:** voer regelmatig controles uit om te zorgen dat de genomen maatregelen effectief zijn en blijven, en om nieuwe risico's te identificeren en aan te pakken.

Het is aan te bevelen om een informatiebeveiligingsfunctionaris aan te stellen die verantwoordelijk is voor de implementatie en evaluatie van de beveiligingsmaatregelen en de incidentenafhandeling. Ook kan het nuttig zijn om externe expertise in te huren om de organisatie te helpen bij het implementeren van de nodige maatregelen en bij het naleven van de Wbni.

BIO

Om te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO) kan een overheidsinstelling de volgende stappen nemen:

1. **Bewustwording:** zorg dat alle medewerkers op de hoogte zijn van de BIO en de gevolgen daarvan voor de organisatie.
2. **Informatiebeveiligingsbeleid:** stel een informatiebeveiligingsbeleid op dat in lijn is met de BIO en waarin duidelijk wordt aangegeven hoe de organisatie omgaat met informatiebeveiliging.
3. **Risicoanalyse:** voer een risicoanalyse uit om de risico's voor de verwerking van informatie te identificeren en te evalueren.
4. **Beveiligingsmaatregelen:** implementeer de nodige beveiligingsmaatregelen om de informatie te beschermen, zoals toegangscontrole, versleuteling, detectie van kwetsbaarheden en beveiliging tegen malware. De BIO geeft hiervoor een aantal maatregelen die specifiek zijn afgestemd op de overheidscontext.
5. **Continuïteitsplan:** stel een plan op voor het geval van een calamiteit, zodat de informatievoorziening van de organisatie gewaarborgd blijft.
6. **Incident management:** zorg voor een plan om informatiebeveiligingsincidenten te managen en te melden.
7. **Documentatie:** documenteer alle stappen die worden genomen om aan de BIO te voldoen, zodat kan worden aangetoond dat de organisatie zich aan de wetgeving houdt.

Het is aan te bevelen om een informatiebeveiligingsfunctionaris aan te stellen die verantwoordelijk is voor de implementatie en evaluatie van de beveiligingsmaatregelen en de incidentenafhandeling. Ook kan het nuttig zijn om externe expertise in te huren om de organisatie te helpen bij het implementeren van de nodige maatregelen en bij het naleven van de BIO.
Het is aan te raden om regelmatig te evalueren of het beleid en de procedures nog adequaat zijn en om eventuele knelpunten op te lossen.