

Programma van Eisen – Leerprogramma Privacy & Informatiebeveiliging

Gemeente Velsen

Voor de gemeente Velsen is het belangrijk dat medewerkers zich bewust zijn van risico's en verantwoordelijkheden op het gebied van informatiebeveiliging en privacy. Daarom wordt een eigentijds en aansprekend leerplatform ingezet dat medewerkers actief betreft, prikkelt en ondersteunt. In dit document beschrijven we onze functionele eisen voor zo'n platform.

1. Inhoudelijke basis: actuele en relevante content

Het platform moet medewerkers informeren over de belangrijkste thema's binnen de AVG en informatiebeveiliging. Denk hierbij aan de omgang met persoonsgegevens, de noodzaak van sterke wachtwoorden, het herkennen van phishing en het voorkomen van datalekken. De content moet aansluiten bij de wettelijke kaders en verplichte normenkaders zoals de AVG en de BIO/ISO27001 maar vertaald zijn naar begrijpelijke en herkenbare situaties voor gemeentelijke medewerkers.

De inhoud moet daarnaast praktisch zijn, met voorbeelden die passen bij het werk in een gemeentelijke context, zodat medewerkers het geleerde direct kunnen toepassen.

2. Contentaanbod en flexibiliteit

In het trainingsprogramma moeten, in ieder geval, de volgende onderwerpen aan bod komen:

- Herkennen van phishing, CEO-fraude en andere vormen van malafide e-mail.
- Wachtwoorden, inclusief het gebruik van wachtwoordmanagers,
- Gebruik van mobiele apparatuur,
- Gebruik van e-mail,
- Werken op afstand,
- Gebruik van social media,
- Fysieke toegangsbeveiliging,
- Werken tijdens reizen,
- Zoeken op internet, gebruik van websites, downloaden van bestanden,
- Wifi en wifi-hotspots,
- Malware en ransomware
- Datalekken en informatiebeveiligingsincidenten,
- Social engineering
- Vragen en/of opdrachten over basisprincipes en onderwerpen uit de AVG: rechtmatigheid, behoorlijkheid, transparantie, doelbinding, dataminimalisatie, juistheid, opslagbeperking, vertrouwelijkheid, rechten van betrokkenen, privacy by design, verwerkers(overeenkomsten) etc.
- Contentaanbod moet aansluiten bij actualiteiten en nieuwe ontwikkelingen

De content moet interactief zijn en opdrachten, vragen en/of toetsen bevatten inclusief feedback op het gegeven antwoord en/of behaalde resultaat.

De look & feel van de trainingen moet aangepast kunnen worden aan de huisstijl van de gemeente, zodat het platform vertrouwd en herkenbaar aanvoelt voor medewerkers. Het platform biedt de mogelijkheid om periodiek een volwassenheidsmeting (nul- en vervolgmeting) uit te voeren. Daarnaast bevat de managementrapportage concrete aanbevelingen per afdeling of doelgroep, gericht op bijsturing en verbetering.

3. Ondersteuning managers en teamleiders

De leverancier biedt ondersteunende middelen voor management en teamleiders, zodat zij het belang van informatiebeveiliging en privacy actief kunnen uitdragen. Denk hierbij aan vergadertemplates, korte presentaties of begeleidende gesprekskaarten.

4. Taal en toegankelijkheid

De content moet standaard Nederlandstalig zijn en op verzoek beschikbaar zijn in ten minste Engels. Het platform moet het eenvoudig mogelijk maken om aanvullende talen toe te voegen. Dit komt tegemoet aan de diversiteit binnen het medewerkersbestand.

De trainingsomgeving moet intuïtief en laagdrempelig zijn, zodat medewerkers zonder technische kennis ermee uit de voeten kunnen.

5. Doelgroepdifferentiatie

Het platform maakt het mogelijk om content, rapportages en communicatie af te stemmen op verschillende doelgroepen binnen de organisatie, waaronder:

- reguliere medewerkers;
- leidinggevendenden;
- high-risk profielen (zoals gegevensverwerkers of functioneel beheerders);
- security-ambassadeurs of -contactpersonen.

6. Functionaliteit

Leermodule moeten gefaseerd aangeboden kunnen worden en te kunnen worden aangemerkt als verplicht te volgen. Daarnaast moet de volgende functionaliteit aanwezig zijn:

- Aanbieden van (korte) e-learningen,
- Uitvoeren van phishing-tests,
- Aanpasbaarheid landingspagina's phishing-tests,
- Mogelijkheid tot het uitvoeren van een nulmeting met vastlegging van resultaten (toetsen volwassenheidsniveau / cultuur),
- Opdrachten, vragen en/of toetsen bij de content (bv. E-learning) incl. feedback op het gegeven antwoord,

- Mogelijkheid om een enquête te sturen om de effectiviteit te meten/evaluatie uit te voeren van de aangeboden content (bv. e-learning).
- Mogelijkheid om deadlines in te stellen,
- Rapportagemodule over voortgang, resultaten en trends, ten behoeve van monitoring die naar behoefte samengestelde rapportages kan opleveren.
- Mogelijkheid om het platform in te richten op basis van de organisatiestructuur (zoals afdelingen, teams en functies).
- Gebruikers moeten tussentijds de opdrachten kunnen pauzeren en op een later moment weer verder kunnen gaan
- Beheerders moeten kunnen instellen hoe vaak er een reminder moet worden gestuurd

7. Vorm en betrokkenheid: gamification, competitie en scenario's

Om medewerkers actief te betrekken en het leerproces aantrekkelijk te maken, moet platform gebruik maken van gamification-elementen zoals quizzes, badges of spelelementen.. Denk hierbij aan spelelementen zoals quizzes, badges of het 'bouwen' aan een virtuele gemeente naarmate men trainingen voltooid.

Het platform faciliteert een vriendelijke competitie binnen de organisatie, bijvoorbeeld tussen teams, afdelingen of domeinen. Zo stimuleren we deelname en bewustwording op een positieve, motiverende manier. De leverancier past een onderbouwde leer- en gedragsstrategie toe, gebaseerd op principes zoals nudging, herhaling, beloning of gedragspsychologie. Deze strategie is gericht op duurzame gedragsverandering en actieve participatie van medewerkers.

Het trainingsprogramma bevat scenario-oefeningen waarmee medewerkers actief kunnen oefenen met het herkennen van en reageren op incidenten op het gebied van privacy en informatiebeveiliging. Het doel hiervan is dat het melden van incidenten consequent en tijdig wordt gedaan en dat lessen uit incidenten worden getrokken.

8. Doorlopende bewustwording

We geloven niet in een eenmalige 'verplichte training'. Het platform ondersteunt structureel doorlopende bewustwording via regelmatige korte modules, maandelijkse quizzes of reminders. Deze doorlopende prikkels kunnen gekoppeld worden aan landelijke campagnes zoals de Week van de Privacy of de Dag van de Informatiebeveiliging. Minimaal jaarlijks verschijnen er updates van het trainingsmateriaal zodat er een actueel aanbod is, conform trends en ontwikkelingen.

9. Technisch/architectuur

De oplossing moet kunnen koppelen en synchroniseren met de Active Directory van de gemeente Velsen (Microsoft Entra-ID) zodat de actieve gebruikers van het platform altijd in dienst zijn bij de gemeente Velsen en Single Sign On-toegang mogelijk is.

Leverancier biedt de gevraagde oplossing aan als SaaS en draagt zelf zorg voor hosting van de applicatie.

Het platform biedt de mogelijkheid om toegang te bieden in verschillende rollen, zoals cursist, manager, beheerder.

Het platform biedt de mogelijkheid voor export van resultaten en rapportages naar de Microsoft Office omgeving (Excel, Word).

De website is volledig functioneel in alle veelvoorkomende internetbrowsers. Minimaal in Microsoft Edge, Google Chrome, Mozilla Firefox en Apple Safari.

Het moet mogelijk zijn om het platform te koppelen aan het gemeentelijke leer- of HRM-systeem via gangbare standaarden. Gemeente Velsen maakt gebruik van het leerplatform van BCS HR Software. Hierdoor kan deelname en voortgang ook worden geregistreerd binnen het gemeentelijke systeem.

10. Handleiding en training

Om effectief gebruik te kunnen maken van het platform stelt de leverancier handleidingen digitaal ter beschikking aan de beheerders bij de gemeente Velsen. Daarnaast biedt de leverancier een opleiding om de noodzakelijke beheertaken in het platform te kunnen uitvoeren.

11. Leverancier

De leverancier ondersteunt bij de inrichting, communicatie, voortgangsbewaking en rapportage van het programma. Er is sprake van een proactieve rol richting de opdrachtgever, met periodieke evaluatie- en afstemmingsmomenten.

De organisatie van de leverancier en zijn dienstverlening dienen in opzet, bestaan en werking te voldoen aan de meest actuele versie van de NEN-EN-ISO/IEC 27001 en toont dat aan d.m.v. een afschrift van het certificaat en de bijbehorende verklaring van toepasselijkheid.

Na opdrachtverstrekking ondertekent de leverancier de, door de opdrachtgever opgestelde, verwerkersovereenkomst/gegevensdelingsovereenkomst voordat er tot de daadwerkelijke verwerking van persoonsgegevens wordt overgegaan. De verwerkersovereenkomst/gegevensdelingsovereenkomst is gebaseerd op het VNG-model. In samenspraak tussen opdrachtgever en opdrachtnemer kunnen wijzigingen worden aangebracht die specifiek voor de opdracht van kracht zijn.