Hoogheemraadschap van Delfland

Standaard beveiligingseisen Delfland voor leveranciers

1. Veilig & betrouwbaar personeel

1.1 Leverancier ondertekent een geheimhoudingsverklaring en/of is contractueel gebonden aan een geheimhoudingsbepaling. (Voor alle leveranciers met toegang tot Delfland data).

1.2 Alvorens medewerkers toegang krijgen tot vertrouwelijke informatie worden zij met goed resultaat gescreend door de leverancier o.b.v. het screeningsbeleid van de leverancier, bijvoorbeeld via een VOG.

1.3 Leverancier voert een bewustwordingsprogramma uit zodat personeel beveiligingsrisico's herkent en daarop acteert. Hierin wordt ook aandacht besteed aan Social Engineering.

2. Beheer van bedrijfsmiddelen

2.1 Informatiesystemen en schijven van desktops en laptops waarop Delfland informatie is of was opgeslagen dienen op zorgvuldige wijze te worden geschoond van rest data volgens een erkende standaard/best practice voor datavernietiging (Secure Erase) en er dient daarna geverifieerd te worden of de overschrijving is gelukt.

2.2 Schijven van servers dienen na uitgebruikname of defect te worden vernietigd.

3. Logische Toegangsbeveiliging

3.1 Delfland heeft een Single sign on beleid waardoor met netwerkaccounts toegang moet worden verkregen tot de Informatiesystemen.

3.2 Het informatiesysteem maakt een koppeling met Entra ID van Delfland (voorheen Azure AD) voor het realiseren van Single sign on en Multi factor authenticatie (MFA).

3.3 Alle lokale accounts waarmee toegang tot SaaS informatiesystemen van Delfland wordt verkregen dwingen Multi factor authenticatie (MFA) af. Indien er geen SSO koppeling gemaakt kan worden met Entra ID van Delfland, wordt MFA afgedwongen.

3.4 Alle gebruikers zijn persoonlijk identificeerbaar via hun eigen account.

3.5 De Delfland Single sign on oplossing voldoet aan het wachtwoordbeleid van Delfland.

3.6 Indien deze oplossing niet wordt gebruikt dienen onderstaande eisen ingevuld te worden m.b.t. wachtwoorden/accounts:

3.6.1 Wachtwoord bestaat uit minimaal 20 karakters.

3.6.2 Het wachtwoord moet minimaal bestaan uit een combinatie van cijfers, hoofd-en kleine letters en speciale tekens.

3.6.3 Voor een account met MFA wordt het wachtwoord jaarlijks gewijzigd.

3.6.4 Voor een account zonder MFA wordt het wachtwoord minimaal elke 3 maanden gewijzigd.

3.6.5 Het nieuwe wachtwoord mag niet hetzelfde zijn als alle voorgaande wachtwoorden.

3.6.6 Het standaard/default account en wachtwoord wordt altijd meteen veranderd.

3.6.7 Wanneer een gebruiker vijf achtereenvolgende keren een fout wachtwoord of een foute combinatie van gebruikersnaam en wachtwoord invoert wordt het account geblokkeerd voor een tijdsduur van minimaal 1 minuut en bij voorkeur via een oplopende lockout policy.

3.7 Voor leveranciers van Procesautomatisering gelden aanvullende eisen voor leverancierstoegang, deze zijn uitgewerkt in een apart document.

3.8 Wachtwoorden moeten via een veilige versleutelde verbinding worden verstuurd

3.9 Sessieduur dient te verlopen binnen 15 minuten.

3.10 Role-based access moet worden toegepast op basis van need to know en least privilege.
3.11 Bij belangrijke transacties zoals handelingen van beheerders en grote betalingen is het 4 ogen principe toegepast.
3.12 De toewijzing en het gebruik van privileges van administrators en systeembeheerders dient beperkt te blijven tot het strikt noodzakelijke systeembeheer.

4. Fysieke toegangsbeveiliging

4.1 Leverancier draagt zorg voor zorgvuldige beheersing van fysieke toegang tot eigen objecten en gebouwen zodat geen onbevoegde toegang kan worden verkregen tot Informatiesystemen waarop Delfland informatie is opgeslagen.

5. ICT aansluitvoorwaarden

5.1 De ICT aansluitvoorwaarden zijn van toepassing in geval van on-premise applicaties.

6. Cryptografie

6.1 Er dient versleuteling voor authenticatie datatransport en opslag te worden toegepast.
6.2 Er mogen enkel cryptografische technieken worden gebruikt die algemeen als veilig zijn beschouwd. Delfland hanteert hierbij de adviezen van het NCSC-NL als standaard.
6.3 Webapplicaties moeten worden voorzien van Certificaten met tenminste SHA256 en een geldigheid van maximaal 1 jaar.
6.4 Er dient gebruik gemaakt te worden van HTTPS voor verzending van gevoelige gegevens.
6.5 Er dient gebruik gemaakt te worden van beveiligde verbindingen zoals VPN
6.6 Certificaten dienen als veilig te worden beschouwd door de bekende browsers (Edge, Firefox, Chrome, Safari) en er dient een proces te zijn om certificaten tijdig te vervangen.
6.7 Voor gevoelige gegevens worden PKI-overheid certificaten gebruikt, bij andere versleutelingsvormen zijn de eisen van ISO 11770 van toepassing.

7. Beveiliging bedrijfsvoering

7.1 De leverancier neemt in alle redelijkheid maatregelen om de beschikbaarheid van data te garanderen.
7.2 Een back-up van gegevens is beschikbaar, versleuteld, niet muteerbaar en wordt beschermd opgeslagen op een andere locatie. Voor on-premise informatiesystemen moet een kopie van de back-up offline worden bewaard.
7.3 Back-up frequentie voldoet aan de eis van Delfland, voortkomend uit een Business impact assessment. Minimaal wordt wekelijks een full back-up gemaakt en dagelijks een gedeeltelijke back-up (differentiële- of incrementele back-up).
7.4 Er wordt voorafgaand getest bij een restoreverzoek en minimaal jaarlijks worden restore procedures door de leverancier getest.
7.5 Gegevens in rust of in bewerking (incl. back-ups) dienen altijd binnen EU grenzen te blijven.
7.6 De leverancier brengt alle relevante informatiebeveiligingsrisico's in kaart, mitigeert deze risico’s en monitort de risico’s.
7.7 Er worden capaciteitscontroles uitgevoerd waarmee aangetoond kan worden dat de applicatie bepaalde toestroom/gebruik aan kan.

7.8 Ongeautoriseerde pogingen tot wijzigingen in software en opgeslagen gegevens dienen te worden gedetecteerd, gerapporteerd en voorkomen.

7.9 Er vindt monitoring op de omgeving plaats en afwijkende activiteiten worden geregistreerd in een Security Information and Event Management (SIEM).

7.10 Logging van alle toegang (inclusief verwijderen en aanpassen) van de data en van het informatiesysteem dient beschikbaar te zijn in een bij Delfland bekende locatie of aangeleverd te kunnen worden (na goedkeuring) voor een periode van minimaal 3 maanden.

7.11 Het Security Operations Center van Delfland monitort de logging van applicaties, indien dit niet het geval is, wordt logging op verzoek aangeleverd.

Logfiles dienen minimaal te bevatten:

- De gebeurtenis;
- De benodigde informatie om een incident met een hoge mate van zekerheid te herleiden tot een natuurlijk persoon, gebruikersnaam of ID
- De unieke id van het betrokken apparaat, component waarop de handeling werd uitgevoerd;
- Host naam
- Operating System (OS)
- Naam van de toepassing
- IP-adres(sen)
- Locatie(s)
- Het object waarop de handeling werd uitgevoerd
- Module die of softwarepakket dat de gebeurtenis veroorzaakt
- Waarop de handeling van de gebruiker betrekking heeft (bijv. klantnummer, veldnaam)
- Het resultaat van de handeling (bijvoorbeeld: geslaagd/niet-geslaagd, en ook het effect en de omvang, bijv. raakt het persoonsgegevens) ;
- De datum en het tijdstip van de gebeurtenis
- Een doorlopende en unieke nummering per logregel

7.12 Activiteiten van systeembeheerders en -operators worden vastgelegd en de logbestanden worden beschermd en regelmatig beoordeeld.

7.13 Alle producten en informatiesystemen die worden ingezet bij het uitvoeren van de overeenkomst worden onderhouden volgens de geadviseerde onderhoudsspecificaties.

7.14 Gebruikte Informatiesystemen en hardware en worden actief ondersteund en bijgehouden.

7.15 Leverancier informeert Delfland proactief over versie upgrades of updates of end of live applicaties.

7.16 Indien de leverancier in de keten geen specificaties heeft meegegeven voor in dienstverlening toegepaste hardware of software dienen internationale best practices te worden ingezet.

7.17 Er dient een procedure opgesteld, afgestemd en geïmplementeerd te zijn en/of SLA met Delfland waarin:

- ontdekte kwetsbaarheden direct aan Delfland worden gemeld aan de ICT servicedesk en accounthouder bij Delfland.
- overleg plaatsvindt over mogelijkheden voor tussentijdse mitigerende maatregelen .
- de risico's verbonden met de installatie van de patch worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).
- patches voor installatie getest worden door de leverancier.

- patching in geval van ernstige kwetsbaarheden (waarbij Delfland de NCSC.NL classificatie en adviezen van NCSC en CERT-WM volgt) binnen een week plaatsvindt.
- in alle andere gevallen dient patching plaats te vinden binnen de reguliere termijn uit de overeenkomst en bij ontbreken daarvan bij de eerstvolgende onderhoudsronde van de informatiesystemen.

8. Netwerkbeveiliging

8.1 Netwerken moeten adequaat beheerd en gecontroleerd worden om te worden beschermd tegen bedreigingen, en om de beveiliging te handhaven voor de systemen en toepassingen die gebruik maken van het netwerk, inclusief informatie in transit.

8.2 Netwerken zijn beveiligd door authenticatie, cryptografie van netwerkverbinding, white listing en hardening.

8.3 Netwerksegmentatie is doorgevoerd binnen de afgenomen omgeving en de eigen leveranciersomgeving.

8.4 Delfland gebruikt geen gesharede resources met andere klanten en vereist bijvoorbeeld een eigen tenant.

9. Acquisitie, ontwikkeling en onderhoud van Informatiesysteem

9.1 Er worden richtlijnen en voorschriften toegepast voor standaarden, best practices en veilig coderen, die tot doel hebben kwetsbaarheden te vermijden.

9.2 Voor de top 10 kwetsbaarheden voor webapplicaties dienen aantoonbaar maatregelen te zijn genomen op basis van de meest recente OWASP top 10.

9.3 Er dienen aantoonbaar formele procedures te worden gehanteerd waarmee wijzingen aan het informatiesysteem worden doorgevoerd en beheerst.

9.4 Wijzigingen worden altijd getest voordat zij in productie gebracht worden.

9.5 Er wordt op een van de productieomgeving gescheiden (acceptatie)test- en ontwikkelomgeving (OTAP) ontwikkeld en getest.

9.6 De Ontwikkel, Test- en Acceptatietest omgeving zijn adequaat beveiligd volgens de laatste stand van de technologie.

9.7 Voor het testen van het informatiesysteem met persoonsgegevens en voor trainingen voor het informatiesysteem worden uitsluitend geanonimiseerde gegevens gebruikt.

10. Leveranciersrelaties

10.1 Leverancier moet kunnen aantonen dat zij beschikken over één van de volgendeThird Party Memorandum/Mededeling (TPM): ISO 27001, ISO27017/18, ISAE3000, SOC2, ISAE3402 met relevant normenkader of vergelijkbaar.

10.2 Leverancier draagt zorg voor zorgvuldige beheersing van zijn toeleveringsketen en onderaannemers.

- De leverancier heeft een totaaloverzicht van alle onderleveranciers en borgt dat de onderleveranciers periodiek beoordeeld worden.

10.3 De leverancier levert rapportages aan ter verantwoording van de geleverde dienstverlening conform de afgesproken servicelevels en beschikbaarheid/prestatie-indicatoren.

10.4 Delfland moet de mogelijkheid krijgen om een audit, (pen)test en code review te doen of uit te laten voeren op alle vereisten zoals vermeld in de overeenkomst

10.5 Bevindingen vanuit audits en door de leverancier uitgevoerde pentesten waaruit blijkt dat in de overeenkomst opgenomen eisen voor informatiebeveiliging &

privacy niet worden nageleefd, dienen onmiddellijk of binnen een met Delfland afgestemde termijn te worden verholpen.

10.6 Indien het de leverancier wordt toegestaan om aan derden informatie van Delfland door te geven dan dient de leverancier alle vereisten op gebied van informatiebeveiliging & privacy zoals opgenomen in de overeenkomst vast te leggen in contractueel overeengekomen afspraken met deze derde partij(en). De eerste leverancier blijft verantwoordelijk en aansprakelijk voor de juiste naleving van de uitvoering van de contractuele afspraken.

10.7 De leverancier dient de afgesproken contactpersoon bij Delfland proactief te informeren over wijzigingen in de organisatie die de dienstverlening gaan raken of ontdekte risico's die de dienstverlening kunnen beïnvloeden.

10.8 De overeenkomst bevat een exit-strategie voor een gecontroleerde en beheerste beëindiging van de dienstverlening. Hierbij wordt overeengekomen dat data wordt teruggegeven in bruikbare versie of vernietigd wordt.

11. Beheer van informatiebeveiligingsincidenten

11.1 Ieder informatiebeveiligingsincident, data lek of vermoedelijk incident gerelateerd aan de vertrouwelijkheid, integriteit of beschikbaarheid van Delfland data/dienstverlening zal direct en zonder onnodige vertraging en altijd binnen 24 uur gemeld worden aan de ICT servicedesk via tel. 015-2608008 (tijdens kantooruren) en de accounthouder bij Delfland.

11.2 Leverancier draagt zorg voor adequate en zorgvuldige afhandeling van security incidenten.

11.3 Leverancier beschikt over een uitgewerkt incident management proces.

11.4 Leverancier voert analyses uit op de security incidenten en deelt de door te voeren verbeteringen.

11.5 Delfland heeft het recht op doormelding van incidenten aan CERT-WM en NCSC en in het kader van NIS2 aan betreffende toezichthouder

11.6 Delfland moet, in aanvulling op de mogelijkheid een audit uit te (laten) voeren, in staat worden gesteld om gedurende of na informatiebeveiligingsincidenten controles uit te voeren op de naleving van de in de overeenkomst genoemde vereisten. Delfland heeft daarbij het recht om een uitvraag te doen naar verbetermaatregelen naar aanleiding van een cyberincident.

12. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

12.1 De leverancier neemt in alle redelijkheid maatregelen om de integriteit en beschikbaarheid van de data te garanderen. Het maximaal aanvaardbare dataverlies (Recovery Point Objective) en de hersteltijd bij calamiteiten (Recovery Time Objective) zijn vastgelegd in een SLA en/of andere afspraken. De leverancier moet op enige wijze aan Delfland aantoonbaar kunnen maken dat dit is geborgd en periodiek wordt geverifieerd en geëvalueerd.

12.2 De leverancier heeft een recoveryplan, waarin zijn opgenomen: alle nodige voorzieningen voor back-up en herstel, kopieën van gegevens en programmatuur, evenals benodigde herstelmaatregelen na een incident zoals b.v. een besmetting met malware.

12.3 De leverancier beschikt over een business continuïteitsplan voor borging van de beschikbaarheid van de dienstverlening en toont aan dat dit minstens jaarlijks wordt getest.

13. Naleving

13.1 Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.
13.2 Informatiesystemen worden door de leverancier zelf periodiek (jaarlijks) gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses, penetratietesten (malware)scanning en monitoring.
13.3 Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter maximaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerstvolgende onderhoudsronde van het systeem.
13.4 Indien dit niet mogelijk is dient direct contact opgenomen te worden met de ICT servicedesk via tel. 015-2608008 en de accounthouder bij Delfland.

Audit bij Hoge impact/Kritieke systemen (bij afwezigheid ISAE 3402 Type 2):

In geval een kritiek systeem geen assurance verklaring kan afgeven worden de volgende assurance vragen gesteld en zal de aantoonbaarheid gecontroleerd worden:

Toon aan of leg uit:

- Controle op business continuïteitsprocessen
  - Is er een BCP opgesteld?
  - Zijn rollen en verantwoordelijkheden bekend?
  - Wordt er jaarlijks geoefend?
- Controle op bewustwordingsprocessen
  - Is er een bewustwordingsprogramma opgesteld?
  - Waaruit bestaat dit bewustwordingsprogramma?
- Controle op change processen
  - Doorlopen wijzigingen een vast wijzigingsproces?
  - Worden wijzigingen beoordeeld op impact op informatiebeveiliging?
- Controle op monitoring processen
  - Vindt er monitoring plaats op de omgevingen?
  - Worden afwijkende activiteiten geregistreerd in SIEM?
- Controle op incident management processen
  - Bestaat er een uitgewerkt incident management proces?
  - Zijn rollen en verantwoordelijkheden bekend?
  - Wordt geïnvesteerd in de juiste kennis voor betrokkenen?
  - Vinden er regelmatig testen plaats in het incident management proces?
- Controle op risico management processen
  - Zijn alle relevante informatiebeveiligingsrisico's in kaart gebracht?
  - Worden risico's actief gemitigeerd en gemonitord?
  - Worden er maatregelen getroffen op basis van de opgestelde en geïdentificeerde risico's?
- Controle op vulnerability management processen
  - Is er een vulnerability management proces?
  - Worden tijdig hoge en kritieke kwetsbaarheden verholpen?

    - Worden regelmatig pentesten uitgevoerd?
        - Worden de aanbevelingen tijdig doorgevoerd?
- Controle op leveranciersmanagement processen
    - Hoe worden risico's in de leverancierskeketen in kaart gebracht, die betrokken is bij het leveren van een dienst of product aan Hoogheemraadschap Delfland ?
    - In hoeverre wordt de naleving van de security afspraken met deze leveranciers gemonitord?
    - Is er overzicht van alle kritieke (onder)leveranciers?