Tactisch Informatieveiligheidsbeleid

Versie	: definitief concept
Auteurs	: Hielco Koeze, Peter Bruin, Michel van der Linden, Wim van Schoonhoven, Ineke Weber, Ellen Manshanden
Begeleiding	: Martijn van Engelen MSc (BMC)
Datum	: 25 november 2015

I Voorwoord

I.I Totstandkoming

In dit document is het tactische informatieveiligheidsbeleid beschreven van De Waddeneilanden.

Het informatieveiligheidsbeleid (waaronder voorliggende tactische deel en het strategische deel vallen) is gebaseerd op de internationale standaarden voor informatieveiligheid: NEN/ISO 27001 en NEN/ISO 27002. Op basis van deze standaard is de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING) opgeleverd. Deze Baseline Informatiebeveiliging geeft een specifieke invulling aan de wijze waarop de veiligheid van informatie binnen gemeentelijke organisaties moet zijn geborgd. De uitgangspunten uit deze baseline zijn integraal opgenomen in dit tactische informatieveiligheidsbeleid. Evenals de richtlijnen van het DigiD beveiligingsassessment (DigiD audit). Hierdoor is een actueel en volledig naar de laatste inzichten opgesteld beleidsplan voor De Waddeneilanden ontstaan.

Dit tactische beleid is zodanig opgezet dat het een naslagwerk vormt voor medewerkers en management die in het kader van werkzaamheden of een project moeten weten aan welke kwaliteitsaspecten aandacht moet worden besteed. De intentie is niet dat alle medewerkers exact weten wat er in het informatieveiligheidsbeleid staat, maar men moet wel weten dat het beleid er is, hoe het te gebruiken en wat de belangrijkste uitgangspunten zijn.

De basis van dit informatieveiligheidsbeleid wordt gevormd door Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING).

I.II Leeswijzer en ambitieniveau

Dit document bevat een verdere tactische uitwerking van hetgeen in het strategische informatieveiligheidsbeleid beschreven en vastgesteld is. Door vaststelling van het strategische informatieveiligheidsbeleid door de colleges van B&W is automatisch ingestemd met de verdere tactische uitwerking van het strategische beleid in voorliggend document.

De gebieden waar informatieveiligheid betrekking op heeft, worden tijdens de fase van risicoanalyse geïnventariseerd en vervolgens van een prioriteit voorzien (zie hoofdstuk 1 van het strategisch informatieveiligheidsbeleid). De organisatie maakt tijdens dit proces zelf keuzes over de prioritering en fasering van de implementatie van de onderdelen van het beleidsplan.
Enkele beleidsuitgangspunten hebben betrekking op aandachtgebieden die pas actueel worden indien de organisatie voor een dergelijke keuze of vraagstuk staat, bijvoorbeeld de inzet van Cloudtechnologie, gezamenlijk uitbesteden van software ontwikkeling of de aanschaf van een nieuw informatiesysteem. In dat specifieke geval hanteert de organisatie de beleidsuitgangspunten in dit document om de veiligheid van informatie bij deze keuze te vergroten.

Met dit document wordt daarnaast bepaald dat de organisatie bij voorkomende keuzes en vraagstukken ten aanzien van de veiligheid van informatieprocessen de beleidsregels in dit document en die uit het strategische informatieveiligheidsbeleid als uitgangspunt hanteert.

1. Classificatie en beheer van informatie en bedrijfsmiddelen

Doelstelling:
Het bepalen, handhaven en waarborgen van het juiste veiligheidsniveau voor informatie, (informatie) systemen en bedrijfsmiddelen.

Resultaat:
Een goed overzicht van alle ICT-componenten en andere relevante bedrijfsmiddelen en een toegewezen eigenaarschap. Een informatieclassificatiesysteem waarmee de behoefte, de prioriteit en de mate van beveiliging kan worden bepaald.

1.1 Inventarisatie van informatie en (informatie) bedrijfsmiddelen

Om een passend veiligheidsniveau te kunnen bieden, moeten de informatie en de bedrijfsmiddelen worden geïnventariseerd en de waarde en het belang ervan worden vastgelegd.

SSL Gemeente Leeuwarden houdt een registratie bij van alle bedrijfsmiddelen die verband houden met (informatie) systemen (configuratiemanagement):

- Informatie (bijvoorbeeld databases, gegevensbestanden, documentatie en procedurebeschrijvingen);
- Programmatuur (bijvoorbeeld systeemprogrammatuur en standaardsoftware inclusief versiebeheer);
- Fysieke bedrijfsmiddelen (bijvoorbeeld apparatuur, schijven, accommodatie en netwerkinfrastructuur en actieve componenten);
- Diensten (bijvoorbeeld communicatiediensten, PKI diensten, energievoorziening ten behoeve van de informatievoorziening).

In de registratie is opgenomen waar de gegevens(bestanden) zijn opgeslagen, op welke computers de programmatuur draait, van welke componenten daarbij gebruik wordt gemaakt en wie de procesverantwoordelijken en beheerders zijn.

Het team Facilitaire Zaken houdt een registratie bij van alle fysieke voorzieningen die verband houden met (informatie) veiligheid van ruimten, gebouw(en) en de directe omgeving van de gemeentekantoren.

1.2 Eigendom van informatie en bedrijfsmiddelen

Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie. Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit is een verantwoordelijk afdelingshoofd benoemd.

1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Er zijn regels vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT voorzieningen en informatieprocessen.

1.4 Classificatie van informatie en bedrijfsmiddelen

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen ten aanzien van informatieprocessen en informatiesystemen worden beveiligingsclassificaties gebruikt. De gemeentelijke informatiesystemen worden geclassificeerd op de drie kwaliteitsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid (BIV). Onderstaande tabel geeft de classificatie niveaus weer. Na deze classificatie is onder meer duidelijk welke specifieke gemeentelijke informatie als vertrouwelijk wordt geclassificeerd. Na dit inzicht is duidelijk welke maatregelen per informatiesysteem nodig zijn.

Classificatietabel			
Niveau	**Vertrouwelijkheid**	**Integriteit**	**Beschikbaarheid**
Geen / 0	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de gemeente*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner)*
Laag / I	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het intranet)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: rapportages)*	**Noodzakelijk** informatie mag incidenteel niet beschikbaar zijn *(bv: administratieve gegevens)*
Midden / II	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, financiële gegevens*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	**Belangrijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: voorwaardelijke primaire proces informatie)*
Hoog / III	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) *(bv: zorggegevens en strafrechtelijke informatie)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: specifieke gemeentelijke informatie op de website o.a waaraan rechten zijn te ontlenen)*	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistraties BRP en SUWI)*

2. Beveiligingsaspecten ten aanzien van personeel

Doelstelling:
Het verminderen van de risico's van menselijke fouten, diefstal, fraude of misbruik van voorzieningen.

Resultaat:
Werknemers, ingehuurd personeel en externe gebruikers kennen en begrijpen hun verantwoordelijkheden en zijn geschikt voor de rollen waarvoor zij (beoogd) worden benoemd.

2.1 Algemene uitgangspunten ten aanzien van personele beveiligingsaspecten

Hieronder volgen de geldende algemene uitgangspunten:

- De teamleider is verantwoordelijk voor het juist afhandelen van de beveiligingsaspecten van het aangaan, wijzigen en beëindigen van een dienstverband of een overeenkomst met externen. Het team P&O houdt toezicht op dit proces;
- De teamleider bepaalt welke rol(len) de medewerker moet vervullen en welke autorisaties voor het raadplegen, opvoeren, muteren en afvoeren van gegevens moeten worden verstrekt;
- Bij inbreuk op de beveiliging gelden voor medewerkers de gebruikelijke disciplinaire maatregelen, zoals onder meer genoemd in het Ambtenarenreglement en gemeentelijke regelingen;
- Regels die volgen uit dit beleid en andere gemeentelijke regelingen gelden ook voor externen, die in opdracht van de gemeente werkzaamheden uitvoeren.

2.2 Voorwaarden tewerkstelling vast personeel

Iedere vaste medewerker in dienst van één van de gemeenten van De Waddeneilanden, legt de eed/belofte af. Alle medewerkers worden geacht te handelen conform het integriteitsbeleid dat ter ondertekening wordt voorgelegd. Daarnaast overleggen medewerkers die belast zijn met de Basisregistratie Personen (BRP) en waarde documenten een Verklaring Omtrent Gedrag (VOG). Bij indiensttreding wijst de teamleider de werknemer bovendien op de aanwezigheid van eventueel aanvullende, specifieke gedragsregels ten aanzien van een informatiesysteem of team. Dit laatste gebeurt in ieder geval bij de Basisregistratie Personen (BRP), Waardedocumenten en SUWI.

2.3 Voorwaarden tewerkstelling externen

Externen die toegang hebben tot vertrouwelijke gemeentelijke informatie, zoals uitzendkrachten, stagiaires en ingehuurde externe personen, tekenen een geheimhoudingsverklaring, en ontvangen het integriteitsbeleid ter inzage. Daarnaast overleggen deze externen een Verklaring Omtrent Gedrag (VOG). De teamleider wijst de tijdelijke werknemer op de aanwezigheid van eventueel aanvullende, specifieke gedragsregels ten aanzien van een informatiesysteem of team. Dit laatste gebeurt in ieder geval bij de Basisregistratie Personen (BRP,) en Waarde documenten.

2.4 Toegang en bevoegdheden personeel

Bij indiensttreding worden de fysieke en logische toegangsbevoegdheden volgens een vastgestelde procedure toegekend. De beslissing hierover moet door geautoriseerde personen worden genomen. Bij dienstbeëindiging of bij wijziging van functie worden alle bedrijfsmiddelen van de organisatie geretourneerd. Autorisaties worden in opdracht van het lijnmanagement met onmiddellijke ingang en volgens een vastgestelde procedure verwijderd of aangepast aan de nieuwe status.

2.5 Opleiding en communicatie

Alle medewerkers (en voor zover van toepassing externe gebruikers van de gemeentelijke systemen) krijgen training in procedures die binnen de gemeente of team gelden voor informatieveiligheid. Deze training dient regelmatig te worden herhaald om het beveiligingsbewustzijn op peil te houden. Ten aanzien van communicatie en bewustwording geldt dat:

- Alle medewerkers binnen de organisatie worden ingelicht over het informatieveiligheidsbeleid en de (beveiligings)procedures van de gemeente en informatie krijgen over het correcte gebruik van de ICT- en toegangsvoorzieningen. Dit geldt eventueel ook voor externe gebruikers;
- De algemeen directeur/gemeentesecretaris, het MT en de teamleiders de algehele communicatie en bewustwording rondom informatieveiligheid bevorderen;
- De teamleider bevordert dat medewerkers (en externe gebruikers van onze systemen) zich houden aan beveiligingsrichtlijnen;
- In werkoverleggen periodiek aandacht wordt geschonken aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd in planningsgesprekken.

2.6 Bijzondere situaties

In het geval van ernstige verdenkingen tegen een medewerker op het gebied van verduistering of gedrag wat in strijd is met de interne regels, is het mogelijk dat de gemeenten gebruik maken van opsporingsmogelijkheden zoals (verborgen) camera's, microfoons en loggegevens. Ook de door de gemeente verstrekte telefoon en automatiseringsmiddelen kunnen in deze gevallen worden onderzocht. Voor de inzet van deze middelen is schriftelijke toestemming nodig van de algemeen directeur/gemeentesecretaris. Dit geldt in algemene zin, niet voor de bijzondere situatie zelf!

3. Fysieke beveiliging

Doelstelling:
De fysieke bescherming van gebouwen, terreinen, informatie en (informatie)systemen tegen onbevoegde fysieke toegang, schade of verstoring van continuïteit.

Resultaat:
Maatregelen en procedures waarmee gebouwen, informatie- en ICT-voorzieningen adequaat worden beschermd tegen ongeautoriseerde toegang, kennisneming, verminking of diefstal, waardoor schade en verstoringen worden voorkomen.

3.1 Algemene uitgangspunten ten aanzien van fysieke beveiliging

- De schade door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) wordt beperkt door passende preventieve maatregelen;
- Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe;
- De uitgifte van toegangsmiddelen wordt geregistreerd;
- De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering (en het risicoprofiel);
- Indien gebruik gemaakt wordt van beeldmateriaal wordt dit beperkt door de Wet Bescherming Persoonsgegevens en nadere regels;
- De fysieke toegang tot ruimten waar zich informatie en ICT-voorzieningen bevinden is voorbehouden aan bevoegd personeel;
- Serverruimtes, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende ‘best practices’.

3.2 Inventarisatie van bedrijfsmiddelen

Om een passend beveiligingsniveau te kunnen bieden, moeten de informatie en de bedrijfsmiddelen worden geïnventariseerd en de waarde en het belang ervan worden onderkend. Het team Facilitaire Dienstverlening houdt een registratie bij van alle bedrijfsmiddelen die verband houden met veiligheid van ruimten, gebouw(en) en de directe omgeving van de gebouwen:

- De preventieve, detectieve, correctieve en repressieve systemen met betrekking tot inbraak, ontruiming, brand en toegang;
- Overzicht van toegangsrechten van personen tot ruimten, gebouwen en directe omgeving van het gebouw, zoals parkeerplaatsen.

3.3 Servicetaken

Indien voor de bewaking van de gebouwen, personen en goederen een externe bewakingsdienst wordt ingehuurd, voldoet deze bewakingsdienst aan de eisen volgens de Wet Particuliere Beveiligingsorganisaties en Recherchebureaus, beschikt deze over een vergunning van het Ministerie van

Justitie en is deze aangesloten bij een brancheorganisatie. Er zijn afspraken gemaakt bij wie de bewakingsdienst verantwoording moet afleggen.

3.4 Fysieke toegang computer- en datacomruimten

De fysieke toegang tot specifieke computer-/serverruimten onder beheer van SSL gemeente Leeuwarden is voorbehouden aan de volgende categorieën personen:

- De leden van de SSL gemeente Leeuwarden die uit hoofde van functie (technische) werkzaamheden aan de centrale computers of telecom apparatuur moeten verrichten;
- De door de IT manager (SSL Leeuwarden) geautoriseerde personen (zoals bijvoorbeeld de Bedrijfshulpverlening);
- Personen die niet onder de genoemde categorieën vallen, mogen de specifieke ruimten alleen betreden onder begeleiding van een geautoriseerde medewerker van SSL gemeente Leeuwarden.

3.5 Bewegwijzering computerruimten

Binnen de vestiging zijn geen wegwijzers aangebracht waaruit de locaties van de ICT-ruimten kunnen worden afgeleid. Ook zijn deze ruimten niet aangegeven op publieke plattegronden of in publicaties, tenzij hieraan andere eisen worden gesteld, bijvoorbeeld door de brandweer.

3.6 Verwijderen apparatuur en gegevensdragers

De SSL gemeente Leeuwarden heeft een procedure voor het verwijderen of gereed maken voor hergebruik van overbodige apparatuur en gegevensdragers waarop gemeentelijke informatie en in licentie gebruikte software is opgeslagen.
Denk hierbij aan de harde schijven van pc's en netwerkservers, cd's/dvd's, back-up tapes, USB sticks en overige gegevensdragers. In deze procedure staan voorschriften voor het verwijderen en zo nodig onbruikbaar maken of vernietigen van die informatie.

3.7 Datakluizen en reserve apparatuur

- De datakluizen voldoen aan de eisen die gesteld worden om opgeslagen gegevensdragers in voldoende mate te beschermen tegen stof, brand, water, beschadiging en diefstal;
- Reserve apparatuur en back-ups worden gescheiden bewaard op een andere locatie of een datacenter om de gevolgen van een calamiteit te minimaliseren.

3.8 Clean desk en clear screen beleid

De Waddeneilanden stellen een "clean desk"-beleid vast voor papieren en verwijderbare opslagmedia, zodat dit soort materialen niet onbeheerd op het bureau liggen. Daarnaast geldt een "clear screen" beleid voor ICT-voorzieningen. Dit betekent dat alle medewerkers bij het verlaten van de werkplek het scherm locken en dat na een bepaald tijdsverloop het beeldscherm "op zwart" gaat en de toegang tot het werkstation wordt geblokkeerd middels een toegangscode. Dit om het risico van onbevoegde toegang tot, verlies van of schade aan informatie, informatiedragers en ICT-voorzieningen tijdens en buiten normale werktijden te beperken.

3.9 Beveiliging van (mobiele) apparatuur

Informatieverwerkende mobiele apparatuur moet zowel binnen als buiten het gebouw zo mogelijk fysiek beschermd worden. Dit betreft laptops, PDA's, tablets (bijvoorbeeld iPad's), memorysticks en mobiele telefoons (smartphones).

4. Beheer van communicatie- en bedieningsprocessen

Doelstelling:
Het garanderen van correcte en veilige bediening en beheer van de ICT-voorzieningen.

Resultaat:
Maatregelen en procedures voor het beheer en de bediening van de ICT-voorzieningen en het adequaat reageren op incidenten.

4.1 Organisatorische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen

- In beginsel mag niemand autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd. Indien dit toch noodzakelijk is, dient een audit trail te worden vastgelegd van alle handelingen en tijdstippen in het proces, dusdanig dat transactie kan worden herleid. De audit trail is niet toegankelijk voor degene wiens handelingen worden vastgelegd;
- In beginsel is er een scheiding tussen beheertaken en overige gebruikstaken. Hierbij worden beheerwerkzaamheden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker. Er wordt echter per specifieke situatie bezien of deze scheiding een werkbare situatie oplevert en of de veiligheid hierdoor in dit specifieke geval wordt verhoogd.

4.2 Uitgangspunten voor controle en logging

Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, worden vastgelegd in logbestanden op een manier die in overeenstemming is met het risico, en zodanig dat tenminste wordt voldaan aan alle relevante wettelijke eisen, met name ten aanzien van de wet BRP en SUWI.

In een logregel worden alleen de voor de rapportage noodzakelijke gegevens opgeslagen.
Er worden maatregelen getroffen om te verzekeren dat gegevens over logging beschikbaar blijven en niet gewijzigd kunnen worden door een gebruiker of systeembeheerder. De bewaartermijnen zijn in overeenstemming met wettelijke eisen.

Ten aanzien van SUWI vraagt de security officer SUWI meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van SUWInet door de gemeente. Ten aanzien van de BRP worden logging rapportages minimaal maandelijks beoordeeld door de BRP beheerder.

4.3 Beheer van de dienstverlening door een derde partij

Bij externe hosting van data en/of services (uitbesteding, cloud computing) blijft de gemeente eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Dit is gebonden aan regels en vereist goede (contractuele) afspraken en controle hierop.
Uitgangspunten bij externe hosting van data en/of services zijn:

- Goedgekeurd door de verantwoordelijke teamleider van de gemeente;
- Voldoet aan de criteria voor leveranciers van webapplicaties en webservices opgenomen in de norm ICT-beveiligingsassessments DigiD;
- In overeenstemming met informatieveiligheidsbeleid en algemeen gemeentelijk beleid;
- Vooraf gemeld bij SSL gemeente Leeuwarden (ICT) ten behoeve van toetsing op beheeraspecten;
- De beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de (bewerkers)overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd;
- De diensten, rapporten en registraties, die door de derde partij worden geleverd, worden gecontroleerd en er bestaat de mogelijkheid voor het uitvoeren van (periodieke) audits;
- In de basis-SLA voor dienstverlening is aandacht besteed aan informatieveiligheid;
- Er is een basiscontract voor de toegang tot de ICT-voorzieningen en/of de informatievoorziening (bestanden, gegevens) door derden waarin de kaders staan voor de toegang tot ICT-voorzieningen door derden.

4.4 Telewerken en thuiswerken

De Waddeneilanden staan telewerken toe (op afstand werken op het netwerk van de gemeente, bijvoorbeeld thuiswerken) na toestemming van de verantwoordelijke teamleider. Hiervoor worden beveiligingsmaatregelen vastgesteld en getroffen die in overeenstemming zijn met het gemeentelijk informatieveiligheidsbeleid en voor zover niet wordt verboden door wet en regelgeving.[1]

4.5 Mobiele (privé-)apparatuur

Ten aanzien van 'Bring Your Own Device/ Choose Your Own Device'' (BYOD/CYOD) wordt beleid opgesteld en worden beveiligingsmaatregelen vastgesteld en getroffen die in overeenstemming zijn met het gemeentelijk informatieveiligheidsbeleid en voor zover niet wordt verboden door wet en regelgeving.[2]

4.6 Gebruik internet en email

E-mail- en internetprotocol
De Waddeneilanden heeft een protocol (gedragscode) ten aanzien van het gebruik van e-mail en het gebruik van internet. In deze protocollen zijn maatregelen opgenomen om beveiligingsrisico's, verbonden aan het gebruik van e-mail en internet, te beperken.

4.7 Sociale media

Het gebruik van sociale media door medewerkers van De Waddeneilanden is toegestaan. De medewerkers dienen zich ervan bewust te zijn dat ze online gezien worden als vertegenwoordigers van de organisatie. Uitingen op het internet worden permanent opgeslagen en kunnen eventueel via andere media opnieuw worden gepubliceerd. Voor het gebruik van sociale media is het protocol Sociale Media beschikbaar.

[1] Vanuit de SUWI regelgeving en de BRP regelgeving wordt thuisgebruik niet zondermeer toegestaan.
[2] Vanuit de SUWI regelgeving en de BRP regelgeving wordt thuisgebruik niet zondermeer toegestaan.

4.8 Uitwisseling van informatie over netwerken

Bij het beheren van netwerken moet onderscheid gemaakt worden tussen het eigen netwerk en netwerken die de grens van de organisatie overschrijden. Voor transport van vertrouwelijke en privacygevoelige gegevens via openbare netwerken zijn extra maatregelen nodig.
Bij gebruik van andere netwerken moet geanalyseerd worden of eigen eisen en de eisen van het andere netwerk in overeenstemming met elkaar zijn en niet leiden tot onoverkomelijke problemen.
Verantwoordelijkheden en procedures voor toegang en het beheer van netwerken
en apparatuur op afstand (inclusief de apparatuur op de werkplek) zijn vastgelegd en worden gecommuniceerd naar betrokken partijen.

5. Logische toegangsbeveiliging

Doelstelling:
Het beheersen van de toegang tot informatie en (informatie)systemen.

Resultaat:
Gedocumenteerd beleid en daarvan afgeleide maatregelen en procedures voor effectieve toegangsbeveiliging tot de informatie-infrastructuur en gegevens en het voorkomen van ongeautoriseerde toegang.

5.1 beleid voor logische toegangsbeveiliging

Om effectieve toegangscontrole tot vertrouwelijke en privacygevoelige informatie te kunnen implementeren en onderhouden is er een organisatiebreed toegangsbeleid. Naast dit organisatiebrede toegangsbeleid heeft ieder informatiesysteem nog een specifiek gedefinieerd toegangsbeleid, wat is afgestemd op de classificatie van de informatie.
De procesverantwoordelijke toetst of de door SSL gemeente Leeuwarden of applicatiebeheer geïmplementeerde bevoegdheden zijn toegekend of verwijderd conform de aanvraag.

5.2 Beheer van toegangsrechten

Voor de beheersing van toewijzing van toegangsrechten is een procedure vastgesteld, waarin de gehele cyclus is opgenomen van het registreren tot het afmelden van gebruikers. Naast wachtwoorden kunnen ook andere technologieën worden toegepast voor gebruikersidentificatie en authenticatie, zoals biometrie, handtekeningverificatie, hardware (bijvoorbeeld token), SMS authenticatie en cryptografische sleutels. Bij het beheer van gebruikerswachtwoorden is vastgelegd op welke wijze het initiële wachtwoord aan de gebruiker kenbaar wordt gemaakt en hoe gehandeld wordt bij het vergeten van het wachtwoord. Verstrekte wachtwoorden moeten onmiddellijk na het eerste gebruik door de gebruiker worden gewijzigd.

5.3 Externe toegang

De gemeente kan een externe partij toegang verlenen tot het gemeentelijke netwerk. Hiervoor dient een procedure gevolgd te worden. Externe partijen kunnen niet op eigen initiatief verbinding maken met het besloten netwerk van de gemeente, tenzij uitdrukkelijk overeengekomen.
De externe partij is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. De gemeente heeft het recht hierop te controleren en doet dat aan de hand van de audit trail en interne logging.

5.4 Controle op toegangsrechten

Alle medewerkers die van het netwerk of applicaties gebruikmaken, moeten door het systeem of applicatie op unieke wijze geïdentificeerd kunnen worden. Om de toegang tot de Informatiearchitectuur

effectief te beheren, wordt periodiek een uitdraai gemaakt van de verstrekte toegangsmachtigingen. Deze uitdraai wordt gecontroleerd op juistheid en volledigheid door de controller informatieveiligheid.

5.5 Toegangsbeveiliging met betrekking tot werkstations

Inlogprocedure werkstations
De toegang tot een informatiesysteem verloopt via een inlogprocedure, bedoeld om het risico van ongeautoriseerde toegang te beperken.

Gebruikersidentificatie en -authenticatie
Identificatie en authenticatie van de gebruiker vindt altijd plaats. Hierdoor zijn activiteiten in het (informatie)systeem herleidbaar tot een natuurlijk persoon. Identificatie en authenticatie kunnen plaatsvinden door middel van gebruikersnamen in combinatie met wachtwoorden, smartcards, tokens of SMS authenticatie.

Schermbeveiliging (clear screen)
Medewerkers moeten bij het verlaten van de werkplek het scherm locken en na een vaste periode van inactiviteit wordt een werkstation automatisch geblokkeerd. Bij werkstations op locaties met verhoogd risico moeten de programma- en netwerksessies afgesloten worden en wordt de gebruiker uitgelogd.

5.6 Toegangsbeveiliging met betrekking tot (informatie)systemen

Toegang tot (informatie)systemen
Autorisatie voor (informatie)systemen wordt verleend op grond van de rol van de medewerker.
Binnen het (informatie)systeem krijgt de medewerker alleen toegang tot de functionaliteit en gegevens die nodig zijn voor de uitvoering van zijn of haar rol/taken. Alle medewerkers hebben een individueel gebruikersprofiel zowel op netwerk als op applicatieniveau waardoor mutaties en zo mogelijk ook raadplegingen altijd zijn terug te herleiden tot een individu.

Componenten van (informatie)systemen
Een (informatie)systeem kan uit meerdere componenten bestaan, zoals applicatie, pc, netwerk, besturingssysteem, database, firewall. Voor elk van deze componenten moet autorisatie apart worden verleend.

(Informatie)systemen met vertrouwelijke of privacygevoelige gegevens
(Informatie)systemen die vertrouwelijke of privacygevoelige gegevens verwerken, vereisen speciale maatregelen, zoals het plaatsen in een aparte beveiligde omgeving of domein.
De procesverantwoordelijke stelt expliciet de gevoeligheid van een (informatie)systeem vast en de noodzaak voor aanvullende maatregelen.

6. Verwerving, ontwikkeling en onderhoud van systemen

Doelstelling:
Het waarborgen dat beveiliging wordt ingebouwd in (informatie)systemen en dat beveiligingseisen worden meegenomen in het proces van systeemontwikkeling en -onderhoud.

Resultaat:
(Informatie)systemen waarin zoveel mogelijk geautomatiseerde beveiligingsmaatregelen zijn ingebouwd. Maatregelen en procedures waarmee de beveiliging tijdens de ontwikkeling en het onderhoud van (informatie)systemen wordt gegarandeerd.

6.1 Beveiligingseisen voor (informatie)systemen

Bij de ontwikkeling van (informatie)systemen moeten beveiligingseisen vanaf aanvang in het ontwerpproces worden meegenomen. Dit geldt ook voor teamoverstijgende (informatie)systemen. Bij standaardprogrammatuur moet voor aanschaf worden vastgesteld of geautomatiseerde beveiligingsmaatregelen zijn ingebouwd. Bij het onderhoud van (informatie)systemen moet informatieveiligheid een vast aandachtspunt zijn.

6.2 Cryptografische beveiliging

Cryptografische systemen en technieken moeten worden toegepast in (informatie)systemen die vertrouwelijke en/of privacygevoelige gegevens verwerken en die onvoldoende kunnen worden beveiligd door andere maatregelen. Dit geldt met name voor gegevens die via openbare, grensoverschrijdende en draadloze netwerken worden getransporteerd (ook USB-sticks) en voor systemen die als standalone toepassing gebruikt worden, bijvoorbeeld op laptops, PDA's, tablets en smartphones.

Wanneer er gebruik gemaakt wordt van cryptografische sleutels dan dient het sleutelbeheer te zijn georganiseerd. Het gaat dan met name om de bescherming van de sleutels, het inrichten van de beheersrollen en de recoverymogelijkheden. Een sleutelbeheersysteem moet er minimaal voor zorgen dat sleutels niet onversleuteld op de servers te vinden zijn.

6.3 Uitbesteding ontwikkeling van (informatie)systemen

In deze situatie ontwikkelt de gemeente niet zelf een (informatie) systeem, maar besteedt het ontwikkel- en productiewerk uit. De gemeente gaat vervolgens over tot aanschaf van het (informatie) systeem of afname van een dienst.

6.4 Hardening van systemen

De hardening van alle systemen maar met name de internet facing systemen dient strak te zijn geregeld. Voor de webapplicaties en systemen geldt: alles dat open staat moet een reden hebben en alles dat open staat moet secure worden aangeboden.

De hardening van interne systemen mag minder stringent. Voor interne systemen moeten de management functies secure zijn, er geen onveilige protocollen worden gebruikt, de default wachtwoorden zijn gewijzigd, en ongebruikte applicaties worden verwijderd.

Systeem hardening is een leverancier specifiek proces, aangezien de verschillende leveranciers het systeem op verschillende manieren configureren en voorzien van verschillende diensten tijdens het standaard (default) installatie proces. Alle componenten van de ICT-infrastructuur moeten deel uitmaken van het hardeningsproces.

Voorbeelden van risico's die door hardening teniet worden gedaan zijn:

- Indien (externe) systemen, zoals webservers en mailservers 'reclame' maken voor hun type en versie, wordt het een aanvaller makkelijker gemaakt om bekende zwakke plekken van deze systemen te exploiteren;
- Systemen die onnodige diensten draaien en poorten open hebben die niet open hoeven te staan zijn makkelijker aan te vallen omdat deze diensten en poorten mogelijkheden bieden om het systeem aan te vallen.

6.5 Hardening van websites

Speciale aandacht krijgen hierbij de websites van de gemeente. Aangezien niet langer gebruikte websites of verouderde informatie die toegankelijk is via het internet een beveiligingsrisico opleveren dient de gemeente deze informatie te (laten) verwijderen. De gemeente en meer in het bijzonder de eigenaar van de specifieke website is hiervoor verantwoordelijk.

7. Beveiligingsincidenten

Doelstelling:
Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden, die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

Resultaat:
Formele procedures voor rapportage van gebeurtenissen en escalatie. Alle werknemers, ingehuurd personeel en externe gebruikers zijn op de hoogte van deze procedures voor het rapporteren van de verschillende soorten gebeurtenissen en zwakke plekken die invloed kunnen hebben op de beveiliging van de bedrijfsmiddelen.

7.1 Definitie beveiligingsincident

Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de beschikbaarheid, de integriteit of de vertrouwelijkheid van informatie of informatiesystemen in gevaar is of kan komen.

Hierbij staat beschikbaarheid voor de garanties over het afgesproken niveau van dienstverlening en over de toegankelijkheid en bruikbaarheid van informatie(systemen) op de afgesproken momenten. Integriteit staat voor de juistheid, volledigheid en tijdigheid van informatie(systemen). Vertrouwelijkheid heeft betrekking op exclusiviteit van informatie en de privacybescherming. Hiermee wordt bedoeld dat uitsluitend gemachtigden toegang mogen hebben tot informatie(systemen).

7.2 Procedure melding en omgang beveiligingsincidenten

Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.

8. Continuïteitsbeheer

Doelstelling:
Het voorkomen van onderbreking van activiteiten van de gemeentelijke ICT-infrastructuur en het beschermen van de kritische bedrijfsprocessen tegen de effecten van ingrijpende storingen of calamiteiten.

Resultaat:
Een beheerst proces voor het waarborgen van de bedrijfscontinuïteit, waarmee de gebruikers, binnen een vastgestelde periode na het optreden van een beveiligingsincident of calamiteit, op aanvaardbaar niveau hun taken kunnen hervatten.

8.1 Proces van continuïteitsmanagement

Er is een beheerst proces vastgesteld om de bedrijfscontinuïteit van de organisatie als geheel te waarborgen. Indien interne of externe uitwijk is gerealiseerd, wordt minimaal jaarlijks een uitwijktest uitgevoerd. De uitwijkprocedures zijn ondergebracht in het draaiboek uitwijk.

8.2 Relatie met nood- en ontruimingsplan

Het team Facilitaire Zaken zorgt voor het vaststellen van een ontruimingsregeling voor de computerruimte(n). Dit in aansluiting op het algemene noodplan en ontruimingsplan. Hierin is aangegeven op welke wijze de computerfaciliteiten worden uitgeschakeld bij calamiteiten, eventueel van buitenaf op afstand te regelen. Voorts is vastgesteld hoe de SSL gemeente Leeuwarden de afgesproken regeling zal testen en met welke frequentie.

8.3 Veiligstelling programmatuur

Voor alle systeemsoftware en informatiesystemen moet een afweging gemaakt worden of de broncodes door middel van bijvoorbeeld een Escrow-contract bij derden moeten worden ondergebracht.

8.4 Monitoring capaciteit

Voor alle relevante ICT-middelen wordt het capaciteitsbeslag dusdanig gepland dat continu wordt voldaan aan de eisen die gesteld worden vanuit de afspraken met de afnemers van het systeem. Performanceproblemen worden tijdig gesignaleerd en geanalyseerd op basis van betrouwbare gegevens.

9. Naleving

Doelstelling:
Het voorkomen van schending van strafrechtelijke of civielrechtelijke wetgeving, wettelijke, reglementaire of contractuele verplichtingen of beveiligingseisen en waarborgen dat systemen en processen voldoen aan het beveiligingsbeleid van De Waddeneilanden.

Resultaat:
Maatregelen en procedures waarmee naleving van wetten, verplichtingen en beveiligingseisen uit het beleid van de gemeente bewaakt wordt.

9.1 Organisatorische uitgangspunten

- Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle gemeentelijke processen waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elk team stuurt.
- De coördinator informatieveiligheid / CISO coördineert namens de algemeen directeur/ gemeentesecretaris de uitvoering van het informatieveiligheidsbeleid;
- De SSL gemeente Leeuwarden (ICT) en (andere) externe hosting providers leggen verantwoording af aan hun opdrachtgevers over de naleving van het informatieveiligheidsbeleid. Bij uitbestede (beheer)processen kan een verklaring bij leveranciers worden opgevraagd (TPM of ISAE3402-verklaring);
- Naleving van regels vergt in toenemende mate ook externe verantwoording, bijvoorbeeld voor het gebruik van DigiD, SUWI en BRP en waardedocumenten. Aanvullend op dit organisatie informatieveiligheidsbeleid kunnen daarom specifieke normen gelden;
- Periodiek wordt de kwaliteit van informatieveiligheid in opdracht van de controller informatieveiligheid onderzocht door gemeentelijke auditors en door onafhankelijke externen (bijvoorbeeld door middel van ‘penetratietesten’). Jaarlijks worden meerdere audits/onderzoeken uitgevoerd. De bevindingen worden gebruikt voor de verdere verbetering van de informatieveiligheid;
- In de P&C cyclus wordt gerapporteerd over informatieveiligheid;
- Er wordt een beveiligingsdocumentatiedossier aangelegd en onderhouden. Dit dossier bevat alle relevante verplichte en niet verplichte documenten waaruit blijkt of kan worden aangetoond dat aan de specifieke beveiligingseisen is voldaan.

9.2 Naleving van informatieveiligheidsbeleid en -plan

Om de naleving van de beveiligingseisen uit het informatieveiligheidsbeleid en -plan te bewaken, legt de procesverantwoordelijke adequate organisatorische en procedurele afspraken vast. Kernelementen in het controle- en evaluatieproces zijn:

- Zelfevaluatie en/of een audit, tenminste eenmaal per jaar, door de procesverantwoordelijke;
- Managementrapportages, tenminste eenmaal per jaar, getoetst door de controller informatieveiligheid op inhoud en vorm, en ingebed in bestaande P&C -cyclus.

9.3 Naleving van wettelijke voorschriften

Relevante eisen uit wet- en regelgeving en contractuele eisen moeten voor ieder (informatie)systeem zijn vastgelegd. Er wordt deskundig advies over specifieke juridische eisen ingewonnen bij de juridische adviseur(s) van de gemeenten. Conform de Archiefwet[3] beschikken de gemeenten van De Waddeneilanden over een systeem waarin opslag, bewaartermijn en vernietiging van gegevens en informatie in analoge en digitale vorm is geregeld.

Aan de bescherming van persoonsgegevens stelt de Wet Bescherming Persoonsgegevens (WBP) duidelijke eisen. De Waddeneilanden stellen een privacy beheerder aan, die de uitvoering en de naleving van de WBP bewaakt.

9.4 Beoordeling van de naleving

Het MT en de procesverantwoordelijken (teamleiders) zorgen voor de controle en evaluatie op de naleving van wettelijke voorschriften van het informatieveiligheidsbeleid. Zij beoordelen of alle beveiligingsprocedures binnen hun verantwoordelijkheidsgebied correct worden uitgevoerd en of hun processen en (informatie)systemen voldoen aan relevante wet- en regelgeving, beveiligingsbeleid, normen en andere beveiligingseisen. Zij controleren de naleving van technische normen door productiesystemen te onderzoeken op de effectiviteit van de geïmplementeerde beveiligingsmaatregelen, bijvoorbeeld door het uitvoeren van een security scan. Daarnaast worden controles uitgevoerd door externe auditors (bv BRP-, SUWI- en BAG-audit en de externe accountant).

[3] De wettelijke plicht voor een gemeentelijk documentair structuurplan (DSP) is afgeschaft, maar het blijft verplicht om als gemeente de archiefbescheiden (document-, proces- of zaakgericht) te ordenen.

Begrippenlijst

Teamoverstijgend informatiesysteem
Systeem dat door meer dan één team wordt gebruikt en waarin gegevens van meerdere organisatieonderdelen worden vastgelegd

Audit (informatieveiligheids-)
Het door een onafhankelijke deskundige kritisch beoordelen van de opzet, het bestaan en de werking van de (beveiligings-) voorzieningen en de organisatie voor informatietechnologie op betrouwbaarheid, doeltreffendheid en doelmatigheid

Authenticatie
Verificatie van de geclaimde identiteit, bijvoorbeeld door gebruik van wachtwoord, token, biometrie of een combinatie hiervan

Autorisatie / autoriseren
Toekenning / toekennen van rechten (aan (groepen van) personen, processen en/of systemen)

Back-up
Reservekopie van een computerbestand of programmatuur

Bedrijfskritisch
Van essentieel belang voor de continuïteit van de bedrijfsprocessen

Beschikbaarheid
zie Continuïteit

Beveiligingsincident
Voorval dat de betrouwbaarheid, beschikbaarheid of vertrouwelijkheid van de Informatievoorziening verstoort, en daarmee de informatieveiligheid kan aantasten

Calamiteit
Gebeurtenis die een zodanige verstoring van de geautomatiseerde gegevensverwerking tot gevolg heeft, dat aanzienlijke maatregelen moeten worden genomen om het oorspronkelijke werkingsniveau te herstellen

Classificatie
Indeling in risicoklassen voor de aspecten beschikbaarheid, betrouwbaarheid en vertrouwelijkheid

Clean desk
Een opgeruimde werkplek waar geen vertrouwelijke of privacygevoelige documenten of andere informatiebronnen rondslingeren

Clear screen

Een uitgeschakeld of afgesloten beeldscherm dat alleen met een inlogprocedure weer actief gemaakt kan worden

Continuïteit (bedrijfs-)
De mate waarin bedrijfsprocessen ongestoord doorgang kunnen hebben

Controller informatieveiligheid
Medewerker die zich richt op de verbijzonderde interne controle op de naleving van het informatieveiligheidsbeleid en de escalatie van beveiligingsincidenten.

Coördinator informatieveiligheid / CISO
Medewerker die organisatiebreed adviseert over informatieveiligheidsvraagstukken in brede zin en activiteiten op het gebied van informatieveiligheid coördineert

Database
Een bestand waarin gedigitaliseerde gegevens op een gestructureerde manier zijn opgeslagen en bevraagd kunnen worden

Document Structuurplan (DSP)
Een DSP biedt een overzicht van alle aanwezige informatie- en archiefbestanden van een organisatie in relatie tot het werk dat in die organisatie gedaan wordt.

Eigenaar
De eigenaar van een proces of een systeem is vanuit het informatieveiligheidsbeleid verantwoordelijk voor het stellen van eisen en de inrichting van de controle hierop, zodat voldaan wordt aan het informatieveiligheidsbeleid en aan de wettelijke eisen.

Escrow
Specifiek in de softwaresector wordt escrow aangewend ter vrijwaring van de belangen van de softwareklant indien die zich wil indekken tegen bepaalde risico's in hoofde van de softwareleverancier (het meest gevreesde daarbij wellicht het faillissement van de leverancier).
De softwareleverancier zal de broncode van de software (en de bijhorende documentatie) in bewaring geven bij de escrowagent, en deze broncode regelmatig updaten indien nieuwe versies op de markt gebracht worden. Indien de leverancier dan failliet zou gaan, heeft de klant tenminste de broncode van haar applicatie en kan zij alsnog trachten haar applicatie aan de praat te houden.

Functiescheiding
Het scheiden van gerelateerde taken en bevoegdheden met als doel het voorkomen van fouten en fraude

Fysieke beveiliging
Beveiliging die met behulp van fysieke (bouwkundige, technische en/of organisatorische) middelen gerealiseerd wordt

Gateway

Verbinding tussen verschillende netwerken waarop wordt bijgehouden welke computers c.q. protocollen met elkaar verbonden mogen worden

Gebruiker / gebruikende partij
Degene die geautoriseerd gebruik maakt van een (informatie)systeem

Gegevensdrager
Een fysiek object waarin/waarop informatie is vastgelegd, bijvoorbeeld een boek, harde schijf, DVD of USB-stick

Gegevensverwerking
Handeling of geheel van handelingen met betrekking tot gegevens

Hardening
Planmatig proces om kwetsbaarheden (en daarmee veiligheidsrisico's) aan een systeem te verminderen.

Informatie- en communicatietechnologie (ICT)
Het vakgebied dat zich bezighoudt met informatiesystemen, telecommunicatie en computers.
Hieronder valt het ontwikkelen en beheren van systemen, netwerken, databanken en websites. Ook het onderhouden van computers en programmatuur en het schrijven van administratieve software valt hieronder. Vaak gebeurt dit in een bedrijfskundige context.

ICT-component
Onderdeel van de informatie- en communicatie infrastructuur, zoals netwerk, bekabeling, servers, werkstations.

Identificatie
Bepaling van de identiteit van een persoon, bijvoorbeeld door een unieke gebruikersnaam of netwerkadres

Incident
Onverwachte of ongewone gebeurtenis

Incident management
Beheer en beheersing van de afhandeling van incidenten

Informatieveiligheid
Samenhangend stelsel van activiteiten, methoden en middelen ter waarborging van beschikbaarheid, betrouwbaarheid en vertrouwelijkheid.

Informatievoorziening
Informatieveiligheidsbeleid Strategie van een organisatie met betrekking tot informatieveiligheid.

Informatieveiligheidsplan

Document waarin beschreven staat welke beveiligingsmaatregelen getroffen worden/zijn op basis van het informatieveiligheidsbeleid

Informatiesysteem
Een samenhangende, gegevensverwerkende functionaliteit voor de besturing of ondersteuning van één of meer bedrijfsprocessen

Informatievoorziening
Het geheel aan processen, bestaande uit het verzamelen, het opslaan, het verwerken van gegevens en het beschikbaar stellen ervan

Internet Protocol (IP)
Veel gebruikt protocol voor netwerkverkeer

Local Area Network (LAN)
Zie Lokaal netwerk

Logische (toegangs)beveiliging
(Toegangs)beveiliging die met behulp van programmatuur gerealiseerd wordt

Lokaal netwerk (LAN)
Fysiek afgegrensd, instellinggebonden netwerk

Medium (opslag-)
Fysieke gegevensdrager

Netwerk
Een verzameling objecten voor communicatie tussen tenminste twee knooppunten van apparatuur en programmatuur, waarbij gebruik gemaakt wordt van voorgeschreven communicatieprotocollen

Netwerkadres (IP Adres)
Unieke identificatie van een element in een netwerk

Noodplan
Document waarin beschreven staat welke acties een organisatieonderdeel moet ondernemen in een noodsituatie

Ontruimingsplan
Document waarin beschreven staat op welke wijze een gebouw ontruimd moet worden in een noodsituatie

Personal Digital Assistant (PDA)
Kleine computer, formaat “binnenzak”

Privacybeheerder

Medewerker die adviseert over privacybescherming en activiteiten ter bescherming van persoonsgegevens en privacy coördineert

Proces
Een samenhangende serie activiteiten ten behoeve van een van tevoren bepaald doel

Procesverantwoordelijkheid / procesverantwoordelijke
Verantwoordelijkheid / verantwoordelijke voor het geheel van activiteiten van een bepaald proces

Programmatuur
Het geprogrammeerde deel van (informatie)systemen

Recovery
Herstel van een computerbestand of programmatuur

Risicoanalyse
Methode die informatie oplevert over de schadeverwachting van bepaalde gebeurtenissen

Service Level Agreement (SLA)
Schriftelijke overeenkomst tussen een aanbieder (service provider) en een afnemer (klant) van bepaalde diensten

Smartphone
Programmeerbare telefoon die voor vele uiteenlopende doeleinden gebruikt kan worden, zoals internet

Systeem
Een verzameling van één of meer samenhangende objecten met tezamen een gespecificeerde functionaliteit. Objecten kunnen zowel fysiek (computersysteem) als logisch (besturingssysteem) zijn

Systeemeigenaar
Verantwoordelijke voor een (informatie)systeem

Systeemprogrammatuur
Fundamentele, ondersteunende programmatuur die behoort tot de technische infrastructuur van een (informatie)systeem

Telewerken
Thuis of op een andere locatie werken op het netwerk van de organisatie met behulp van een externe lijnverbinding

Third Party Mededeling (TPM)
Verklaring van een onafhankelijke derde partij die door betrokken partijen vertrouwd wordt

Webapplicatie
Toepassingsprogrammatuur die via een internetbrowser benaderd kan worden

Wide Area Network (WAN)
Netwerk dat zich niet beperkt tot één fysieke locatie en waaraan meerdere lokale netwerken (LAN's) gekoppeld kunnen zijn.

BIJLAGE 1 Rollen en namen informatieveiligheidsorganisatie

Generieke rollen

Rol	Naam
Coördinator Informatieveiligheid	Peter Bruin
Controller Informatieveiligheid	Hielco Koeze
Beveiligingsbeheerder DigiD	Joop Beijaard
Beveiligingsbeheerder ICT	Peter Bruin (SSL gemeente Leeuwarden)

Specifieke rollen

Ameland

Rol	Naam
Beveiligingsbeheerder BRP en WD	Pedro Kooiker
Beveiligingsbeheerder BAG	Ronald Leijstra
Beveiligingsbeheerder SUWI	Jeroen Wijnberg
Beveiligingsbeheerder FZ	
Beveiligingsbeheerder DIV	Koos Molenaar
Beveiligingsbeheerder P&O	Jan Jaap Werkman
Privacy beheerder	

Schiermonnikoog

Rol	Naam
Beveiligingsbeheerder BRP en WD	Marty Cotie
Beveiligingsbeheerder BAG	Piet Huisman
Beveiligingsbeheerder SUWI	Gemeente Dantumadiel
Beveiligingsbeheerder FZ	Piet Huisman
Beveiligingsbeheerder DIV	Annie Kootstra
Beveiligingsbeheerder P&O	Grytske Klazema
Privacy beheerder	

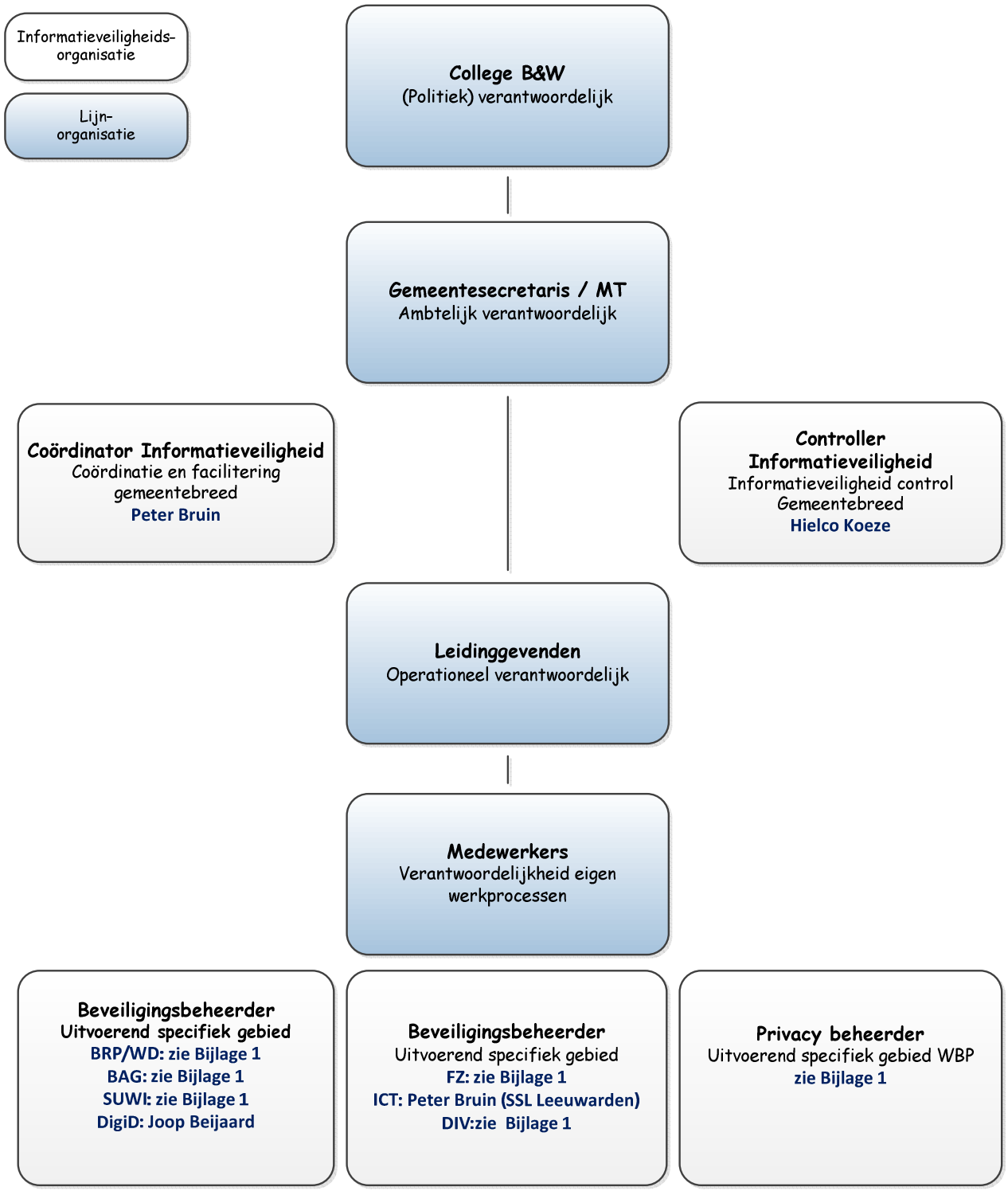
Terschelling

Rol	Naam
Beveiligingsbeheerder BRP en WD	Tanja Fischer
Beveiligingsbeheerder BAG	Jauk Hek
Beveiligingsbeheerder SUWI	Dienst SoZaWe
Beveiligingsbeheerder FZ	Remko Pals
Beveiligingsbeheerder DIV	Arend Roos
Beveiligingsbeheerder P&O	Mandy Rieks
Privacy beheerder	Edward Petersen

Vlieland

Rol	Naam
Beveiligingsbeheerder BRP en WD	Jan Smit
Beveiligingsbeheerder BAG	Marja Veerdig

Beveiligingsbeheerder SUWI	Dienst SoZaWe
Beveiligingsbeheerder FZ	André de Bie
Beveiligingsbeheerder DIV	Carin Winkelman
Beveiligingsbeheerder P&O	Uitbesteed aan gemeente Leeuwarden
Privacy beheerder	Lobke Buren


Informatieveiligheids-organisatie
Lijn-organisatie
College B&W
(Politiek) verantwoordelijk
Gemeentesecretaris / MT
Ambtelijk verantwoordelijk
Coördinator Informatieveiligheid
Coördinatie en facilitering gemeentebreed
Peter Bruin
Controller Informatieveiligheid
Informatieveiligheid control Gemeentebreed
Hielco Koeze
Leidinggevenden
Operationeel verantwoordelijk
Medewerkers
Verantwoordelijkheid eigen werkprocessen
Beveiligingsbeheerder
Uitvoerend specifiek gebied
BRP/WD: zie Bijlage 1
BAG: zie Bijlage 1
SUWI: zie Bijlage 1
DigiD: Joop Beijaard
Beveiligingsbeheerder
Uitvoerend specifiek gebied
FZ: zie Bijlage 1
ICT: Peter Bruin (SSL Leeuwarden)
DIV:zie Bijlage 1
Privacy beheerder
Uitvoerend specifiek gebied WBP
zie Bijlage 1

BIJLAGE 2 Conversietabel functies en teams

In zowel het Strategische als het Tactische gedeelte van het Informatieveiligheidsbeleid worden functies en afdelingen genoemd. Daar deze documenten gelden voor de vier gemeenten van De Waddeneilanden zit er verschil in de benamingen van deze afdelingen. In onderstaande tabel staat per benaming wat er per gemeente gelezen dient te worden.

Algemeen	**Ameland**	**Schiermonnikoog**	**Terschelling**	**Vlieland**
Managementteam	Directieteam	Managementteam	Directie	Teamleidersoverleg
Teamleider(s)	Coördinatoren	Teamleider(s)	Teamleider(s)	Teamleider(s)
Facilitaire Zaken	Gebouwbeheerder	Gebouwbeheerder	Gebouwbeheerder	Team Uitvoering & Ondersteuning
P&O	Team P&O	P&O-functionaris	Staf HRM	Team Beleid
Communicatie	Staf	Communicatie	Staf Communicatie	Team Beleid