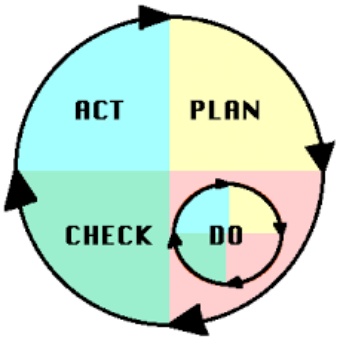
gemeente
TEYLINGEN

Informatiebeveiligingsbeleid
2016

Opsteller: Roza van Cappellen



Inhoud

1 Uitgangspunten informatiebeveiligingsbeleid van de gemeente Teylingen

Het belang van informatie(veiligheid)

Informatie is één van de voornaamste bedrijfsmiddelen van Teylingen. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging is het proces dat dit belang dient.

Visie

> De komende jaren zet de gemeente Teylingen in op het verhogen van informatieveiligheid en verdere professionalisering van de Informatie Beveiligings-functie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven.[1] Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Het proces van informatiebeveiliging is primair gericht op bescherming van gemeentelijke informatie, maar is tegelijkertijd een 'enabler'. Het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken. De focus is informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Het gaat ook niet alleen over ICT. Verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.[2]

Doelstelling

Dit informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen, zodat de gemeente voldoet aan relevante wet en regelgeving. Teylingen streeft er naar om 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn, dat er een SMART (Specifiek, Meetbaar, Acceptabel, Realistisch, Tijdsgebonden)-planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in de PDCA (Plan, Do, Check, Act)-cyclus.

Uitgangspunten

- Het informatiebeveiligingsbeleid van Teylingen is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.[3]
- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- Het beleid wordt vastgesteld door het college van B&W. Het management herijkt periodiek dit-beleid.

---

[1] *Met betrouwbaarheid wordt bedoeld: beschikbaarheid (continuïteit van de bedrijfsvoering), integriteit (juistheid, volledigheid) en vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.*

[2] Medewerker = (1) a*mbtenaar in de zin van het Ambtenarenreglement of (2) degene die op arbeidsovereenkomst of anderszins betaalde of niet-betaalde werkzaamheden voor een de gemeente Teylingen verricht.*

[3] Daarbij geldt het 'comply or explain' principe (pas toe of leg uit)

Risicobenadering

De aanpak van informatiebeveiliging in Teylingen is 'risk based'. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets op de BIG van VNG/KING (GAP-analyse). Indien een systeem meer maatregelen nodig heeft, wordt een risicoanalyse uitgevoerd. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beschermingseisen van de informatie. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces en wordt bepaald door de proceseigenaar: **risico = kans x impact**.

Doelgroepen

Het gemeentelijk informatiebeveiligingsbeleid is bedoeld voor alle in- en externe medewerkers van de gemeente.

Doelgroep	Relevantie voor informatiebeveiligingsbeleid
College van B&W	Integrale verantwoordelijkheid
Managementteam	Kaderstelling en implementatie
Afdelingshoofden/Teamcoördinatoren	Sturing op informatieveiligheid en controle op naleving
Allen	Gedrag en naleving
Gegevenseigenaren	Classificatie: bepalen van beschermingseisen van informatie
Beleidsmedewerkers	Planvorming binnen informatiebeveiligingskaders
Teamcoördinatoren	Dagelijkse coördinatie van informatiebeveiliging
Personeelszaken	Arbeidsvoorwaardelijke zaken
Facilitaire zaken	Fysieke toegangsbeveiliging
ICT- en applicatiebeheerders	ICT Technische beveiliging
Auditors en controller	Onafhankelijke toetsing
Leveranciers en ketenpartners	Compliance

Scope

- De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen (bijv. politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Zie hiervoor ook hoofdstuk 2.3.
- Dit gemeentelijke beleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen.[4]

Uitwerking

Na vaststelling van dit informatiebeveiligingsbeleid wordt de uitwerking van het beleid vastgelegd in het informatiebeveiligingsplan. Dit plan is de basis voor de PDCA-cylus (Plan Do Check Act). Beleid en uitvoering dienen steeds met elkaar in overeenstemming te blijven, zodat informatiebeveiliging een vast onderdeel in de organisatie blijft.

De te nemen maatregelen moeten worden afgestemd op de risico's, waarbij rekening dient te worden gehouden met technische mogelijkheden en de kosten van maatregelen. Dit is vaak situatie afhankelijk. Naarmate de gegevens een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico inhouden, dienen zwaardere eisen aan de beveiliging van die gegevens te worden gesteld. In het algemeen kan worden gesteld, dat indien met naar verhouding geringe extra kosten meer

[4] Bijvoorbeeld SUWI (Structuur Uitvoeringsorganisatie Werk en Inkomen) en gemeentelijke basisregistraties.

beveiliging kan worden bewerkstelligd dit als 'passend' kan worden beschouwd. Extra beveiliging is echter niet meer passend, indien de kosten voor het afzwakken van de risico's disproportioneel hoog zijn.[5] Kort gezegd: risico's en tegenmaatregelen dienen in balans te zijn.

Gebruik

Dit informatiebeveiligingsbeleid en het informatiebeveiligingsplan vervangen de losse (beleids)plannen die in het verleden werden gebruikt voor diverse audits en toetsingen op dit gebied. Per specifiek ondedeel, zoals bijvoorbeeld de BPR (Basisregistratie Personen) kan aanvullend beleid worden vastgesteld. Voor elke interne of externe audit worden het vastgestelde informatiebeveiligingsbeleid en het informatiebeveiligingsplan als basis genomen. Door de PDCA-cyclus wordt actualatisatie gewaarborgd.

Werking

Dit informatiebeveiligingsbeleid treedt in werking na vaststelling door college van B&W. Hiermee komt het oude informatiebeveiligingsbeleid van de gemeente Teylingen van 2014 te vervallen.

[5] Dit is uitgebreid beschreven in: 'Beveiliging van persoonsgegevens', CBP richtsnoeren, 2013.

2 Organisatie van de informatiebeveiliging

2.1 Interne organisatie

Risico's

Wanneer verantwoordelijkheden en bijbehorende activiteiten, procedures en instrumenten niet expliciet belegd worden, kan het daadwerkelijk en structureel uitvoeren en borgen van de beheersmaatregelen een probleem worden. Hierdoor kunnen belangen van burgers, bedrijven en (keten) partners geschaad worden.

Doelstelling

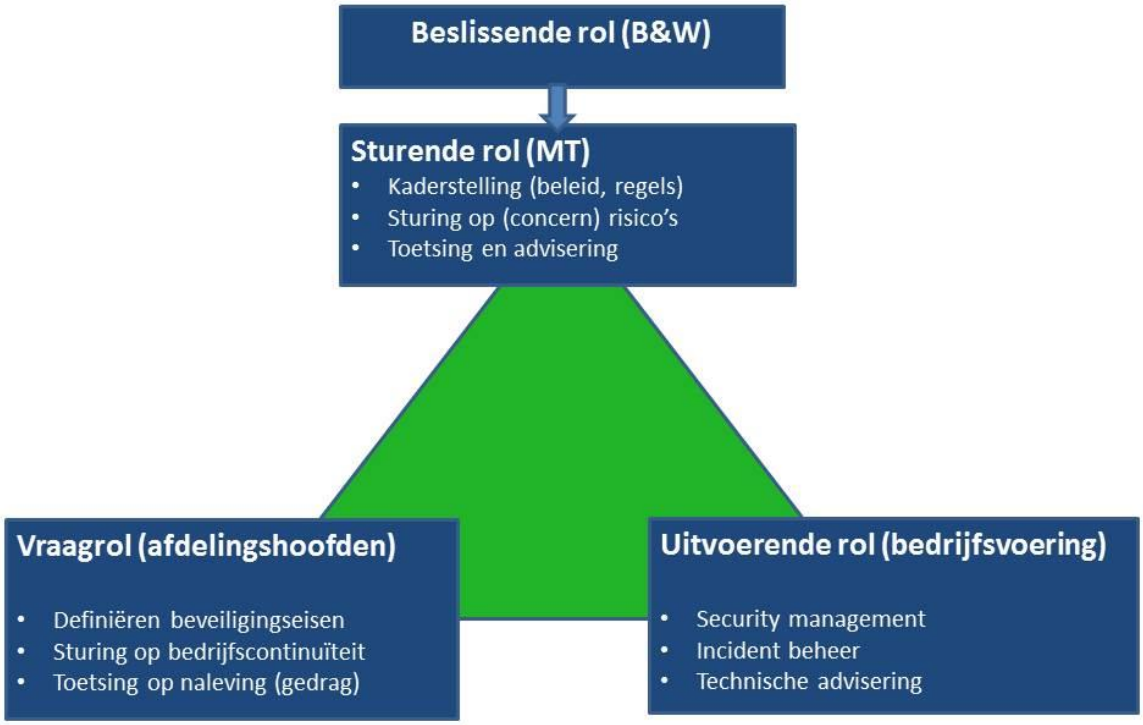
- *Beheren van de informatiebeveiliging binnen de organisatie.*
- *Vaststellen van het beheerkader om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.*
- *Goedkeuring door het management van het informatiebeveiligingsbeleid, de toewijzing van de rollen en de coördinatie en beoordeling van de implementatie van het beleid binnen de organisatie.*

Verantwoordelijkheden

- Het college van Burgemeester en Wethouders is integraal verantwoordelijk voor de beveiliging (beslissende rol) van informatie binnen de werkprocessen van Teylingen.[6]
  Het college:
  - stelt kaders voor informatiebeveiliging op basis van de actuele landelijke en Europese wet- en regelgeving en landelijke normenkaders;
- Het MT (in sturende rol) is verantwoordelijk voor kaderstelling en sturing.
  Het MT:[7]
  - stuurt op concern risico's;
  - controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
  - evalueert periodiek beleidskaders en stelt deze waar nodig bij.
- De afdelingen binnen de gemeente (in vragende rol) zijn verantwoordelijk voor de integrale beveiliging van hun organisatieonderdelen.[8]
  De afdelingshoofden:
  - stellen op basis van een expliciete risicoafweging betrouwbaarheidseisen voor de informatiesystemen vast (classificatie);
  - zijn verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
  - sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
  - rapporteren over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de managementrapportages.

[6] Zie ook: strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
[7] Met betrekking tot de i-functie geeft het afdelingshoofd Bedrijfsvoering op dagelijkse basis namens de directie invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan.
[8] Zie ook: strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten

- De afdeling Bedrijfsvoering (in uitvoerende rol) is verantwoordelijk voor uitvoering.[9]
  De afdeling Bedrijfsvoering:
  - is verantwoordelijk voor beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen, die voortvloeien uit betrouwbaarheidseisen (classificaties);
  - is verantwoordelijk voor alle beheeraspecten van informatiebeveiliging, zoals ICT security management, incident en problem management, facilitaire en personele zaken;
  - verzorgt logging, monitoring en rapportage;
  - levert klanten (technisch) beveiligingsadvies.
- Het team Personeelszaken (in uitvoerende rol) is verantwoordelijk voor de arbeidsvoorwaarden en personele zaken.



Figuur 1: relaties

2.2 Taken en rollen

- Het College van B&W stelt het informatiebeveiligingsbeleid vast. De uitvoering van het beleid moet gecontroleerd worden, zowel het College als de Raad (controle functie) kunnen opdracht geven om dit te (laten) controleren. Het MT adviseert B&W over het vast te stellen beleid.
- De teamcoördinator Informatisering en Automatisering (TC IA) geeft namens het MT op dagelijkse basis invulling aan de sturende rol door besluitvorming in het MT voor te bereiden en toe te zien op de uitvoering ervan. De informatiebeveiligingstaken die hieruit voortvloeien zijn belegd bij de 'Chief Information Security Officer' (CISO). De CISO bevordert en adviseert gevraagd en ongevraagd over informatiebeveiliging en rapporteert eens per half jaar concernbreed aan het MT over de stand van zaken.

[9] Let op, afdeling Bedrijfsvoering is tegelijk ook klant, het gaat hier echter om de uitvoerende rol.

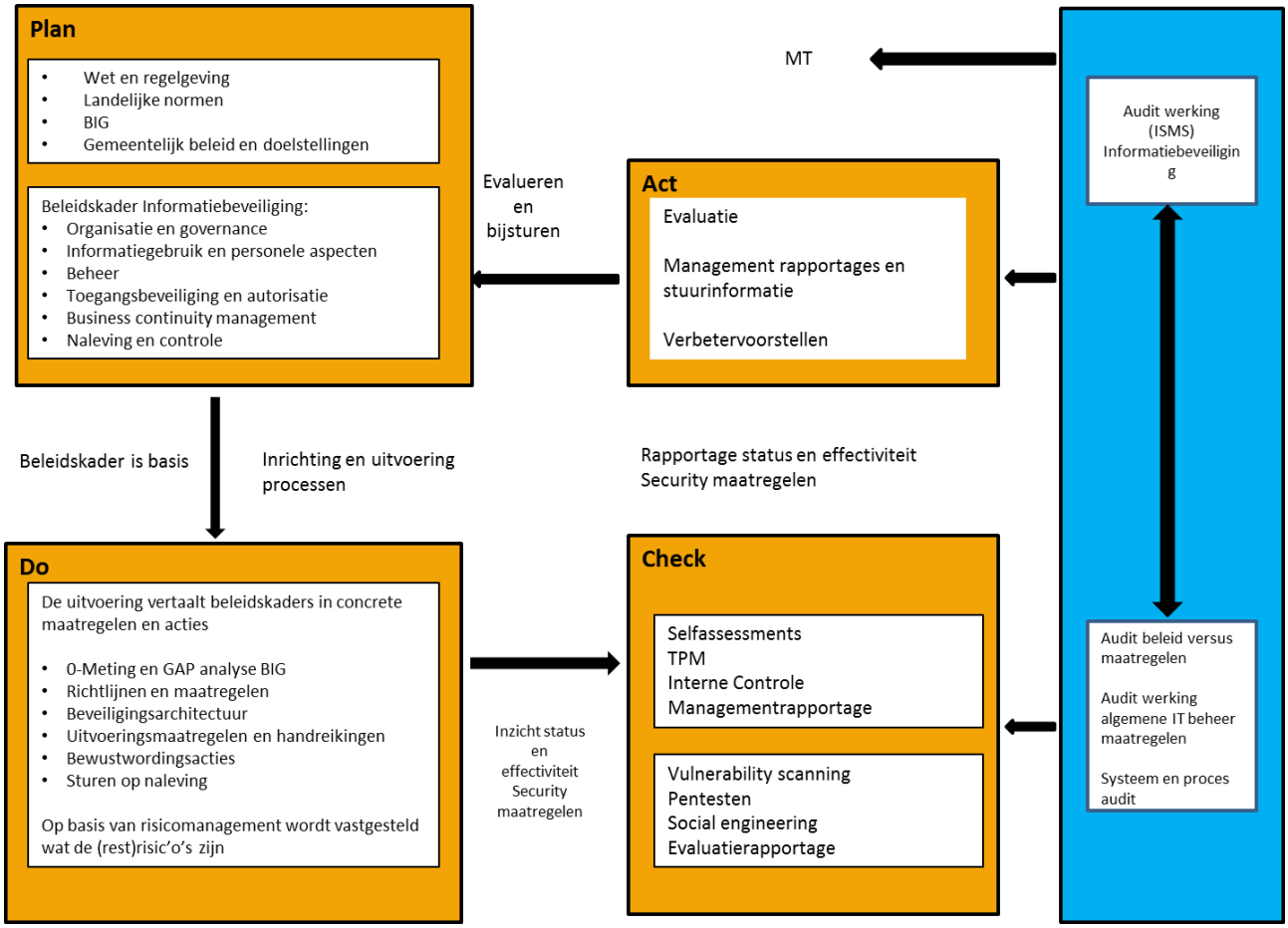
- De coördinatie van informatiebeveiliging is belegd bij een Security officer (CISO). Uitvoerende taken zijn zoveel mogelijk belegd bij de teamcoördinatoren. Zij rapporteren aan de CISO. Over het functioneren van informatiebeveiliging wordt jaarlijks gerapporteerd conform de P&C cyclus.
- De afdeling Bedrijfsvoering stelt een Security Functionaris (SF) aan voor dagelijks beheer van technische informatiebeveiligingsaspecten. De security functionaris rapporteert aan de CISO. Informatiebeveiliging is onderdeel van de service management rapportage.

Wie	Plan: Kaderstelling	Do: Uitvoering	Check: Controle	Act: Verbetering
Sturen: MT dagelijkse uitvoering: CISO	Ontwikkelen van kaders (beleid en architectuur); reglementen; meerjarenplanning.	Inbedding landelijke en EU-richtlijnen, advisering, handreikingen, crisisbeheersing en incident respons.	Controle, audit, pentesten.	Bijsturen: opdrachtverstrekking voor verbeteracties. Rapportage aan MT/ B&W
Vragen: Afdelingen	Formuleren van beveiligingseisen (classificatie) en opstellen clusterbeleid en beveiligingsplannen.	Stimuleren van beveiligingsbewustzijn bij medewerkers, risico- en bedrijfscontinuïteitmanagement.	Interne controle (IC), sturen op naleving van regels door medewerkers (gedrag), compliancy.	Verbeteren bedrijfscontinuïteit. Rapportage aan CISO/MT.
Uitvoeren: Bedrijfsvoering (in uitvoerende rol)	Beleidsvoorbereiding, technische onderzoeken (marktverkenningen).	Leveren van security management en services (ICT), incidentbeheer, logging, monitoring en advies.	Vulnerability scanning, evaluatie en rapportage.	Uitvoeren verbeteracties. Advies aan de CISO over aanpassingen aan de informatievoorziening.

PDCA

- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging.[10] Deze kwaliteitscyclus is in figuur 2 weergegeven.
- Toelichting figuur 2 (hieronder):
  - Plan: De cyclus start met het maken van een informatiebeveiligingsplan, gebaseerd het vastgestelde informatiebeveiligingsbeleid. Het informatiebeveiligingsplan werkt regels uit voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Het informatiebeveiligingsplan wordt jaarlijkse bijgesteld. De planning op hoofdlijnen is onderdeel van het ICT jaarplan.
  - Do: Het beleidskader is de basis voor risicomanagement, uitvoering van (technische) maatregelen en bevordering van beveiligingsbewustzijn. Uitvoering maakt integraal onderdeel uit van het dagelijkse werkproces.
  - Check: Control is onderdeel van het werkproces met als doel: waarborgen van de kwaliteit van informatie en ICT, en compliance aan wet- en regelgeving.
    Externe controle: betreft controle buiten het primaire proces door een externe auditor.[11] Dit heeft het karakter van een steekproef. Jaarlijks worden meerdere van dergelijke onderzoeken uitgevoerd, waarbij de CISO in principe opdrachtgever is. De externe auditor rapporteert aan de CISO en het MT.
  - Act: De cyclus is rond met de uitvoering van verbeteracties op basis van check en (externe) controle. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning en beveiligingsplannen.

[10] NEN/ISO 27001
[11] Van onder meer de accountant, rijksoverheid (voor bijv. basisregistraties) en gemeentelijke auditors (intern).



Figuur 2: Information Security Management System

2.3 Rapportage en escalatielijn voor informatiebeveiliging, externe partijen

De CISO stelt een organisatie voor van security gerelateerde functionarissen binnen de gemeente en de CISO organiseert tenminste eenmaal per halfjaar een (security) overleg. Het overleg heeft binnen de gemeente een adviesfunctie richting het MT en richt zich met name op beleid en adviseert over tactisch/strategische informatiebeveiliging kwesties.
Het onderwerp Informatiebeveiliging dient verder een vast onderdeel te zijn op de agenda van het Coördinatorenoverleg zodat er sturing plaatsvindt op de uitgevoerde activiteiten.

Rapportage en escalatielijn voor informatiebeveiliging

Security verantwoordelijke → CISO → MT[12]

Externe partijen

In een aantal gevallen zal de gemeente niet zelf taken uitvoeren, maar wel de regie voeren over de taken die namens de gemeente worden uitgevoerd door een externe partij. Daarbij blijft de gemeente verantwoordelijk het garanderen van de veiligheid van de informatie. Met name de veiligheid van persoonsgegevens moet gegarandeerd kunnen worden bij het uitbesteden van taken.

[12] De CISO is adviseur van het MT en rapporteert tegelijkertijd direct aan de wethouder.

- Informatiebeveiligingsbeleid, landelijke normen en wet- en regelgeving gelden ook voor externe partijen (leveranciers, ketenpartners) waarmee de gemeente samenwerkt (en informatie mee uitwisselt).[13] Ook voor externe partijen geldt hierbij het 'comply or explain' beginsel (pas toe of leg uit).
- Bij contractuele overeenkomsten gelden in beginsel altijd de Algemene Inkoop Voorwaarden (AIV) die zijn vastgesteld door de gemeente Teylingen of de Algemene Inkoop Voorwaarden van Stichting Rijk, waarin onder meer geheimhouding en aansprakelijkheid is geregeld. Afwijkingen op de AIV worden getoetst aan informatiebeveiligingsbeleid. Vereiste beveiligingsmaatregelen worden aanvullend vastgelegd in contracten en/of bewerkersovereenkomsten. Daarin is onder meer geborgd dat beveiligingsincidenten onmiddellijk worden gerapporteerd en dat de gemeente het recht heeft afspraken te (laten) controleren.[14]
  Voor ICT gerelateerde producten kunnen daarnaast de meest recent vastgestelde ARBIT voorwaarden van de Rijksoverheid of de specifieke ICT Voorwaarden van Stichting Rijk van toepassing worden verklaard.
- Voor het tot stand brengen van datakoppelingen met externe partijen, geldt naast generiek informatiebeveiligingsbeleid een gemeentelijke procedure 'Aanvragen externe toegang Internet'. Het doel van de procedure is risicobeheersing.
- Voor externe hosting van data en/of services gelden naast generiek informatiebeveiligingsbeleid de richtlijnen voor cloud computing.[15] De gemeente is gehouden aan:
  - regels omtrent grensoverschrijdend dataverkeer;
  - toezicht op naleving van regels door de externe partij(en);
  - hoogste beveiligingseisen voor bijzondere categorieën gegevens;[16]
  - melding bij college bescherming persoonsgegevens (CBP) bij doorgifte van persoonsgegevens naar derde landen (buiten de EU).

ICT crisisbeheersing en landelijke samenwerking

- Voor interne crisisbeheersing wordt een kernteam informatiebeveiliging geïnstalleerd, bestaande uit
  - CISO;
  - security functionaris ICT;
  - relevante applicatiebeheerders;
  - communicatie medewerkers;
  - P&O medewerkers.

  De werkwijze moet zijn vastgelegd.
- Gemeente Teylingen participeert in relevante landelijke platforms en onderhoudt contacten met andere sectoraal georganiseerde informatiebeveiligingsplatforms.

[13] Beleidsregels voor externe partijen zijn beschreven in de Baseline Informatiebeveiliging Nederlandse Gemeenten.
[14] Hiervoor kan gebruik worden gemaakt van een 'third party mededeling' (TPM) of een ISAE 3402-verklaring.
[15] Zie NCSC: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html
[16] *Ras of etnische afkomst, politieke opvattingen, religie of overtuiging, het lidmaatschap van een vakvereniging, genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen*

3 Beveiligingsonderdelen

3.1 Verantwoordelijkheid voor bedrijfsmiddelen

Risico's

- Bedrijfsmiddelen en informatie zijn blootgesteld aan risico's zoals diefstal, beschadiging of onoordeelkundig gebruik, waarbij niet voor alle ICT-configuratie items is vastgelegd wie de eigenaar/hoofdgebruiker is.
- Onduidelijkheid wie verantwoordelijk is voor gegevensbestanden, waardoor ook niemand verantwoordelijk is voor de beveiliging en kan optreden bij incidenten.

Doelstellingen

Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.

Voor alle bedrijfsmiddelen is de eigenaar vastgelegd alsook de verantwoordelijke voor het handhaven van de beheersmaatregelen.

3.2 Classificatie van informatie

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen t.a.v. processen en informatiesystemen worden beveiligingsclassificaties gebruikt.[17] Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt direct duidelijk welke maatregelen nodig zijn. Er wordt geclassificeerd op drie betrouwbaarheidsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid(BIV).

Er zijn vier beschermingsniveaus van geen naar hoog. De niveaus zijn in onderstaande tabel weergegeven. Tussen haakjes staan voorbeelden. Deze niveaus zijn bedacht om het proces van classificeren te vereenvoudigen.

[17] Dit is in detail beschreven in de component architectuur Informatiebeveiliging 2014, CIO, 2014.

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

Risico's

- Geen inzicht in welke componenten, zowel hardware als software, het belangrijkst zijn voor de primaire processen.
- Onjuiste classificatie draagt bij aan het onjuist beschermen van informatie en bedrijfsmiddelen met als risico, dat deze verloren kunnen gaan of openbaar worden gemaakt terwijl dat niet de bedoeling is.

Doelstellingen

Adequate niveaus van bescherming van informatie.

3.3 Beveiliging van personeel

Risico's

- Het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door externe medewerkers verdient extra aandacht, omdat menselijk falen en bedreigingen van menselijke aard significante invloed kunnen hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

Doelstellingen

Werknemers, ingehuurd personeel en externe gebruikers begrijpen hun verantwoordelijkheden en zijn geschikt voor de rol.

3.4 Fysieke beveiliging en beveiliging van de omgeving

Risico's

- Toegang tot kritieke systemen of waardevolle informatie. Bij het ontbreken van registratie zijn incidenten bovendien niet herleidbaar tot individuen.
- Niet-medewerkers krijgen toegang tot de panden.
- Toegang tot informatie die (bedrijfs)vertrouwelijk of geheim is.
- Verlies van, schade aan of diefstal van apparatuur.
- Schade door fysieke bedreigingen en gevaren van buitenaf.

Doelstellingen

Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie, bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.

Goed beschermde en beveiligde ICT-voorzieningen (met kritieke of gevoelige bedrijfsactiviteiten) tegen toegang door onbevoegden, schade en storingen.

Het voorkomen van verlies, schade of diefstal van apparatuur en bescherming tegen fysieke bedreigingen en gevaren van buitenaf.

3.5 Beveiliging van apparatuur en informatie

Risico's

- Het ontbreken van documentatie kan leiden tot fouten, niet-uniforme wijze van gegevensinvoer, of in geval de beheerder/bediener uitvalt, tot problemen rondom de continuïteit.
- Onjuiste autorisaties kunnen leiden tot foutieve handelingen, fraude en verduistering.
- Het niet uitvoeren en vastleggen van technische en functionele applicatietesten en/of de resultaten hiervan, kan in bepaalde omstandigheden (tijdsdruk, vakantieperiodes, etc.) leiden tot een verhoogd risico van uitval of gegevens verlies.
- De gemeente gaat steeds meer samenwerken (en informatie uitwisselen) in ketens en besteedt meer taken uit. Bij beheer van systemen en gegevens door een derde partij, kan ook informatie van de gemeente op straat komen te liggen. De gemeente blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.
- Programmatuur en ICT-voorzieningen zijn kwetsbaar voor virussen.
- Het ontbreken van een regeling voor antivirus bescherming bij medewerkers thuis leidt tot hogere beveiligingsrisico's.

Doelstellingen

Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.
Vastgestelde verantwoordelijkheden en procedures voor beheer en bediening van alle ICT-voorzieningen. Dit omvat tevens de ontwikkeling van geschikte bedieningsinstructies.

Toepassing, waar nodig, van functiescheiding om het risico van nalatigheid of opzettelijk misbruik te verminderen.

Risico's ten aanzien van externe partijen

De gemeente gaat steeds meer samenwerken en informatie uitwisselen in ketens en besteedt meer taken uit. Bij beheer van systemen en gegevens door een derde partij kan ook informatie van de gemeente op straat komen te liggen. De gemeente heeft hierbij een regiefunctie en blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.

Een passend niveau van informatiebeveiliging implementeren en bijhouden en dit vastleggen in een (bewerkers)overeenkomst, contracten en/of convenanten.

De organisatie controleert de implementatie van de maatregelen, die zijn vastgelegd overeenkomsten, bewaakt de naleving van de overeenkomsten en beheert wijzigingen om te waarborgen dat de beveiliging aan alle eisen voldoet, die met de derde partij zijn overeengekomen.

3.6 Logische toegangsbeveiliging

De identiteit van een gebruiker die toegang krijgt tot gemeentelijke informatie dient te worden vastgesteld.[18] Logische toegang is gebaseerd op de classificatie van de informatie.

Risico's

- Wanneer toegangsbeheersing niet expliciet gebaseerd is op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en/of een aanvullende risicoanalyse, is niet duidelijk of het juiste niveau van beveiliging wordt gehanteerd.
- Verstoringen door onjuist gebruik van ICT-ruimtes of ICT-componenten (m.n. waar ook niet ICT-teams toegang hebben).

Doelstellingen

Beheersen van de toegang tot informatie, ICT-voorzieningen en bedrijfsprocessen op grond van bedrijfsbehoeften en beveiligingseisen.

[18] Een gebruiker kan een medewerker, leverancier, burger, bedrijf, samenwerkingspartner of applicatie zijn.

3.7 Beveiligingsincidenten

Risico's

- Als incidenten niet geregistreerd worden, is niet duidelijk waar en wanneer er zich incidenten voor doen of voor hebben gedaan. Op deze wijze kan er geen lering worden getrokken uit deze incidenten om deze in de toekomst te voorkomen of om preventief betere maatregelen te implementeren.

Doelstellingen

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

3.8 Bedrijfscontinuïteit

Risico's

- Wanneer er niet of nauwelijks invulling gegeven wordt aan de continuïteitsplanning is er naast een vals gevoel van veiligheid, ook grote kans op ad hoc maatregelen als een calamiteit zich voordoet.
- Het uitvallen van medewerkers (ziekte, sterven, ontslag) kan een reële bedreiging zijn.

Doelstellingen

- *Onderbreken van bedrijfsactiviteiten tegengaan.*
- *Beschermen kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen.*
- *Tijdig herstel van activiteiten en informatie bewerkstelligen.*

3.9 Naleving

De vastgestelde procedures, contracten en afspraken moeten nageleefd worden. Er moet aantoonbaar gewerkt worden volgens het vastgestelde kader en de geldende wet- en regelgeving.

Risico's

- Het afgesproken kader wordt een papieren tijger.
- Afspraken en uitvoering komen niet elkaar overeen, processen worden niet gevolgd.
- Niet naleven van wettelijke eisen, waardoor burgers, bedrijven en ketenpartners schade kunnen oplopen.

Doelstellingen

Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen of van beveiligingseisen.

Organisatorische aspecten

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 elke afdeling stuurt. De kwaliteit wordt gemeten aan:

- de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;
- efficiency en effectiviteit van de geïmplementeerde maatregelen;
- de mate waarin de informatiebeveiliging het bereiken van de strategische doelstellingen ondersteunt.

De CISO zorgt namens het MT voor het toezicht op de uitvoering van het informatiebeveiligingsbeleid.

(Wettelijke) kaders

Een overzicht van relevante wet en regelgeving is te vinden bij KING.[19] Zo is het gebruik van persoonsgegevens bijvoorbeeld geregeld in de Wet Bescherming Persoonsgegevens, maar hebben ook de (europese) Privacy verordening en de Wet meldplicht Datalekken daar invloed op.[20]

[19] Een concept overzicht van wetten, regelingen en andere kaders is beschikbaar op de website van KING.
[20] Zie ook: CBP richtsnoeren

4 Relevante documenten en bronnen

4.1 Intern

- Algemene Inkoop Voorwaarden gemeente Teylingen
- ICT Voorwaarden Stichting Rijk
- Arbit voorwaarden
- Bewerkersovereenkomst gemeente Teylingen / Stichting Rijk 2015

4.2 Extern

- NEN/ISO 27001 (2005) en 27002 (Code voor Informatiebeveiliging) (2007)
- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), KING, 2013
- Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- Tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- CBP richtsnoeren 'beveiliging van persoonsgegevens', 2013: http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx
- GEMMA: https://www.kinggemeenten.nl/secties/gemma/gemma