SharedServiceCenter Zuid-Limburg

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 558
16 april
2018

Officiële uitgave van de gemeenschappelijke regeling Shared Service Center Zuid-Limburg

Informatiebeveiligingsbeleid SSC-ZL

Het Bestuur van het Shared Service Center Zuid-Limburg

OVERWEGING
gelet op het bepaalde in Informatiebeleid SSC-ZL;
mede gelet op het bepaalde in artikel 10, tweede en derde lid, van de Grondwet;
mede gelet op het bepaalde in hoofdstuk 2 en in het bijzonder in artikel 13 van de Wet Bescherming Persoonsgegevens;
mede gelet op het bepaalde in artikel 1.4.1 en het bepaalde in hoofdstuk 15 van de CAR-UWO;
mede gelet op het bepaalde in het wetboek van Strafrecht (Sr) en het wetboek van Strafvordering (Sv) over computercriminaliteit;
mede gelet op de Archiefwet;
mede gelet op Code voor Informatiebeveiliging (ISO 27001:2005 en ISO 27002:2007);
mede gelet de Richtlijn voor Cloudcomputing en de ICT-Beveiligingsrichtlijnen voor Webapplicaties, beiden van het Nationaal Cyber Security Centrum (NCSC);
mede gelet op dat vergelijkbaar beleid ook reeds van toepassing is bij de moederorganisaties, zijnde de gemeente Heerlen, de gemeente Maastricht en de gemeente Sittard-Geleen;

BESLUIT
vast te stellen het navolgende beleid: Informatiebeveiligingsbeleid SSC-ZL

Hoofdstuk 1 Algemeen

Artikel 1 Beleidsinhoud
Dit document bevat beleidsuitgangspunten op het gebied van informatieveiligheid en de organisatie van informatieveiligheid waarbij de rollen en verantwoordelijkheden aangaande informatieveiligheid en het verantwoordingsmechanisme staan beschreven.

Artikel 2 Inwerkingtreding
Dit beleid treedt in werking na Publicatie in het Blad Gemeenschappelijke Regeling Shared Service Center Zuid-Limburg.

Artikel 3 Voorwoord
In dit document is het informatiebeveiligingsbeleid beschreven van het SSC-ZL. Dit beleid is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING) dat gebaseerd is de internationale standaarden voor informatieveiligheid: NEN/ISO 27001 en NEN/ISO 27002. Tijdens het buitengewone VNG ledencongres op 29 november 2013, is de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen. Hierin is opgenomen dat de Nederlandse gemeenten de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt nemen om de informatiebeveiliging binnen de gemeentelijke organisaties te waarborgen. Als gemeenschappelijke regeling voor gemeenten sluiten wij hierop aan.
Het 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 dat alle medewerkers 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 (BIG - VNG/IBD). Daarnaast heeft in samenwerking met deskundigen van de gemeenten Heerlen, Maastricht en Sittard-Geleen op een aantal punten aanscherping plaatsgevonden. Daarbij zijn specifieke inzichten en accenten samengebracht in dit document.

Artikel 4 Leeswijzer en ambitieniveau
Dit document bevat beleidsuitgangspunten op het gebied van informatieveiligheid en de organisatie van informatieveiligheid waarbij de rollen en verantwoordelijkheden aangaande informatieveiligheid en het verantwoordingsmechanisme staan beschreven. Dit document dient ook als kapstok voor de verdere inbedding van het informatiebeveiligingsbeleid, de standaarden, de procedures en de processen.
In dit document is op basis van de Baseline Informatiebeveiliging Gemeenten (BIG) het inhoudelijke normenkader beschreven. Hierin zijn alle normen en maatregelen vanuit de BIG verder uitgewerkt, die leidend zijn voor alle organisatieonderdelen van het SSC-ZL.
Met dit document wordt daarnaast bepaald dat het SSC-ZL bij voorkomende keuzes en vraagstukken ten aanzien van de veiligheid van informatieprocessen de beleidsregels in dit document als uitgangspunt

hanteert. Dit document geeft het uiteindelijke ambitieniveau weer, en met behulp van periodieke quick scans wordt telkens de huidige situatie weergegeven ten opzichte van het ambitieniveau. De verschillen worden uitgewerkt in een informatiebeveiligingsplan waarin acties worden uitgewerkt.

Artikel 5 Inleiding

In dit document is een aanzienlijk aantal beleidsuitgangspunten nader uitgewerkt en zijn beveiligingseisen en -maatregelen opgenomen, die voor alle processen en systemen gelden. Onderdeel van dit document is een beheerstructuur voor informatiebeveiliging, waarmee verantwoordelijkheden voor informatiebeveiliging worden belegd en informatiebeveiliging wordt ingebed in de reguliere planning- en controlcyclus binnen de (kwaliteitshandhaving van de) bedrijfsvoeringsprocessen van het SSC-ZL. De toegepaste hoofdstukken uit de Strategische variant van de Baseline Informatiebeveiliging voor Gemeenten (hierna BIG) zijn:

1. Hoofdstuk 1 Uitgangspunten informatiebeveiliging;
2. Hoofdstuk 2 Organisatie van informatiebeveiliging;
3. Hoofdstuk 3 Beheer van bedrijfsmiddelen;
4. Hoofdstuk 4 Beveiliging van personeel;
5. Hoofdstuk 5 Fysieke beveiliging en beveiliging van de omgeving;
6. Hoofdstuk 6 Beveiliging van apparatuur en informatie;
7. Hoofdstuk 7 Logische toegangsbeveiliging;
8. Hooofdstuk 8 Beveiligingsincidenten;
9. Hoofdstuk 9 Bedrijfscontinuïteit;
10. Hoofdstuk 10 Naleving.

Artikel 6 Algemene oriëntatie en positionering van informatiebeveiliging

Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. Het begrip 'informatiebeveiliging' heeft betrekking op:

1. beschikbaarheid/continuïteit: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
2. exclusiviteit/vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
3. integriteit/betrouwbaarheid: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Artikel 7 Waarom informatiebeveiliging?

Informatie is één van de belangrijkste bedrijfsmiddelen van een organisatie. Toegankelijke en betrouwbare informatie is essentieel voor de organisatie, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan de deelnemers en klanten en die met minimale middelen maximale resultaten behaalt. De bescherming van waardevolle informatie is hetgeen waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen getroffen moeten worden.

Artikel 8 Reikwijdte en afbakening informatiebeveiliging

Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm et cetera) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekort schietende organisatie. Voorbeelden van informatiebeveiligingsmaatregelen zijn: clean desk policy, hoe om te gaan met mobiele devices en aanwijzingen voor telewerken.

Artikel 9 Definities

In dit Informatiebeveiligingsbeleid SSC-ZL wordt verstaan onder:

1. Betrouwbaarheid: beschikbaarheid (continuïteit van de bedrijfsvoering), integriteit (juistheid, volledigheid), en vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.
2. Beveiligingslek: als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek.
3. Beveiligingsincident: bijvoorbeeld het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker.
4. CIO: Chief Information Officer, geeft namens de directie op dagelijkse basis invulling aan de sturende rol door besluitvorming voor te bereiden en toe te zien op de uitvoering ervan.

5. CISO: Chief Information Security Officer, bevorderd en adviseert gevraagd en ongevraagd over informatiebeveiliging en rapporteert eens per kwartaal concernbreed aan het SIO over de stand van zaken. Ook is de CISO verantwoordelijk voor het actueel houden van het informatiebeveiligingsbeleid.
6. Datalek: er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan, en er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunt uitsluiten.
7. ENSIA: staat voor Eenduidige Normatiek Single Informatie Audit. ENSIA helpt gemeenten om in één keer slim verantwoording af te leggen over informatieveiligheid.
8. Gebruiker: een gebruiker kan een medewerker, leverancier, burger, bedrijf, samenwerkingspartner of applicatie zijn.
9. Medewerker: (1) ambtenaar in de zin van het Ambtenarenreglement of (2) degene die op arbeidsovereenkomst of anderszins betaalde of niet-betaalde werkzaamheden voor het SSC-ZL verricht
10. Mobile code: software die wordt uitgevoerd zonder expliciete toestemming van de gebruiker, zoals scripts (Java), Java applets, ActiveX controls en Flash animaties. Dergelijke software wordt gebruikt voor functies binnen (web)applicaties.
11 OWASP: het Open Web Application Security Project (OWASP) is een wereldwijde charitatieve not-profitorganisatie met als doel de beveiliging van applicatiesoftware te verbeteren. Hun missie is om applicatiebeveiliging zichtbaar te maken, zodat mensen en organisaties een weloverwogen beslissingen kunnen nemen over de veiligheidsrisico's met betrekking tot applicaties.
12 SIO: Strategisch Informatie Overleg, overleg waarin bewaakt wordt de ketengerichte belangenafweging in de informatiehuishouding. Deelnemers aan het SIO zijn minimaal de CIO, de CISO, en een vertegenwoordiger van de lijnafdelingen.

Hoofdstuk 2 Uitgangspunten informatiebeveiliging

Artikel 10 Samenhang
Deze hoofdstukken vormen een onlosmakelijk geheel met het informatiebeveiligingsbeleid van het SSC-ZL. Deze hoofdstukken corresponderen met de hoofdstukken 5 tot en met 15 uit de Tactische variant van de BIG. Ze geven een nadere invulling van het informatiebeveiligingsbeleid.

Artikel 11 Het belang van informatie(veiligheid)
Informatie is één van de voornaamste bedrijfsmiddelen van het SSC-ZL. 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 de deelnemers in het SSC-ZL en daardoor voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging (IB) is het proces dat dit belang dient.

Artikel 12 Visie
De komende jaren zet het SSC-ZL in op het verhogen van informatieveiligheid en verdere professionalisering van de IB-functie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de organisatie en de basis voor het beschermen in de hoedanigheid van hostingspartij en verwerker, van de informatiesystemen en gegevens van de deelnemers en overige klanten.Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.
Het proces van informatiebeveiliging is primair gericht op bescherming van 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 alle medewerkers is essentieel voor informatieveiligheid.

Artikel 13 Doelstelling
Dit informatiebeveiligingsbeleid (IB-beleid) is het kader voor passende technische en organisatorische maatregelen om informatie te beschermen en te waarborgen, dat het SSC-ZL voldoet aan relevante wet en regelgeving. Het SSC-ZL streeft er naar om 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat het SSC-ZL weet welke maatregelen genomen zijn en dat er een SMART-planning is van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in de eigen PDCA-cyclus.

Artikel 14 Uitgangspunten

1. Het informatiebeveiligingsbeleid van SSC-ZL is in lijn met het algemene beleid van de organisatie en de relevante landelijke en Europese wet- en regelgeving. Daarbij geldt het 'comply or explain' principe (pas toe of leg uit).
2. Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
3. Het IB-beleid wordt vastgesteld door het Bestuur van de Gemeenschappelijke Regeling SSC-ZL. De Directie herijkt periodiek het IB-beleid.

Artikel 15 Risicobenadering

De aanpak van informatiebeveiliging (IB-beleid) in het SSC-ZL is 'risk based'. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets tegen de Baseline Informatiebeveiliging Nederlandse Gemeenten (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.

Artikel 16 Doelgroepen

Het IB-beleid is bedoeld voor alle in- en externe medewerkers van het SSC-ZL:

1. Bestuur: Integrale verantwoordelijkheid
2. Directie: Kaderstelling en implementatie
3. Lijnmanagement (proceseigenaren): Sturing op informatieveiligheid en controle op naleving
4. Medewerkers: Gedrag en naleving
5. Gegevenseigenaren: Classificatie, bepalen van beschermingseisen van informatie
6. Beleidsmakers: Planvorming binnen IB-kaders
7. IB-functionarissen: Dagelijkse coördinatie van IB
8. Personeelszaken: Arbeidsvoorwaardelijke zaken
9. Facilitaire zaken: Fysieke toegangsbeveiliging
10. ICT-diensten (en –ontwikkelaars): Technische beveiliging
11 Auditors: Onafhankelijke toetsing
12 Leveranciers en ketenpartners: Compliance

Artikel 17 Scope

1. De scope van dit beveiligingsbeleid omvat alle SSC-ZL processen, onderliggende informatiesystemen, informatie en gegevens van de deelnemende organisaties 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.
2. Dit IB-beleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen. Bijvoorbeeld SUWI (Structuur Uitvoeringsorganisatie Werk en Inkomen) en gemeentelijke basisregistraties.

Artikel 18 IB-beleid en architectuur

IB is onderdeel van de informatiearchitectuur en uitgewerkt in de IB-architectuur. Deze architectuur beschrijft onder meer principes, richtlijnen en maatregelen o.b.v. verschillende beschermingsniveaus (classificatie). De processen van informatiebeveiliging worden onderdeel van de volgende GEMMA versie om daarmee de basis voor informatieveiligheid te verankeren als integraal onderdeel van de bedrijfsvoering.

Hoofdstuk 3 Organisatie van de informatiebeveiliging

Paragraaf 3.1 Interne organisatie

Artikel 19 Risico's

Het niet expliciet beleggen van verantwoordelijkheden en bijbehorende activiteiten, procedures en instrumenten, verhindert het daadwerkelijk en structureel uitvoeren en borgen van de beheersmaatregelen.

Artikel 20 Doelstelling

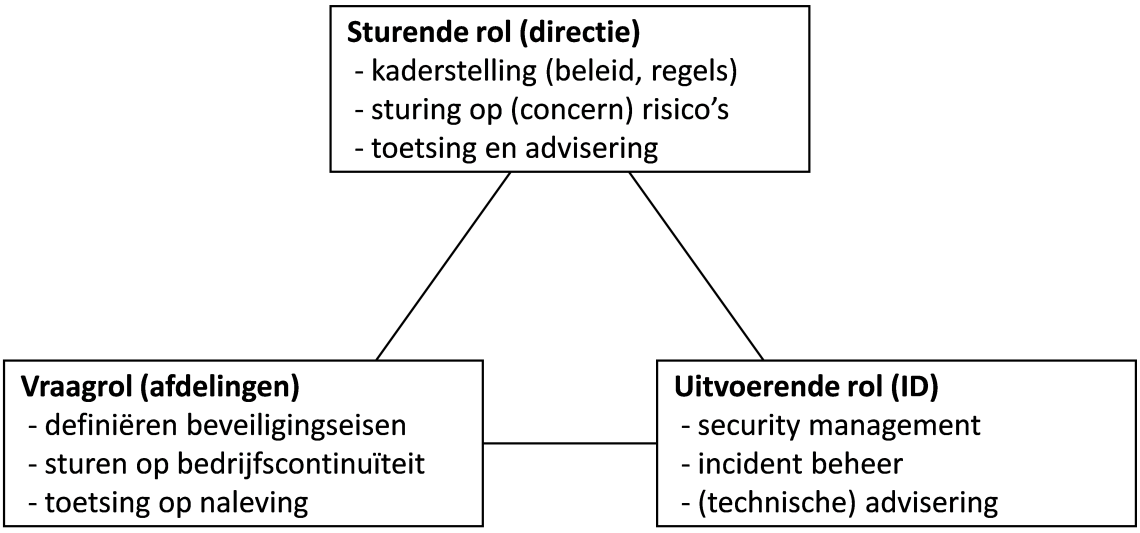
1. Beheren van de informatiebeveiliging (IB) binnen de organisatie.

2. Er is een beheerkader vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.
3. Goedkeuring door de directie van het informatiebeveiligingsbeleid, de toewijzing van de rollen en de coördinatie en beoordeling van de implementatie van het beleid binnen de organisatie.

Artikel 21 Verantwoordelijkheden

1. Het Bestuur van de Gemeenschappelijke Regeling SSC-ZL is integraal verantwoordelijk voor de beveiliging (beslissende rol) van informatie binnen de werkprocessen van het SSC-ZL;
1a. stelt kaders voor informatiebeveiliging (IB) op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders;
2. De directie (in sturende rol) is verantwoordelijk voor kaderstelling en sturing. Met betrekking tot de i-functie geeft de CIO 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. De directie:
2.a. stuurt op concern risico's;
2.b. controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
2.c. evalueert periodiek beleidskaders en stelt deze waar nodig bij;
2.d. stelt op basis van een expliciete risicoafweging betrouwbaarheidseisen voor zijn informatiesystemen vast (classificatie).
3. De afdelingen binnen het SSC-ZL (in hun vragende rol) zijn verantwoordelijk voor de integrale beveiliging van hun organisatieonderdelen. De lijnmanager:
3.a. is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
3.b. stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
3.c rapporteert over compliance aan wet- en regelgeving en algemeen beleid van het SSC-ZL in de managementrapportages.
4. De Service Organisatie (nu PSA, ID en Inkoop, maar ook de eigen interne bedrijfsvoering en ook interne HRM, telkens in uitvoerende rol) is verantwoordelijk voor uitvoering. Let op, de serviceorganisatie, stafdienst, afdeling bedrijfsvoering is tegelijk ook klant, het gaat hier echter om de uitvoerende rol. De Service Organisatie:
4.a. is verantwoordelijk voor beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen, die voortvloeien uit betrouwbaarheidseisen (classificaties);
4.b. is verantwoordelijk voor alle beheeraspecten van informatiebeveiliging, zoals ICT security management, incident en problem management, facilitaire en personele zaken;
4.c. verzorgt logging, monitoring en rapportage;
4.d. levert klanten (technisch) beveiligingsadvies.

Gezien de bijzondere constructie van het SSC-ZL vervullen sommige organisatieonderdelen een dubbele rol: enerzijds vervullen zij als lijnafdeling de vraagrol, maar anderzijds vervullen zij gelijktijdig de uitvoerende rol.



Artikel 22 Taken en rollen

1. Het Bestuur van de Gemeenschappelijke Regeling SSC-ZL stelt formeel het IB-beleid vast. De uitvoering van het beleid moet gecontroleerd worden door het bestuur van de Gemeenschappelijke Regeling SSC-ZL. De directie adviseert over het vast te stellen beleid.
2. De CIO (Chief Information Officer) of vergelijkbare rol geeft namens de directie op dagelijkse basis invulling aan de sturende rol door besluitvorming voor te bereiden en toe te zien op de uitvoering ervan. De IB taken die hieruit voortvloeien zijn belegd bij de 'Chief Information Security Officer' (CISO). De CISO bevordert en adviseert gevraagd en ongevraagd over IB en rapporteert eens per kwartaal concernbreed aan het Strategisch Informatie Overleg (SIO) over de stand van zaken. Ook is de CISO verantwoordelijk voor het actueel houden van het informatiebeveiligingsbeleid.
3. Het Strategisch informatieoverleg (SIO) bewaakt de ketengerichte belangenafweging in de informatiehuishouding. Deelnemers aan het SIO zijn minimaal de CIO, de CISO en een vertegenwoordiging van de lijnafdelingen.
4. Sturende rol (directie)-kaderstelling (beleid, regels)-sturing op (concern) risico's-toetsing en adviseringUitvoerende rol (ID)-security management-incident beheer-(technische) adviseringVraagrol (afdelingen)-definiëren beveiligingseisen-sturen op bedrijfscontinuïteit-toetsing op naleving
5. De coördinatie van informatiebeveiliging is belegd bij de CISO. Uitvoerende taken zijn zoveel mogelijk belegd bij (decentrale) i-security functionarissen. De afdelingen rapporteren aan de CISO. Over het functioneren van informatiebeveiliging wordt jaarlijks gerapporteerd conform de P&C cyclus en door het afgeven van een BIG compliant TPM verklaring aan de deelnemers en overige klanten ten behoeve van hun ENSIA audit.
6. De service organisatie (met name ICT) heeft een security functionaris aangesteld voor dagelijks beheer van technische IB-aspecten. 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: Directie **Dagelijkse uitvoering:** CIO / CISO	Ontwikkelen van kaders (beleid en architectuur); regelementen; meerjarenplanning	Inbedding landelijke en EU-richtlijnen, advisering, handreikingen, crisisbeheersing en incident respons	Contole, audit, pentesten	Bijsturen: opdrachtverstrekking voor verbeteracties. Rapportage aan directie en bestuur
Vragen: alle afdelingen	Formuleren van beveiligingseisen (classificatie) en opstellen afdelingsbeleid 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 SIO (CIO/CISO)
Uitvoeren: Service Organisatie (in uitvoerende rol)	Beleidsvoorbereiding, technische onderzoeken (marktverkenning)	Leveren van security management en services (ICT), incidentbeheer, logging, monitoring en advies	Vulnerability scanning, evaluatie en rapportage	Uitvoeren verbeteracties. Advies aan het SIO (CIO/CISO) over aanpassingen in de informatie-voorziening

Artikel 23 Functioneel overleg informatieveiligheid

1. De CISO van het SSC-ZL stelt een organisatie voor van security gerelateerde functionarissen binnen het SSC-ZL en de CISO organiseert tenminste eenmaal per kwartaal een (security) overleg met dit gremium. De CISO is voorzitter. Het overleg heeft binnen het SSC-ZL een adviesfunctie richting het SIO en richt zich met name op beleid en adviseert over tactisch/strategische informatiebeveiliging kwesties.
2. Het onderwerp Informatiebeveiliging dient verder een vast onderdeel te zijn op de agenda van het MT-overleg en alle afdelingsoverleggen zodat er sturing plaatsvindt op de uitgevoerde activiteiten.

Artikel 24 Rapportage en escalatielijn voor IB

(Decentrale) Security verantwoordelijk -> CISO -> CIO -> Directeur/Bestuur

Paragraaf 3.2 Externe partijen

Artikel 25

1. IB-beleid, landelijke normen en wet en regelgeving gelden ook voor externe partijen (leveranciers, ketenpartners) waarmee het SSC-ZL samenwerkt (en informatie mee uitwisselt). Ook voor externe partijen geldt hierbij het 'comply or explain' beginsel (pas toe of leg uit).

2. Bij contractuele overeenkomsten gelden in beginsel altijd de Algemene Inkoop Voorwaarden (AIV), waarin onder meer geheimhouding en aansprakelijkheid is geregeld. We streven ernaar om de GIBIT van toepassing te laten verklaren op ICT-aanbestedingen. Afwijkingen op de AIV dienen te worden getoetst aan IB-beleid. Vereiste beveiligingsmaatregelen worden aanvullend vastgelegd in contracten en/of bewerkersovereenkomsten. Daarin is onder meer geborgd dat beveiligingsincidenten onmiddellijk worden gerapporteerd en dat het SSC-ZL het recht heeft afspraken te (laten) controleren.
3. Voor het tot stand brengen van datakoppelingen met externe partijen, geldt naast generiek IB-beleid een procedure 'Aansluitvoorwaarden derde partijen. Het doel van de procedure is risicobeheersing.
4. Voor externe hosting van data en/of services gelden naast generiek IB-beleid de richtlijnen voor cloud computing. Het SSC-ZL is gehouden aan:

4.a regels omtrent grensoverschrijdend dataverkeer;
4.b toezicht op naleving van regels door de externe partij(en);
4.c hoogste beveiligingseisen voor bijzondere categorieën gegevens (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);
4.d melding bij Autoriteit Persoonsgegevens (AP) bij doorgifte van persoonsgegevens naar derde landen (buiten de EU).

Artikel 26 Bijzondere externe partijen: GR-deelnemers

Deze paragraaf dient ter verduidelijking van de verantwoordelijkheid die de deelnemende organisaties in het totaal van informatiebeveiliging hebben. De deelnemende organisaties hebben besloten om (delen van) de ontwikkeling, exploitatie of het onderhoud van systemen uit te besteden aan het SSC-ZL. In al deze gevallen blijven de deelnemende organisaties verantwoordelijk voor de beveiliging van het individuele systeem. De deelnemende organisaties communiceren de betrouwbaarheidseisen van het systeem die zij op basis van het eigen beleid en expliciete risicoafweging stellen aan het SSC-ZL c.q. andere derde partijen. Het SSC-ZL treedt ook op als hostingpartij en bewerker voor de deelnemende organisaties.
In het kader van de relatie van de deelnemende organisaties met het SSC-ZL zijn met name de volgende punten van belang:

1. Harmonisatie van informatiebeveiligingsbeleid en –uitvoering, en auditing: gezien de onderlinge afhankelijkheden die ontstaan door de samenwerking via het SSC-ZL streven alle partijen zo veel mogelijk naar een gelijkluidend informatiebeveiligingsbeleid, gebaseerd op wet- en regelgeving, landelijke normen zoals de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en 'best practices', uitgewerkt in regels voor onder informatiegebruik, bedrijfscontinuïteit, en naleving.
2. Samenwerking rondom de informatiebeveiligingsfunctie: voor het bewaken van de informatieveiligheid en de daarmee samenhangende doelstellingen van iedere deelnemende organisaties is het van belang dat er een eenduidige gemeenschappelijke Governance-structuur bestaat rondom informatiebeveiliging. Er dient een duidelijk en aantoonbaar proces te worden afgesproken over de wijze waarop alle activiteiten gericht op het naleven van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) georganiseerd en gemanaged worden. Daartoe wordt een platform geboden waar zij gezamenlijk in gesprek kunnen treden volgens een vast stramien. Dit platform wordt als volgt vorm gegeven:

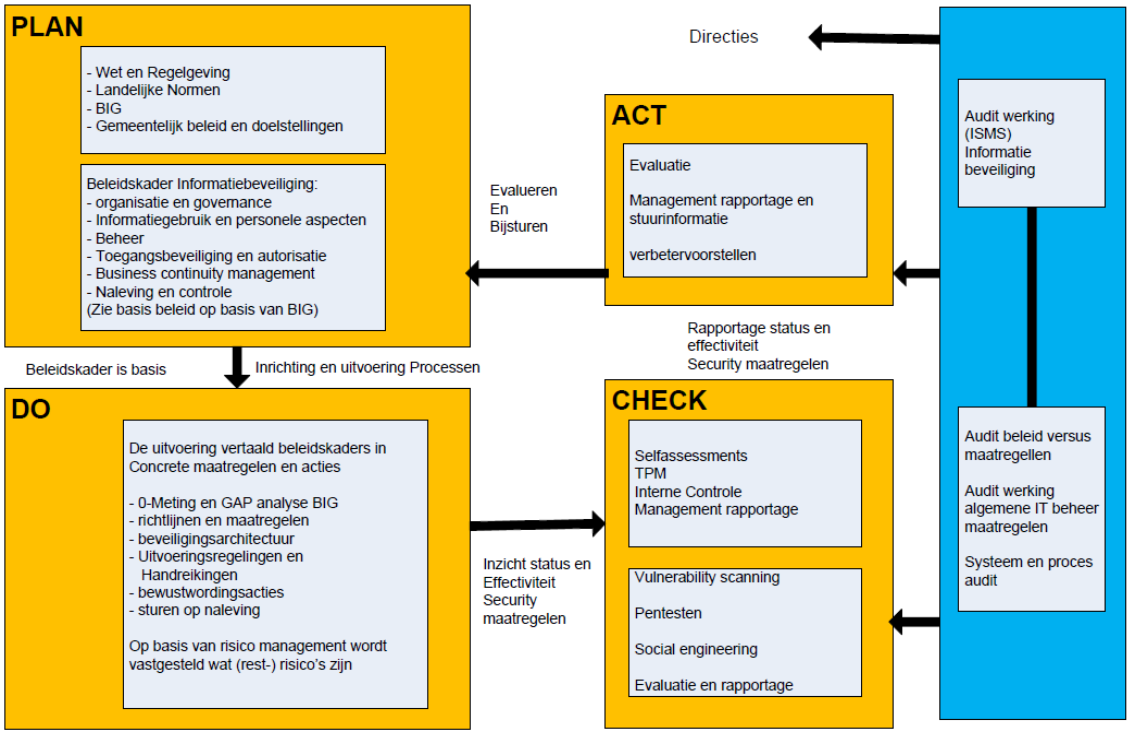
2.a Opdrachtgeversoverleg (OGO): bespreekt rapportages en escalaties van het CISO-overleg. In dit overleg participeren de directeuren bedrijfsvoering (of vergelijkbaar) van de deelnemers en de directeur van het SSC-ZL.
2.b CISO-overleg: houdt zich bezig met alle relevante zaken rondom de informatieveiligheid van de (gewenste) dienstverlening van het SSC-ZL. In dit overleg participeren minimaal de CISO's van de deelnemende gemeenten, de functionarissen Informatiebeveiliging van alle deelnemers en de CISO van het SSC-ZL; de CISO van het SSC-ZL is voorzitter. Auditing (ENSIA) maar ook nieuwe ontwikkelingen worden hier besproken en waar mogelijk vertaald naar actueel beleid c.q. acties. Ook mogelijke dreigingen ten aanzien van de informatieveiligheid worden hier ingebracht en indien nodig geëscaleerd naar het Opdrachtgeversoverleg.

Artikel 27 ICT crisisbeheersing en landelijke samenwerking

Voor interne crisisbeheersing wordt een kernteam IB geïnstalleerd, bestaande uit CISO, de functionaris informatiebeveiliging, security functionaris ICT Service organisatie, relevante experts en de communicatie afdeling. De werkwijze wordt vastgelegd in een aparte regeling.
Waar nodig participeert de security functionaris SSC-ZL Informatie Diensten of andere relevante experts van het SSC-ZL ook in de kernteams IB van de deelnemende gemeenten.
Het SSC-ZL participeert in relevante landelijke platforms en onderhoudt contacten met andere sectoraal georganiseerde IB-platforms.

Artikel 28 PDCA

Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging (NEN/ISO 27001). Deze kwaliteitscyclus is in onderstaande figuur weergegeven.
Toelichting op onderstaande figuur:
- Plan: De cyclus start met IB-beleid, gebaseerd op wet- en regelgeving, landelijke normen zoals de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en 'best practices', uitgewerkt in regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. De planning op hoofdlijnen is onderdeel van het CIO/ICT jaarplan en uitgewerkt in het informatiebeveiligingsplan (op basis van het IB-beleid) van het SSC-ZL. Ook afdelingsspecifieke activiteiten worden in deze plannen.
- Do: Het beleidskader is de basis voor risicomanagement, uitvoering van (technische) maatregelen en bevordering van beveiligingsbewustzijn. Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het 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 auditor; van onder meer de accountant, rijksoverheid (voor bijv. basisregistraties) en SSC-ZL auditors (intern). Dit heeft het karakter van een steekproef. Jaarlijks worden meerdere van dergelijke onderzoeken uitgevoerd, waarbij de CIO/ICT in principe opdrachtgever is. Bevindingen worden gerapporteerd aan de CIO en de directie.
- Act: De cyclus is rond met de uitvoering van verbeteracties o.b.v. check en externe controle. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning en beveiligingsplannen. De bevindingen worden in beginsel gerapporteerd aan de directie. Voor ingrijpende verbeteracties wordt een gevraagde beslissing voorgelegd.



Information Security Management System

Hoofdstuk 4 Beheer van bedrijfsmiddelen

Paragraaf 4.1 Verantwoordelijkheid voor bedrijfsmiddelen

Artikel 29 Risico's

1. 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.
2. Onduidelijkheid wie verantwoordelijk is voor gegevensbestanden, waardoor ook niemand verantwoordelijk is voor de beveiliging en kan optreden bij incidenten.

Artikel 30 Doelstellingen

1. Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.
2. Voor alle bedrijfsmiddelen is de eigenaar vastgelegd alsook de verantwoordelijke voor het handhaven van de beheersmaatregelen.

Artikel 31 Beheersmaatregelen

1. Alle bedrijfsmiddelen moeten geïdentificeerd zijn er moet een inventaris van worden bijgehouden.
2. Alle informatie en bedrijfsmiddelen, die verband houden met ICT-voorzieningen aan een 'eigenaar' (een deel van de organisatie) toewijzen.
3. Regels vaststellen, documenteren implementeren voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen.
4. Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.
5. De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de eigenaar worden gedelegeerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.
6. Medewerkers dienen bij het gebruik van ICT-middelen, social media en informatie de nodige zorgvuldigheid te betrachten en de integriteit en goede naam van het SSC-ZL te waarborgen.
7. Medewerkers gebruiken SSC-ZL informatie primair voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
8. Privégebruik van SSC-ZL informatie en bestanden is niet toegestaan.
9. Voor het werken op afstand en het gebruik van privémiddelen worden nadere regels opgesteld. Echter, de medewerker is gehouden aan regels zoals:

9.a. Illegale software mag niet worden gebruikt voor de uitvoering van het werk.
9.b. Er bestaat de plicht om vanuit goed huisvaderschap de eigen computer te beveiligen.
9.c. Het verbod op ongewenst gebruik in de (fysieke) kantooromgeving geldt ook als dat via de eigen computer plaatsvindt.

10 De medewerker neemt passende technische en organisatorische maatregelen om informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:

10.a. de beveiligingsclassificatie van de informatie (zie hieronder);
10.b de beveiligingsvoorschriften (o.a. dit informatiebeveiligingsbeleid);
10.c aan de werkplek verbonden risico's;
10.d het risico door het benaderen van SSC-ZL informatie met andere dan door het SSC-ZL verstrekte of goedgekeurde ICT-apparatuur.

Paragraaf 4.2 Classificatie van informatie

Artikel 32

1. Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen t.a.v. processen en informatiesystemen worden beveiligingsclassificaties gebruikt. 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).
2. Er zijn drie beschermingsniveaus van laag naar hoog. Daarnaast is er nog een niveau 'geen'. Dit niveau geeft aan dat er geen beschermingseisen worden gesteld, bijvoorbeeld omdat informatie openbaar is. De niveaus zijn in onderstaande tabel weergegeven. Tussen haakjes staan voorbeelden. Deze niveaus zijn bedacht om het proces van classificeren te vereenvoudigen.

Artikel 33 Risico's

1. Geen inzicht in welke componenten, zowel hardware als software, het belangrijkst zijn voor de primaire processen.
2. 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.

Artikel 34 Doelstellingen

1. Informatie heeft een geschikt niveau van bescherming.
2. Classificatie van informatie om bij verwerking de noodzaak en bescherming te kunnen aangeven.

3. Adequate niveaus van bescherming van informatie zijn gedefinieerd en de noodzaak voor aparte verwerkingsmaatregelen is gecommuniceerd.

Artikel 35 Beheersmaatregelen

1. Informatie classificeren met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.
2. Opstellen en uitdragen classificatiebeleid binnen de deelnemende organisaties of SSC-ZL.
3. Er dienen geschikte samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de classificering en verwerking van informatie overeenkomstig het classificatiesysteem dat is vastgesteld.

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van het SSC-ZL)*	**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	**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	**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: primaire proces informatie)*
Hoog	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) *(bv: zorggegevens en strafrechtelijke informatie)*	**Absoluut** het bedrijfsproces staat geen fouten toe	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistraties)*

Artikel 36 Uitganspunten

1. De classificatietabel heeft betrekking op alle in beheer zijnde gegevensverzamelingen, gegevensdragers, informatiesystemen, servers en netwerkcomponenten. Het object van classificatie is informatie. We classificeren op het niveau van informatiesystemen (of informatieservices). Alle classificaties van alle bedrijfskritische systemen zijn centraal vastgelegd door de CISO en dienen jaarlijks gecontroleerd te worden door de eigenaren.
2. Informatie kan meer of minder gevoelig of kritisch zijn. Voor bepaalde informatie kan een extra niveau van bescherming of een speciale verwerking nodig zijn.
3. De eigenaar van de gegevens (veelal ook de proceseigenaar) bepaalt het vereiste beschermingsniveau (classificatie). Indien sprake is van wettelijke eisen, wordt dit expliciet aangegeven. De eigenaar van de gegevens bepaalt tevens wie toegang krijgt tot welke gegevens.
4. Er wordt gestreefd naar een zo ‘laag’ mogelijk classificatieniveau; te hoge classificatie leidt tot onnodige kosten. Bovendien dient informatie in beginsel voor zoveel mogelijk mensen beschikbaar te zijn (transparante overheid).
5. Er wordt gestreefd naar een balans tussen het te lopen risico en de kosten van tegenmaatregelen én daarnaast verdient een technische oplossing altijd de voorkeur boven gedragsverandering.

Artikel 37 Toelichting

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 beveiliging kan worden bewerkstelligd dit als ‘passend’ kan worden beschouwd. Extra beveiliging is echter niet meer passend, indien de kosten voor het mitigeren van de risico’s disproportioneel hoog zijn (dit is uitgebreid beschreven in: ‘Beveiliging van persoonsgegevens’, CBP richtsnoeren, 2013). Kort gezegd: risico’s en tegenmaatregelen dienen in balans te zijn.

Hoofdstuk 5 Beveiliging van personeel

Artikel 38 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.

Artikel 39 Doelstellingen

1. Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.
2. De verantwoordelijkheden ten aanzien van beveiliging is vóór het dienstverband vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden.
3. Alle kandidaten voor een aanstelling, ingehuurd personeel en externe gebruikers worden gescreend, in het bijzonder voor vertrouwensfuncties.
4. Werknemers, ingehuurd personeel en externe gebruikers, die ICT-voorzieningen gebruiken tekenen een overeenkomst over hun beveiligingsrollen en –verantwoordelijkheden.

Artikel 40 Beheersmaatregelen

1. Het lijnmanagement is verantwoordelijk voor het juist afhandelen van de beveiligingsaspecten van het aangaan, wijzigen en beëindigen van een dienstverband of een overeenkomst met externen. De HRM-adviseur houdt toezicht op dit proces.
2. Bij beëindiging van het dienstverband en inhuur worden alle bedrijfsmiddelen van de organisatie geretourneerd. Autorisaties worden in opdracht van het lijnmanagement geblokkeerd.
3. Medewerkers die werken met vertrouwelijke of geheime informatie overleggen voor indiensttreding een Verklaring Omtrent het Gedrag (VOG). De VOG wordt indien nodig herhaald tijdens het dienstverband.
4. Het lijnmanagement bepaalt welke rol(len) de medewerker moet vervullen en welke autorisaties voor het raadplegen, opvoeren, muteren en afvoeren van gegevens moeten worden verstrekt.
5. Alle medewerkers (en voor zover van toepassing externe gebruikers van onze systemen) krijgen training in procedures die binnen het SSC-ZL of afdeling gelden voor informatiebeveiliging. Deze training wordt regelmatig herhaald om het beveiligingsbewustzijn op peil te houden.
6. Bij inbreuk op de beveiliging gelden voor medewerkers de gebruikelijke disciplinaire maatregelen, zoals onder meer genoemd in het Ambtenarenreglement en SSC-ZL regelingen.
7. Regels die volgen uit dit beleid en andere SSC-ZL regelingen gelden ook voor externen, die in opdracht van het SSC-ZL werkzaamheden uitvoeren.

Artikel 41 Bewustwording

1. Het SSC-ZL/de directie/de afdeling bevordert algehele communicatie en bewustwording rondom informatieveiligheid.
2. Het lijnmanagement bevordert dat medewerkers (en externe gebruikers van onze systemen) zich houden aan beveiligingsrichtlijnen. Afspraken hierover worden vastgelegd in de afdelingsjaarplannen.
3. In werkoverleggen wordt periodiek aandacht geschonken aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd in planningsgesprekken.

Hoofdstuk 6 Fysieke beveiliging en beveiliging van de omgeving

Artikel 42 Risico's

1. Onbevoegde toegang tot kritieke systemen of waardevolle informatie. Bij het ontbreken van registratie zijn incidenten bovendien niet herleidbaar tot individuen.
2. Door bijvoorbeeld de inzet van externen, de toeloop van leveranciers en andere niet-medewerkers of het feit dat de medewerkers op meerdere locaties op geruime afstand van elkaar gevestigd zijn, is het betrekkelijk eenvoudig voor niet-medewerkers om toegang tot de panden te krijgen door tegelijk met een geautoriseerde medewerker naar binnen te gaan.
3. Als informatie zichtbaar op bureaus ligt, is er een verhoogd risico mert betrekking tot de de vertrouwelijkheid.
4. Geen procedures voor het veilig verwijderen of hergebruiken van ICT-apparatuur.
5. Bescherming van apparatuur, waaronder apparatuur die buiten de locatie wordt gebruikt en het verwijderen van bedrijfseigendommen, is noodzakelijk om het risico van toegang door onbevoeg-

den tot informatie te verminderen en om de apparatuur en informatie te beschermen tegen verlies of schade.

Artikel 43 Doelstellingen

1. 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.
2. ICT-voorzieningen, die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, behoren fysiek te worden ondergebracht in beveiligde ruimten, beschermd door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. Ze behoren fysiek te worden beschermd tegen toegang door onbevoegden, schade en storingen.
3. Het voorkomen van verlies, schade of diefstal van apparatuur en bescherming tegen fysieke bedreigingen en gevaren van buitenaf.

Artikel 44 Beheersmaatregelen

1. Alle objecten (gebouwen) van het SSC-ZL krijgen op basis van generieke profielen een risicoprofiel toegewezen. Dit is het generieke risicoprofiel dat het beste aansluit bij het object.
2. De schade door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) wordt beperkt door passende preventieve maatregelen.
3. Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
4. De uitgifte van toegangsmiddelen wordt geregistreerd.
5. In gebouwen met beveiligde zones houdt beveiligingspersoneel toezicht op de toegang. Hiervan wordt een registratie bijgehouden.
6. De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering (en het risicoprofiel).
7. In diverse panden van het SSC-ZL (o.a. de datacenters) wordt gebruik gemaakt van cameratoezicht. Het gebruik van beeldmateriaal is beperkt door de Wet Bescherming Persoonsgegevens en nadere regels.
8. De fysieke toegang tot ruimten waar zich informatie en ICT-voorzieningen bevinden is voorbehouden aan bevoegd personeel. Registratie van de verleende toegang ondersteunt de uitvoering van de toegangsregeling.
9. Serverruimtes, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende ‘best practices’.
10. (Data)verbindingen worden beschermd tegen interceptie of beschadiging. Reserve apparatuur en back-ups zijn gescheiden in twee locaties of datacenters, om de gevolgen van een calamiteit te minimaliseren.
11 Gegevens en programmatuur worden van apparatuur verwijderd of veilig overschreven, voordat de apparatuur wordt afgevoerd. Informatie wordt bewaard en vernietigd conform de Archiefwet 1995 en de daaruit voortvloeiende archiefbesluiten.

Hoofdstuk 7 Beveiliging van apparatuur en informatie

Artikel 45 Risico's

1. 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.
2. Onjuiste autorisaties kunnen leiden tot foutieve handelingen, fraude en verduistering.
3. 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.
4. Het SSC-ZL 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 het SSC-ZL op straat komen te liggen. Het SSC-ZL blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.
5. Programmatuur en ICT-voorzieningen zijn kwetsbaar voor virussen.
6. Medewerkers die zich niet houden aan afgesproken gedragsregels rondom het flexibel werken.

Artikel 46 Doelstellingen

1. Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.

2. Vastgestelde verantwoordelijkheden en procedures voor beheer en bediening van alle ICT-voorzieningen. Dit omvat tevens de ontwikkeling van geschikte bedieningsinstructies.
3. Toepassing, waar nodig, van functiescheiding om het risico van nalatigheid of opzettelijk misbruik te verminderen.

Paragraaf 7.1 Beheersmaatregelen

Artikel 47 Organisatorische aspecten

1. 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.
2. Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker. Bij externe hosting van data en/of services (uitbesteding, cloud computing) blijft het SSC-ZL eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Dit is gebonden aan regels en vereist goede (contractuele) afspraken en controle hierop.
3. Externe hosting van data en/of services is:

3.a. goedgekeurd door verantwoordelijk lijnmanager;
3.b. in overeenstemming met IB-beleid en algemeen SSC-ZL beleid;
3.c. vooraf gemeld bij ICT t.b.v. toetsing op beheeraspecten.

Artikel 48 Systeemplanning en –acceptatie

1. Nieuwe systemen, upgrades en nieuwe versies worden getest op impact en gevolgen en pas geïmplementeerd na formele acceptatie en goedkeuring door de opdrachtgever (veelal de proceseigenaar). De test en de testresultaten worden gedocumenteerd.
2. Systemen voor Ontwikkeling, Test en/of Acceptatie (OTA) zijn logisch gescheiden van Productie (P).
3. Faciliteiten voor ontwikkeling, testen, acceptatie en productie (OTAP) zijn gescheiden om onbevoegde toegang tot of wijziging in het productiesysteem te voorkomen.
4. In de OTA worden testaccounts gebruikt. Er wordt in beginsel niet getest met productie accounts, mits voor de test absoluut noodzakelijk.
5. Vertrouwelijke of geheime data uit de productieomgeving mag niet worden gebruikt in de ontwikkel-, test-, opleidings-, en acceptatieomgeving tenzij de gegevens zijn geanonimiseerd. Indien het toch noodzakelijk is om data uit productie te gebruiken, is uitdrukkelijke toestemming van de eigenaar van de gegevens vereist en dienen er procedures te worden gevolgd om data te vernietigen na ontwikkelen en testen.
6. Het gebruik van ICT-middelen wordt gemonitord ten behoeve van een tijdige aanpassing van de beschikbare capaciteit aan de vraag.

Artikel 49 Technische aspecten

1. Alle gegevens anders dan classificatie ‘geen’ worden versleuteld conform beveiligingseisen in de SSC-ZL IB-architectuur.

1.a. Classificatieniveau ‘laag’: transportbeveiliging buiten het interne netwerk;
1.b. Classificatieniveau ‘midden’: transportbeveiliging;
1.c. Classificatieniveau ‘hoog’: transport en berichtbeveiliging.

2. Versleuteling vindt plaats conform ‘best practices’ (de stand der techniek), waarbij geldt dat de vereiste encryptie sterker is naarmate gegevens gevoeliger zijn.
3.. Gegevens op papier worden beschermd door een deugdelijke opslag en regeling voor de toegang tot archiefruimten.
4. Bij het openen of wegschrijven van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. Ook inkomende en uitgaande e-mails worden hierop gecontroleerd. De update voor de detectiedefinities vindt in beginsel dagelijks plaats.
5. Op verschillende niveaus binnen de ICT-infrastructuur (netwerkcomponenten, servers, pc’s) wordt antivirus software van verschillende leveranciers toegepast.
6. Alle apparatuur die is verbonden met het netwerk van het SSC-ZL moet kunnen worden geïdentificeerd.
7. ‘Mobile code’ wordt uitgevoerd in een logisch geïsoleerde omgeving om de kans op aantasting van de integriteit van het systeem te verkleinen. De ‘mobile code’ wordt altijd uitgevoerd met minimale rechten zodat de integriteit van het host systeem niet aangetast wordt.

8. Documenten, opslagmedia, in- en uitvoergegevens en systeemdocumentatie worden beschermd tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.
9. Het (ongecontroleerd) kopiëren van 'geheime' gegevens is niet toegestaan, behalve voor back-up door bevoegd systeembeheer.
10. Alle informatie, die wordt geplaatst op websites van het SSC-ZL, wordt beschermd tegen onbevoegde wijziging. Op algemeen toegankelijke websites wordt alleen openbare informatie gepubliceerd.
11. Groepen informatiediensten, gebruikers en informatiesystemen worden op het netwerk gescheiden zodat de kans op onbevoegde toegang tot gegevens verder wordt verkleind.
12. Afhankelijk van de risico's die verbonden zijn aan online transacties worden maatregelen getroffen om onvolledige overdracht, onjuiste routing, onbevoegde wijziging, openbaarmaking, duplicatie of weergave te voorkomen.
16 Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau (service levels) komt.

Artikel 50 Mobiele (privé-)apparatuur en thuiswerkplek

1. Beveiligingsmaatregelen hebben betrekking op zowel door de het SSC-ZL verstrekte middelen als privé-apparatuur ('bring your own device' (BYOD)). Op privé-apparatuur waarmee verbinding wordt gemaakt met het SSC-ZL netwerk is het SSC-ZL bevoegd om beveiligingsinstellingen af te dwingen. Dit betreft onder meer: controle op wachtwoord, encryptie, aanwezigheid van malware, etc. Het gebruik van privé-apparatuur waarop beveiligingsinstellingen zijn verwijderd ('jail break', 'rooted device') is niet toegestaan.
2. Op verzoek van het SSC-ZL dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan (denk bijvoorbeeld aan 'mobile device management software'). De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van SSC-ZL informatie en integriteit van het SSC-ZL netwerk.
3. In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privémiddelen en privébestanden.

Artikel 51 Back-up en recovery

1. In opdracht van de eigenaar van data, maakt ICT reservekopieën van alle essentiële bedrijfsgegevens en programmatuur zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd.
2. De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering, zoals gedefinieerd door de eigenaar van de gegevens.
3. Bij ketensystemen dient het back-up mechanisme de data-integriteit van de informatieketen te waarborgen.
4. De back-up en herstelprocedures worden regelmatig (tenminste 1 x per jaar) getest om de betrouwbaarheid ervan vast te stellen.

Artikel 52 Informatie-uitwisseling

1. Voor het gebruik van SSC-ZL informatie gelden de rechten en plichten zoals vastgelegd in de diverse documenten, zoals het CAR-UWO, geheimhoudingsverklaring, huisregels.
2. Digitale documenten van het SSC-ZL waar burgers en bedrijven rechten aan kunnen ontlenen, maken gebruik van PKI Overheid certificaten voor tekenen en/of encryptie. Hiervoor wordt een richtlijn PKI en certificaten opgesteld.
3. Er is een (spam) filter geactiveerd voor inkomende e-mail berichten.

Artikel 53 Controle

1. 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 (In sommige processen is het wettelijk verplicht of zeer gewenst dat geautoriseerde toegang wordt vastgelegd, zodat achteraf steeds kan worden vastgesteld wie toegang tot de gegevens heeft gehad). Relevante zaken om te loggen zijn:

1.a. type gebeurtenis (zoals back-up/restore, reset wachtwoord, betreden ruimte);
1.b. handelingen met speciale bevoegdheden;
1.c. (poging tot) ongeautoriseerde toegang;

1.d. systeemwaarschuwingen;
1.e. (poging tot) wijziging van de beveiligingsinstellingen.
2. Een logregel bevat minimaal:
2.a een tot een natuurlijk persoon herleidbare gebruikersnaam of ID;
2.b. de gebeurtenis;
2.c. waar mogelijk de identiteit van het werkstation of de locatie;
2.d. het object waarop de handeling werd uitgevoerd;
2.e. het resultaat van de handeling;
2.f. de datum en het tijdstip van de gebeurtenis.
3. In een logregel worden alleen de voor de rapportage noodzakelijke gegevens opgeslagen.
4. 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.

Paragraaf 7.2 Beheer van de dienstverlening door een derde partij

Artikel 54 Risico's
Het SSC-ZL 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 het SSC-ZL op straat komen te liggen. Het SSC-ZL blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.

Artikel 55 Doelstellingen
1. Een passend niveau van informatiebeveiliging implementeren en bijhouden en dit vastleggen in een (bewerkers)overeenkomst, contracten en/of convenanten.
2. De organisatie controleert de implementatie van de maatregelen, die zijn vastgelegd in 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.

Artikel 56 Beheersmaatregelen
1. 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.
2. De diensten, rapporten en registraties, die door de derde partij worden geleverd, worden gecontroleerd en beoordeeld en er worden periodiek audits uitgevoerd.
3. Wijzigingen in de dienstverlening door derden, in bijvoorbeeld bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, worden beheerd.

Artikel 57 Uitgangspunten
1. In de basis-SLA voor dienstverlening is aandacht besteed aan informatiebeveiliging.
2. Er is een basiscontract voor de toegang tot de ICT-voorzieningen en/of de informatievoorziening (bestanden, gegevens) door derden waarin kaders staan voor de toegang tot ICT-voorzieningen door derden. In contractbeheer, applicatiebeheer en functioneel beheer is naleving van de gemaakte afspraken opgenomen.
3. Programmatuur en ICT-voorzieningen zijn kwetsbaar voor virussen.
4. Het ontbreken van een regeling voor antivirus bescherming bij medewerkers thuis leidt tot hogere beveiligingsrisico's.

Paragraaf 7.3 Behandeling van media

Artikel 58 Risico's
Verwijderbare media kan informatie bevatten, die in onbevoegde handen kan vallen bij onjuist gebruik, verlies of diefstal.

Artikel 59 Doelstellingen
1. Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van informatie en bedrijfsmiddelen.
2. Media worden beheerst en fysiek beschermd.
3. Vastgestelde procedures om documenten, opslagmedia (bijvoorbeeld USB-sticks, back-up tapes, schijven), in- en uitvoergegevens en systeemdocumentatie te beschermen tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.

Artikel 60 Beheersmaatregelen

1. Er dienen procedures te worden vastgesteld voor het beheer van verwijderbare media.
2. Er dienen procedures te worden vastgesteld voor het op een veilige manier verwijderen van media als ze niet langer nodig zijn.
3. Systeemdocumentatie dient te worden beschermd tegen onbevoegde toegang.

Artikel 61 Uitgangspunten

1. Er zijn procedures voor het beheer van verwijderbare media en voor het veilig verwijderen of hergebruiken van ICT-apparatuur.
2. Harde schijven en andere media worden adequaat gewist of vernietigd bij afstoting of hergebruik. In ieder geval indien er vertrouwelijke informatie is opgeslagen en/of licentie plichtige programmatuur op is geïnstalleerd.
3. Er zijn richtlijnen voor het opbergen van papieren en computermedia. In ieder geval voor gevoelige of kritieke bedrijfsinformatie.
4. Innamebeleid voor mobiele apparatuur, zoals laptops, pda's, iPads, voor wanneer deze niet meer worden gebruikt.
5. Encryptie op informatie met het classificatielabel vertrouwelijk en zeer geheim.

Paragraaf 7.4 Uitwisseling van informatie

Artikel 62 Risico's

Verlies of diefstal van laptops, USB-sticks, iPads e.d., waarbij bovendien informatie in verkeerde handen komt.

Artikel 63 Doelstellingen

1. Handhaven van beveiliging van informatie en programmatuur, die wordt uitgewisseld binnen een organisatie en met enige externe entiteit.
2. Een formeel uitwisselingsbeleid met betrekking tot de uitwisseling van informatie en programmatuur tussen organisaties, dat in lijn is met de uitwisselingsovereenkomsten en relevante wetgeving.
3. Vastgestelde procedures en normen ter bescherming van informatie en fysieke media, die informatie bevatten die wordt getransporteerd.

Artikel 64 Beheersmaatregelen

1. Vaststellen formeel beleid, formele procedures en formele beheersmaatregelen om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.
2. Vaststellen overeenkomsten voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.
3. Beschermingsmaatregelen voor media die informatie bevatten tegen onbevoegde toegang, misbruik of het corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.
4. Bescherming van informatie, die een rol speelt bij elektronische berichtuitwisseling.

Artikel 65 Uitgangspunten

1. Geformaliseerde situatie rondom het transport van de back-ups en de mogelijkheden van leveranciers om toegang tot het netwerk te verkrijgen.
2. Een basisraamwerk met randvoorwaarden voor gegevensuitwisseling met ketenpartners.
3. Gevoelige informatie (classificatie vertrouwelijk en zeer geheim) wordt nooit bekend gemaakt via telefoon of fax, in verband met bijvoorbeeld afluisteren.
4. Bewustzijn en sociale controle om het risico op het lekken van informatie via telefoon e.d. te laten afnemen.

Hoofdstuk 8 Logische toegangsbeveiliging

Artikel 66

De identiteit van een gebruiker die toegang krijgt tot SSC-ZL informatie dient te worden vastgesteld. Logische toegang is gebaseerd op de classificatie van de informatie.

Artikel 67 Risico's

1. 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.
2. Verstoringen door onjuist gebruik van ICT-ruimtes of ICT-componenten (m.n. waar ook niet ICT-teams toegang hebben).

Artikel 68 Doelstellingen

1. Beheersen van de toegang tot informatie, ICT-voorzieningen en bedrijfsprocessen op grond van bedrijfsbehoeften en beveiligingseisen.
2. Beleid ten aanzien van informatieverspreiding en autorisatie is van toepassing.

Artikel 69 Uitgangspunten

1. De eigenaar van de data is bevoegd toegang te verlenen.
2. Er worden in de regel geen 'algemene' identiteiten gebruikt. Voor herleidbaarheid en transparantie is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd. Indien dit geen (wettelijke) eis is kan worden gewerkt met functionele accounts.
3. Het SSC-ZL maakt, waar mogelijk, gebruik van bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatiebeveiliging (zoals: DigiD en eHerkenning).

Artikel 70 Authenticatie en autorisatie

1. Wachtwoorden hebben een maximale geldigheidsduur van 60 dagen. Wachtwoorden dienen aan eisen te voldoen, deze worden afgedwongen door het systeem. Voor medewerkers met speciale bevoegdheden (systeem en functioneel beheerders) gelden strengere eisen.
2. De gebruiker is verantwoordelijk voor het geheim blijven van zijn wachtwoord.
3. Authenticatiemiddelen zoals wachtwoorden worden beschermd tegen inzage en wijziging door onbevoegden tijdens transport en opslag (door middel van encryptie).
4. Autorisatie is rol gebaseerd. Autorisaties worden toegekend via functie(s) en organisatie onderdelen.
5. Toegang tot informatie met classificaties 'midden' of 'hoog' vereist 'multi-factor' authenticatie (bijv. naam/wachtwoord + token).

Artikel 71 Externe toegang

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

Artikel 72 Mobiel en thuiswerken

1. Voor werken op afstand is een thuiswerkomgeving beschikbaar. Toegang tot vertrouwelijke informatie wordt verleend op basis van multifactor authenticatie.
2. Mobiele bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen SSC-ZL informatie wordt opgeslagen op het mobiele apparaat ('zero footprint'). SSC-ZL informatie dient te worden versleuteld bij transport en opslag conform classificatie eisen (separaat document).
3. Voorzieningen als webmail, als ook sociale netwerk en clouddiensten (Dropbox, Gmail, etc.) zijn door het lage beschermingsniveau (veelal alleen naam en wachtwoord, het ontbreken van versleuteling) niet geschikt voor het delen van vertrouwelijke en geheime informatie.

Artikel 73 Overige maatregelen

Het bedrijfsnetwerk van het SSC-ZL is waar mogelijk gesegmenteerd.

Paragraaf 8.1 Beveiliging van informatiesystemen (software)

Artikel 74 Doelstelling

Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

Artikel 75 Organisatorische aspecten

1. Toetsing op IB-beleid is onderdeel van de toets voor projecten met een ICT-component en onderdeel van de project start architectuur (PSA) en eind architectuur (zie hiervoor de projectmanagement methodiek Prince2).
2. Projecten met een hoog risicoprofiel vallen onder toezicht van ICT. Toetsing op architectuur en informatiebeveiliging is hier onderdeel van.
3. Projectmandaten worden ten behoeve van behandeling in intern overleg (onder meer) voorzien van een advies op informatiebeveiliging.
4. In het programma van eisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen worden ook relevante beveiligingseisen opgenomen.

Artikel 76 Softwareontwikkeling en onderhoud

1. Applicaties worden ontwikkeld en getest o.b.v. landelijke richtlijnen voor beveiliging, zoals richtlijnen voor beveiliging van webapplicatie van het NCSC. Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de OWASP top 10.
2. Web applicaties worden voor de in productie name onder meer getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL injectie, cross site scripting, etc.).
3. De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).
4. Alleen gegevens die noodzakelijk zijn voor de gebruiker worden uitgevoerd (doelbinding), rekening houdend met beveiligingseisen (classificatie).
5. Toegang tot de broncode is beperkt tot de medewerkers, die deze code onderhouden of installeren.
6. Technische kwetsbaarheden worden regulier met een minimum van 4 keer per jaar gerepareerd door ‘patchen’ van software, of ‘ad hoc’ bij acute dreiging. Welke software wordt geüpdatet wordt mede bepaald door de risico’s.

Artikel 77 Encryptie (versleuteling)

1. Het SSC-ZL gebruikt encryptie conform PKI-overheid standaard (Public Key Infrastructure voor de overheid waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail, websites of andere gegevensuitwisseling).
2. Intern dataverkeer (‘machine to machine’) wordt conform classificatie beveiligd met certificaten.
3. Beveiligingscertificaten worden centraal beheerd binnen het SSC-ZL.

Hoofdstuk 9 Beveiligingsincidenten

Artikel 78 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.

Artikel 79 Doelstellingen

1. Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden, die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.
2. 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.
3. Er is een verplichte meldingssystematiek in werking om alle informatiebeveiligingsgebeurtenissen en zwakke plekken zo snel mogelijk te rapporteren aan de aangewezen contactpersoon.

Artikel 80 Melding en registratie

1. De medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten direct te melden bij de functionaris informatiebeveiliging van het SSC-ZL.
2. Beveiligingsincidenten die worden gemeld bij de service desk, worden als zodanig geregistreerd en voorgelegd aan de security functionaris binnen ICT. Voor afhandeling geldt de reguliere rapportage en escalatielijn.
3. Indien er sprake is van een datalek is er een meldplicht bij de Autoriteit Persoonsgegevens (Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (zowel

bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een datalek hebben).
4. Ernstige incidenten, waarbij een alarmfase (zie onder) in werking treedt, worden opgenomen in de kwartaalrapportage van de CISO.

Artikel 81 Alarmfasen
Bij grote incidenten wordt gehandeld en opgeschaald conform de draaiboeken ICT- crisisbeheersing.

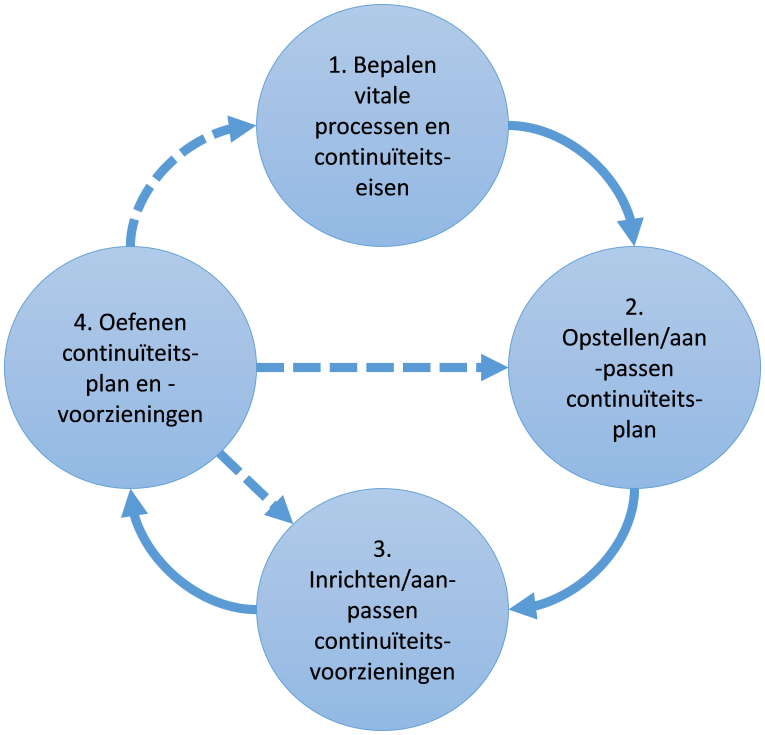
Alarm fase	Kenmerk	Impact	Opschaling	Bijzonderheden
1	Lokaal ICT-incident bij één afdeling.	Oplosbaar probleem: bronbestrijding.	In beginsel niet. Probleem wordt opgelost door SSC-ZL ID.	Melding aan CISO
2	ICT-Incident bij meerdere afdelingen.	Nog steeds een geïsoleerd probleem: bron - + effectbestrijding.	In beginsel niet. Probleem wordt opgelost door SSC-ZL ID.	Melding aan CISO. Melding bij IBD indien nodig. SSC-ZL communicatie is optioneel.
3	Concernbreed ICT-incident (en mogelijk andere gemeenten)	Impact op de SSC-ZL dienstverlening wordt echt ervaren.	Kernteam IB komt bij elkaar. Afhankelijk van het incident (impact) treedt de GRIP structuur in werking. Bestuur, CIO en directies worden geïnformeerd.	Melding aan CISO. Melding bij IBD (indien nodig). SSC-ZL afdeling communicatie is vereist.
4	ICT-Incident is concern overstijgend (landelijk)	Impact op de SSC-ZL dienstverlening is manifest.	Mogelijk treedt de GRIP structuur in werking. Het kernteam IB is dan in beginsel adviserend en voert desgewenst coördinatie (binnen het ICT domein).	Er is sprake van landelijke opschaling via de technische lijn (IBD -> NCSC) of via de maatschappelijke lijn (NCC).

Hoofdstuk 10 Bedrijfscontinuïteit

Artikel 82 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. Bijvoorbeeld het uitvallen van medewerkers (ziekte, sterven, ontslag) kan een reële bedreiging zijn.

Artikel 83 Doelstellingen
1. Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen
2. tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.
3. Een adequaat beheerproces van bedrijfscontinuïteit om de uitwerking op de organisatie, veroorzaakt door het verlies van informatie en het herstellen daarvan tot een aanvaardbaar niveau te beperken.
4. Informatiebeveiliging is een integraal onderdeel van het totale bedrijfscontinuïteitsproces en andere beheerprocessen binnen de organisatie.

Artikel 84 Impactanalyse & BCM
1. Elke SSC-ZL afdeling voert een business impactanalyse uit. Afhankelijk van de bevindingen worden per afdeling vervolgacties gepland.
2. Elke afdeling heeft een eigen plan voor Business Continuity Management (BCM) (bedrijfscontinuïteitsbeheer). In de continuïteitsplannen wordt minimaal aandacht besteed aan:
2.a. risico's;
2.b. identificatie van essentiële procedures voor bedrijfscontinuïteit;
2.c. wie het plan mag activeren en wanneer, maar ook wanneer er weer gecontroleerd wordt teruggegaan;
2.d. veilig te stellen informatie (aanvaardbaarheid van verlies van informatie);
2.e. prioriteiten en volgorde van herstel en reconstructie;
2.f. documentatie van systemen en processen;
2.g. kennis en kundigheid van personeel om de processen weer op te starten.
3. Er worden minimaal jaarlijks oefeningen of testen gehouden om de BCM plannen te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.



Artikel 85 Beleidsuitgangspunt

1. Er zijn voor de belangrijkste processen en systemen continuïteits-/uitwijkplannen welke door middel van een beheerst proces tot stand komen.
2. Continuïteitsplannen moeten regelmatig worden getest en actueel worden gehouden.

Hoofdstuk 11 Naleving

Artikel 86

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

Artikel 87 Organisatorische aspecten

1. Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle SSC-ZL 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:

1.a. de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;

1.b. efficiency en effectiviteit van de geïmplementeerde maatregelen;

1.c. de mate waarin de informatiebeveiliging het bereiken van de strategische doelstellingen ondersteunt.

2. De CISO zorgt namens de directeur voor het toezicht op de uitvoering van het IB-beleid.
3. ICT en externe hosting providers leggen verantwoording af aan hun opdrachtgevers over de naleving van het IB-beleid. Bij uitbestede (beheer)processen kan een verklaring bij leveranciers worden opgevraagd (TPM of ISAE3402-verklaring).
4. Naleving van regels vergt in toenemende mate ook externe verantwoording, bijvoorbeeld voor het gebruik van DigiD, SUWI, BAG, BGT, PUN en BRP. Aanvullend op dit concern IB-beleid kunnen daarom specifieke normen gelden.
5. Periodiek wordt de kwaliteit van informatieveiligheid in opdracht van de CIO onderzocht door SSC-ZL auditors en door onafhankelijke externen (bijvoorbeeld door middel van 'penetratietesten'). Jaarlijks worden ca. 3 audits/onderzoeken gepland. De bevindingen worden gebruikt voor de verdere verbetering van de informatieveiligheid.
6. In de P&C cyclus wordt gerapporteerd over informatieveiligheid aan de hand van het 'in control' statement.

7. 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.

Artikel 88 (Wettelijke) kaders

1. Een overzicht van relevante wet en regelgeving is te vinden bij KING. Zo is het gebruik van persoonsgegevens geregeld in de Wet Bescherming Persoonsgegevens (Zie ook: CBP richtsnoeren). Met ingang van 25 mei 2018 wordt de Wet Bescherming Persoonsgegevens vervangen door de Europese Algemene Verordening Gegevensbescherming (AVG).
2. Voor elk type registratie wordt de bewaartermijn, het opslagmedium en eventuele vernietiging bepaald in overeenstemming met wet, regelgeving, contractuele verplichtingen en bedrijfsmatige eisen. Bij de keuze van het opslagmedium wordt rekening gehouden met de bewaartermijn, de achteruitgang van de kwaliteit van het medium in de loop van de tijd en de voortdurende beschikbaarheid van hulpmiddelen (zoals hard- en software) om de gegevens te raadplegen en te bewerken.
3. Bij het (laten) vervaardigen en installeren van programmatuur, wordt er voor gezorgd dat de intellectuele eigendomsrechten die daar op rusten niet worden geschonden.

Aldus vastgesteld in de vergadering van het bestuur van 4 april 2018
J. Aarts
Voorzitter
W. Lousberg
Secretaris

Bijlage 1 Relevante documenten en bronnen

Intern

1. Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) (nog vast te stellen door het bestuur)
2. volgt

Extern

1. NEN/ISO 27001 en 27002 (Code voor Informatiebeveiliging)
2. Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), KING, 2013
3. Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
4. Tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
5. CBP richtsnoeren 'beveiliging van persoonsgegevens', 2013: http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx
6. GEMMA: http://www.kinggemeenten.nl/king-kwaliteitsinstituut-nederlandse-gemeenten/e-dienstverlening-verbeteren/gemma
7. De website ENSIA: https://www.kinggemeenten.nl/ensia
8. Richtlijn Cloudcomputing van het NCSC: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html
9. ICT-Beveiligingsrichtlijnen voor Webapplicaties van het NCSC: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html
10. OWASP top 10: https://www.owasp.org