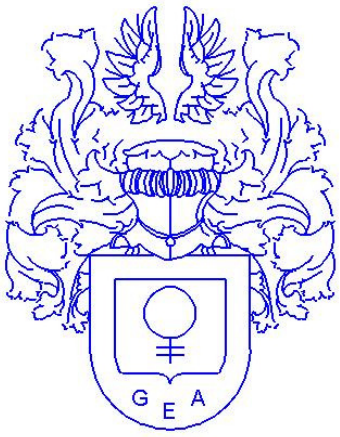
Preview

Algemeen Handboek Informatiebeveiliging

NEN-ISO/IEC 27002 (CvI / BIG)

*



Gemeentelijk Efficiency Adviesbureau bv
Schoonouwenseweg 10
2821 NX Stolwijk
☎0182-341350
info@gea-bv.nl

---

* Versie: preview
Datum: oktober 2014

INHOUDSOPGAVE

1. Onderwerp en toepassingsgebied

1.1 Algemeen

Dit handboek geeft een nadere invulling van de algemene aspecten van het "Informatiebeveiligingsbeleid". Het geldt voor de gehele organisatie en wordt via het Intranet bekend gemaakt.

Naast de richtlijnen en adviezen uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en Code voor Informatiebeveiliging (NEN-ISO/IEC 27002) is ook het rapport "Beveiliging van persoonsgegevens" (achtergrondstudies en verkenningen 23) van het College Bescherming Persoonsgegevens gebruikt.

Alleen door bewust te werken aan informatiebeveiliging en mensen expliciet op hun taken, verantwoordelijkheden en bevoegdheden te wijzen, kunnen een aantal essentiële stappen gezet worden in dit traject.

Ook de wettelijke eisen die aan basisregistraties worden gesteld zijn van invloed op de wijze van beveiliging en zijn hierin meegenomen. Als gevolg hiervan en door de steeds verdere uitbreiding van het aantal basisregistraties, is dit een dynamisch document en zal regelmatig geactualiseerd worden.
Ook de stand van de techniek en organisatieveranderingen zijn reden voor een actualisering. Zeker niet op de laatste plaats heeft een beleidswijziging invloed op de inhoud van dit document.

De huidige stand van technologie biedt ons de mogelijkheid om onze zaken veelal elektronisch af te handelen. We wisselen e-mail uit en kunnen elektronisch winkelen. Gegevens worden met behulp van de meest uiteenlopende communicatiemedia uitgewisseld en komen in diverse systemen bij verschillende organisaties voor. We zijn afhankelijk van technologie. Welke gevaren voor onze persoonlijke levenssfeer de toepassing van deze technologie in werkelijkheid met zich meebrengt, is vaak nog onbekend.

Sinds het begin van de jaren tachtig probeert de overheid de privacy van de burgers in de huidige informatiemaatschappij met bijzondere wet- en regelgeving te beschermen.

Het Europese parlement en de Raad van de Europese Unie hebben daarom een richtlijn vastgelegd. Aansluitend hierop is door de Informatiebeveiligingsdienst voor gemeenten (IBD) de BIG opgesteld.

Met de Wet Bescherming Persoonsgegevens (WBP) wordt deze richtlijn in Nederland uitgevoerd. De WBP dicteert een aantal dwingende normen omtrent de verwerking van en omgang met persoonsgegevens. Waar persoonsgegevens geautomatiseerd worden verwerkt, is het beveiligen van de daarbij gebruikte informatiesystemen een noodzakelijke voorwaarde om aan de doelstellingen van de wet te voldoen.

In toenemende mate worden informatiesystemen, zowel openbare als private netwerken, onderling verbonden. De onderlinge verbondenheid en het delen van informatiemiddelen maken het steeds moeilijker om de toegang te beveiligen. Veel informatiesystemen zijn niet ontworpen met het oog op veiligheid. De beveiliging die met technische middelen kan worden bereikt is begrensd en dient te worden ondersteund door passende maatregelen en procedures.

Bij een aantal hoofdstukken en paragrafen is een verwijzing opgenomen naar het "Informatiebeveiligingsbeleid".
Dit betekent dat de uitvoering zonder afwijking is gerealiseerd zoals in het Informatiebeveiligingsbeleid is vermeld of in één van de specifieke handboeken nader is beschreven.

1.2 Bewaarplaats handboek

Dit handboek bevat waardevolle en vertrouwelijke informatie die niet in handen mag komen van onbevoegden.

Na vaststelling wordt dit handboek in pdf-formaat op het intranet geplaatst zodat het voor iedere medewerker toegankelijk is.

Een werkexemplaar, in papieren vorm, wordt bewaard op afdeling Informatiebeheer en Automatisering. Dit exemplaar is tevens beschikbaar voor inzage.

2. Termen en definities

Voor dit hoofdstuk wordt verwezen naar het “Informatiebeveiligingsbeleid”.

3. Structuur van deze norm

Voor de invulling van dit handboek is uitgegaan van de beveiligingseisen van algemene aard die in het beveiligingsbeleid zijn gedefinieerd.

In het handboek zijn de afspraken, maatregelen en procedures vastgelegd die het verloren gaan van informatie moet voorkomen. Ook het tegengaan van ongeoorloofd gebruik van informatie krijgt de aandacht.

3.1 Hoofdstukken

In dit handboek is dezelfde hoofdstukindeling aangehouden als in het "Informatiebeveiligingsbeleid". Deze indeling komt weer overeen met de Code voor Informatiebeveiliging. De BIG sluit ook weer aan bij de Code voor Informatiebeveiliging. Door het volgen van deze indeling, zijn enkele hoofdstuk en paragrafen (nog) niet nader beschreven of slechts heel summier.

Naast de tekst zijn ook bijlagen opgenomen. Deze bijlagen zijn zowel werkprocedures ter ondersteuning van de afspraken als bewijsstuk dat aan de eisen wordt voldaan en zijn van algemene aard. Naast deze bijlagen zijn in aparte documenten werkprocedures opgesteld.

Een verklarende woordenlijst is als bijlage in dit handboek opgenomen.

Hoe de gemeentelijke organisatie is ingericht, is te vinden op de website van de gemeente.

4. Risicobeoordeling en risicobehandeling

Voor dit hoofdstuk wordt verwezen naar het “Informatiebeveiligingsbeleid”.

5. Beveiligingsbeleid

5.1 Informatiebeveiligingsbeleid

Het Beveiligingsbeleid van de gemeente is vastgelegd in een apart document onder de naam “Informatiebeveiligingsbeleid”.
In dat document zijn de contouren van het beleid gedefinieerd. De uitwerking en de getroffen maatregelen van algemene aard zijn beschreven in dit “Algemeen Handboek Informatiebeveiliging”.
De specifieke eisen die o.a. aan basisregistraties worden gesteld, worden ook in aparte documenten voor die registratie beschreven. Een voorbeeld hiervan is het “Handboek Burgerzaken” waarin de eisen rond de BRP, de Reisdocumenten en de Rijbewijzen zijn beschreven. Voor de Basisregistratie Adressen en Gebouwen (BAG) moet dit nog gebeuren.

Voor verder invulling van dit hoofdstuk wordt verwezen naar het “Informatiebeveiligingsbeleid”.

6. Organisatie van informatiebeveiliging

Zoals eerder opgemerkt worden in dit handboek alleen de specifieke algemene beveiligingsaspecten beschreven.
De maatregelen om aan de eisen die in het “Informatiebeveiligingsbeleid” zijn gedefinieerd en nog niet of slechts gedeeltelijk zijn getroffen, zijn in het “Beveiligingsplan” opgenomen.

6.1 Interne organisatie

6.1.1 Betrokkenheid van de directie bij informatiebeveiliging

6.1.2 Coördinatie van informatiebeveiliging

6.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging

Het informatiebeveiligingsbeleid is niet een zaak voor één of meerdere individuele medewerkers. Het is een zaak van iedereen.
In het “Informatiebeveiligingsbeleid”zijn de specifieke taken nader beschreven.

6.1.4 Goedkeuringsproces voor IT-voorzieningen

6.1.5 Geheimhoudingsovereenkomst

Door elk personeel is een geheimhoudingsverklaring ondertekend.
Nieuw in diensttredende medewerkers leggen de ambtseed of – belofte af.

6.1.6 Contact met overheidsinstanties

6.1.7 Contact met speciale belangengroepen

6.1.8 Onafhankelijke beoordeling van informatiebeveiliging

6.2 Externe partijen

6.2.1 Identificatie van risico’s die betrekking hebben op externe partijen

6.2.2 Beveiliging behandelen in de omgang met klanten

6.2.3 Beveiliging in overeenkomsten met een derde partij

Zoals al in het “Informatiebeveiligingsbeleid”is aangegeven worden afspraken e.d. met derden schriftelijk vastgelegd.

7. Beheer van bedrijfsmiddelen

7.1 Verantwoordelijkheid voor bedrijfsmiddelen

7.1.1 Inventarisatie van bedrijfsmiddelen

Om alle bedrijfsmiddelen op de juiste wijze te kunnen beveiligen, is het uiteraard wel noodzakelijk te weten welke bedrijfsmiddelen er aanwezig zijn.

Naast voordelen die een accurate registratie biedt, zijn deze bruikbaar voor activabeheer en verzekeringstechnische redenen.

Automatiseringshulpmiddelen, zoals servers, PC's, laptops, beeldschermen en printers, worden in een digitaal register bijgehouden.

7.1.2 Eigendom van bedrijfsmiddelen

7.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

7.2 Classificatie van informatie

7.2.1 Richtlijnen voor classificatie

Informatie is vaak primair bedoeld om verspreid te worden. Een deel van de informatie kan een vertrouwelijk karakter hebben, waarbij dit na verloop van tijd weer verdwijnt. Door informatie op de juiste wijze te classificeren, kan door medewerkers direct beoordeeld worden hoe met deze informatie omgegaan dient te worden.

7.2.2 Labeling en verwerking van informatie

Het labelen wordt handmatig uitgevoerd. De registratie vindt plaats binnen een softwaretoepassing waarbinnen alle relevante stukken (poststukken met hun eigen nummering en archiefstukken met de juiste classificatie-code) opgenomen zijn.
De elektronische post (e-mail) wordt op dezelfde wijze behandeld als de traditionele post en wordt dus, indien relevant, ook ingeboekt.

8. Beveiliging van personeel

8.1 Voorafgaand aan het dienstverband

8.1.1 Rollen en verantwoordelijkheden

8.1.2 Screening

Veel medewerkers krijgen vertrouwelijke en/of privacygevoelige informatie onder ogen. Verwacht wordt dat hier op een integere wijze mee wordt omgegaan.

Om deze integriteit te bevorderen is de ”Nota integriteit” ingevoerd en is (wordt) aan ieder (nieuw)personeelslid uitgereikt.

Bij tijdelijk extern personeel wordt informatiebeveiliging expliciet onder de aandacht gebracht in combinatie met de ”Nota integriteit”.

8.1.3 Arbeidsvoorwaarden

Gemeentelijk personeel wordt aangesteld op basis van een benoemingsbesluit van het College van Burgemeester en Wethouders.

Ambtenaren zijn in ieder geval gebonden aan de van toepassing zijnde regels (de CAR) en regels zoals deze door de werkgever zijn opgesteld. Voorbeeld hiervan is de “Nota integriteit” die aan iedere medewerker is uitgereikt.

8.1.3.1 Arbeidscontract

In de meeste gevallen is geen sprake van een arbeidscontract maar van een benoemingsbesluit binnen de gemeente.

8.1.3.2 Tijdelijk personeel

Alle eisen, regels, procedures enz. zoals deze in dit handboek en andere handboeken en regelingen zijn opgenomen, gelden voor iedere medewerker. Zij kunnen tijdelijk in dienst zijn, op contractbasis werken of welke overeenkomst dan ook aan de aanwezigheid van een medewerker ten grondslag ligt.

8.2 Tijdens het dienstverband

8.2.1 Directieverantwoordelijkheid

8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

De bewustwording wordt gerealiseerd door ze een instructie te geven over informatiebeveiliging, gerelateerd aan de werkzaamheden en de uitwerking daarvan.

8.2.2.1 Voorlichting

Alle medewerkers zijn voorgelicht rond beveiligingszaken.

8.2.2.2 Instructie binnengemeentelijk gebruik persoonsgegevens

Alle medewerkers binnen de gemeentelijke organisatie die inzage hebben in persoonsgegevens zijn verplicht de beveiligingsaspecten serieus te nemen. Jaarlijks wordt instructie gegeven over deze aspecten en de voorwaarden van het gebruik van de persoonsgegevens. Deze instructie wordt verzorgd door de afdeling Burgerzaken.

8.2.2.3 Gedragsregels

Om allerlei problemen te voorkomen zijn gedragsregels opgesteld die voor elke medewerker binnen de organisatie gelden.

8.2.3 Disciplinaire maatregelen

Voor het college van burgemeester en wethouders is het mogelijk om disciplinaire maatregelen te nemen.

8.3 Beëindiging of wijziging van het dienstverband

8.3.1 Beëindiging van verantwoordelijkheden

8.3.2 Retournering van bedrijfsmiddelen

8.3.3 Blokkering van toegangsrechten

9. Fysieke beveiliging en beveiliging van de omgeving

9.1 Beveiliging van ruimten

Er is een duidelijke afbakening binnen de verschillende niveaus van de beveiliging. We onderscheiden: toegang tot het terrein, toegang tot het gebouw en toegang tot verschillende werkruimten.

De beveiliging is zeer minimaal. Er is sprake van een 'open gebouwen' - cultuur. De deuren staan “open” voor de mensen die op het gemeentehuis of één van de andere locaties moeten zijn.

9.1.1 Fysieke beveiliging van de omgeving

9.1.2 Fysieke toegangsbeveiliging

9.1.2.1 Gemeentehuis

9.1.2.1.1 Toegangsbeveiliging

Alle buitendeuren (behalve de hoofdingang) zijn door geautoriseerde personen te openen met behulp van een TAG.

Met behulp van deze Tag kunnen bepaalde ruimtes worden betreden.

9.1.2.1.2 Receptie voor opvang bezoekers

Er is een receptie die alle bezoekers op kan vangen. Mensen die niet weten waar zij moeten zijn melden zich bij de receptie.

9.1.2.1.3 Fysieke toegangsbeveiliging

Een bezoeker die op afspraak komt, wordt door de medewerker opgehaald en na afloop van het gesprek weer naar de uitgang begeleid.

9.1.2.2 Beveiliging in niet-publieke ruimten

9.1.2.2.1 Archiefruimte

De gemeente bewaart veel (bron)documenten, dossiers en andere zaken in een aparte archiefruimte.

9.1.2.2.2 Beveiliging van de archiefruimte

De deur van het archief is beveiligd tegen inbraak en brandvertragend.

9.1.3 Beveiliging van kantoren, ruimten en faciliteiten

9.1.3.1 Kantoren

De kantoren bevinden zich op zeven fysieke locaties die publiekelijk toegankelijk zijn via één of meerdere ingangen.

9.1.3.2 Computerruimten

De computerruimten bevinden zich op verschillende locaties.

9.1.3.3 Archiefkasten.

De officiële archiefkasten bevinden zich eveneens op verschillende locaties binnen de gebouwen van de gemeente.
De archiefkasten zijn in principe niet toegankelijk voor derden.

9.1.4 Bescherming tegen bedreigingen van buitenaf

9.1.4.1 Inbraakalarm

Het gemeentehuis is voorzien van een inbraakalarm (op basis van bewegingsdetectoren).

9.1.4.2 Brandalarm

Bij alarm is er een directe signalering naar de alarmcentrale.

9.1.4.3 Brandblusapparatuur

Het gehele gemeentehuis is voorzien van zogenaamde kleine blusmiddelen. Deze blusmiddelen staan aangegeven op het ontruimingsplan en worden éénmaal per jaar getest en onderhouden door het bedrijf dat de middelen geplaatst heeft.

9.1.4.4 Rookmelder

Het hele gemeentehuis is voorzien van rookmelders.

9.1.4.5 Bliksemafleider

Het gemeentehuis is voorzien van een bliksemafleider die voldoet aan de norm NEN 14014.

9.1.5 Werken in beveiligde ruimten

Er is geen specifiek beleid ten aanzien van het werken in beveiligde ruimten. Een ieder die toegang heeft tot deze ruimte, kan daar aan de gang.

9.1.6 Openbare toegang en gebieden voor laden en lossen

9.2 Beveiliging van apparatuur

9.2.1 Plaatsing en bescherming van apparatuur

De apparatuur wordt zodanig opgesteld dat het risico van schade en storing van buitenaf en de kansen op ongeautoriseerde toegang zo beperkt mogelijk zijn.
De pc's staan zoveel mogelijk in speciale rekken onder het bureau.

Laptops worden in een af te sluiten kast opgeborgen en zijn niet tegen misbruik beveiligd.

9.2.1.1 RAID systeem

De gemeente gebruikt een RAID systeem. Dit systeem bevat meerdere schijven. Als een schijf crasht neemt de "reserveschijf" de taken van de uitgevallen schijf over.

9.2.1.2 Computerruimte

9.2.1.2.1 Airco

De ruimten waar computerhardware (servers/patchpanel, enz.) staat zijn voorzien van één of meerdere airco’s tegen hoge temperaturen.

9.2.1.2.2 Stroomvoorziening

De gemeente beschikt over een UPS (Uninteruptible Power Supply) systeem, dit is te vergelijken met een kleine accu. Dit systeem vangt de stroomtoevoer naar de servers minimaal 15 minuten op bij stroomuitval. Alle servers zijn aan deze UPS gekoppeld.

9.2.1.2.3 Noodaggregaat

Het gemeentehuis is voorzien van een noodaggregaat. Dit noodaggregaat schakelt automatisch in indien de netspanning wegvalt en voorziet, met uitzondering van enkele minder belangrijke apparaten, het hele gemeentehuis van stroom.

9.2.2 Nutsvoorzieningen

9.2.3 Beveiliging van kabels

Stroomvoorziening, netwerkkabels en telefoonkabels zijn weggewerkt in kabelgoten in de vloeren en goten boven de plafonds. In de looproutes mogen geen kabels los over de vloer liggen.

Alleen aansluitingen die daadwerkelijk gebruikt worden zijn gepatched. Er wordt een patch-administratie bijgehouden. Hierdoor is het niet mogelijk aansluitingen oneigenlijk te gebruiken.

9.2.4 Onderhoud van apparatuur

Er zijn geen contracten om de apparatuur jaarlijks te laten inspecteren en schoon te laten maken door een gespecialiseerd bedrijf.

9.2.4.1 Onderhoudscontract

Voor de servers is een onderhoudscontract afgesloten. Dit is een 4 uurs contract.

9.2.5 Beveiliging van apparatuur buiten het terrein

In een aantal gevallen hebben medewerkers toestemming van hun afdelinghoofd om thuis op een laptops van de gemeente te werken. Door het Nieuwe Werken (flexwerken, HNW) neemt dit aantal toe. Ook smartphones en tablets worden steeds meer gebruikt.

Laptops moeten in een daartoe beschermende tas worden vervoerd.

9.2.5.1 Het verplaatsen of uitlenen van bedrijfseigendommen

Alle automatiseringsapparatuur die op de werkplek staat opgesteld, mag alleen door of na toestemming van automatiseringspersoneel verplaatst worden.

9.2.6 Veilig verwijderen of hergebruik van apparatuur

9.2.7 Verwijdering van bedrijfseigendommen

10. Beheer van communicatie- en bedieningsprocessen

Het doel van communicatie- en bedieningsprocessen is het garanderen van een correcte en veilige bediening en beheer van ICT-voorzieningen.

Het dagelijks beheer van de server (backups etc.) wordt uitgevoerd door systeembeheer. Voor grotere beheerswerkzaamheden is een contract gesloten met een externe partij.

10.1 Bedieningsprocedures en verantwoordelijkheden

10.1.1 Gedocumenteerde bedieningsprocedures

Voor het naleven van instructies ten aanzien van apparatuur en programmatuur, dienen deze gedocumenteerd en onderhouden te worden. Deze documenten hebben geen formele status.

Van (werk)procedures dient een compleet exemplaar bij het afdelingshoofd aanwezig te zijn.

10.1.2 Wijzigingsbeheer

Er zijn geen formele afspraken voor het beheren van wijzigingen.
Installaties, updates en wijzigingen die verder gaan dan een enkele gebruiker, worden alleen uitgevoerd als er twee systeembeheerders aanwezig zijn. Dit ter voorkoming van problemen in de combinatie van wijzigingen en onderbezetting.

10.1.2.1 Versiebeheer software

De afdeling ICT houdt van alle documentatie (en applicaties) de versies en bijzonderheden bij.

10.1.2.2 Software documentatie

Bij programma-updates beoordeelt de applicatiebeheerder de doorgevoerde programmawijzigingen.

10.1.2.3 Procedure van update programma's en handleidingen

Er zijn diverse procedures vastgelegd omtrent het updaten van systemen en applicaties. In deze procedures is ook het update van handleidingen verwerkt. Voor het updaten van systemen is systeembeheer verantwoordelijk.

10.1.2.4 Actualisatie handleidingen

De digitale handleidingen van de programmatuur worden geactualiseerd zodra een nieuwe versie beschikbaar is.

10.1.3 Functiescheiding

Op cruciale punten is functiescheiding aangebracht. Hieronder staat kort vermeld op wat voor gebied en op welke wijze dit gerealiseerd is.

10.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie

De productieomgeving dient fysiek gescheiden te zijn van de voorzieningen voor testdoeleinden.
Voor de testomgeving geldt uiteraard een andere inlogcode dan voor de productieomgeving.

10.2 Beheer van dienstverlening door een derde partij

Er wordt gebruik gemaakt van diensten door derden (bijv. Centric en Pinkroccade). Voor

deze medewerkers dient er (afhankelijk van de werkzaamheden) een inlogcode met wachtwoord beschikbaar te zijn.

10.2.1 Dienstverlening

10.2.1.1 Uitbesteding

Uitbesteding kan op verschillende manieren zijn vorm krijgen. Dit kan zijn voor korte tijd of zelfs permanent.

In Bewerkerovereenkomsten en contracten zijn de door de bewerkers de uit te voeren taken vastgelegd.

10.2.2 Controle en beoordeling van dienstverlening door de derde partij

10.2.3 Beheer van wijzigingen in dienstverlening door een derde partij

10.3 Systeemplanning en acceptatie

10.3.1 Capaciteitsbeheer

De capaciteit valt uiteen in een aantal facetten binnen verschillende deelgebieden.
Voor alle servers zijn van cruciaal belang:

1. capaciteit processor;
2. hoeveelheid intern geheugen;
3. hoeveelheid vrije schijfruimte.

10.3.2 Systeemacceptatie

Voor de acceptatie van nieuwe soft- en hardware is geen vaste testomgeving aanwezig.

Op verzoek van de applicatiebeheerder kan een testomgeving worden aangemaakt.

10.4 Bescherming tegen virussen en ‘mobile code’

10.4.1 Maatregelen tegen virussen

De gemeente heeft een licentie op het virus detectieprogramma McAfee. Elke nieuwe versie wordt dagelijks automatisch naar de gemeente verzonden en direct automatisch geïnstalleerd. Deze virusscanner draait constant.

10.4.1.1 Weigering van met virus besmette media

Media die geïnfecteerd zijn met een virus worden niet gebruikt. Ook niet wanneer het officiële media betreft van softwareleveranciers c.q. instanties.

10.4.2 Maatregelen tegen ‘mobile code’

De gemeente maakt gebruikt van antivirus software van McAfee. Deze sofware scant al het mogelijk inkomende verkeer op servers en pc's, variërend van cd’s in randapparatuur, USB, aanwezige software en bestanden op schijven, binnenkomende e-mails met bijlagen en internetverkeer dat binnenkomt.

10.5 Back-up

Beveiliging heeft in dit geval betrekking op de diverse gebruikersapplicaties en de systeemapplicaties. Hierbij moet rekening gehouden worden met het feit dat iedereen met de systeemapplicaties werkt zodat deze applicaties op het gehele gemeentehuis beveiligd moeten worden. Daarnaast is er sprake van beveiligingsmaatregelen van documentatie van software.

10.5.1 Reservekopieën maken (back-ups)

Als waarborg van de continuïteit wordt naast een tapeback-up ook een back-upsysteem actueel gehouden.
Met een hoge frequentie wordt het back-upsysteem geactualiseerd. Bij een eventuele calamiteit is daardoor slechts een gering verlies van informatie.

10.6 Beheer van netwerkbeveiliging

10.6.1 Maatregelen voor netwerken

De operationele verantwoordelijkheid voor het netwerk ligt bij de systeembeheerders. De systeembeheerders houden een registratie bij van alle poorten op routers en switches.

10.6.2 Beveiliging van netwerkdiensten

10.7 Behandeling van media

10.7.1 Beheer van verwijderbare media

Media die binnen de gemeente niet langer benodigd zijn (denk aan tapes van een buiten gebruik gestelde tape-unit) dienen op verantwoorde wijze buiten gebruik worden.

10.7.2 Verwijdering van media

In dit document zijn de afspraken over het afvoeren van media beschreven. Hierdoor is voor een ieder inzichtelijk welke regels hiervoor gelden.

10.7.2.1 Vervanging

Een tape mag bij regelmatig en frequent gebruik (meer dan 12 maal per jaar) maximaal één jaar gebruikt worden.

10.7.2.2 Vernietiging oude media

Niet meer te gebruiken back-up tapes worden ter vernietiging aangeboden aan de afdeling Interne Zaken. Zij verzamelen de tapes en zodra er voldoende exemplaren zijn worden deze door een gespecialiseerd bedrijf vernietigd.

10.7.3 Procedures voor de behandeling van informatie

10.7.3.1 Opslag media in kluis intern

Om verlies van data te voorkomen worden alle back-ups bewaard in de beveiligde kluis.

10.7.3.2 Opslag media in kluis extern

Naast opslag van back-ups in de kluis op de afdeling Interne Zaken, wordt er één keer in de week een (full) back-up van de vrijdagtape extern bewaard.

10.7.4 Beveiliging van systeemdocumentatie

10.7.4.1 Procedures

De procedures ten aanzien van het beheer van de systemen, applicaties en gegevens/informatie, zijn in ordners verzameld en staan in een grote afsluitbare kast.

10.8 Uitwisselen van informatie

10.8.1 Beleid en procedures voor informatie-uitwisseling

10.8.2 Uitwisselingsovereenkomsten

Uitwisseling van informatie, anders dan de reguliere aanlevering van gegevens zoals het BRP-berichtenverkeer en SUWI, vindt enkel en alleen plaats na beoordeling van de aanvrager.

10.8.3 Fysieke media die worden getransporteerd

Voor het transport van media kent de gemeente verschillende vormen bijv.:

1. Transport van media door systeembeheerders
2. Transport tapes door medewerkers Burgerzaken

10.8.4 Elektronische berichtenuitwisseling

Er worden enkele digitale (of elektronische) diensten via de website aangeboden. Hierbij wordt voor de authenticatie gebruik gemaakt van DigiD en andere wettelijk toegelaten middelen. Voorbeelden hiervan zijn eHerkenningen en DigiD-machtigingen.

10.8.4.1 Beveiligingsrisico's

Berichten in de persoonlijke postbus zijn alleen voor de medewerker toegankelijk.

Als een e-mail fout is geadresseerd krijgt de afzender automatisch een bericht dat de mail niet kan worden bezorgd.
Gelijktijdig met de verkrijging tot e-mailfaciliteiten wordt aan alle (nieuwe) medewerkers en bestuurders een introductiepakket met daarin de gedragsregels voor internet en e-mail uitgereikt.

10.8.4.2 Beleid ten aanzien van elektronische post

Alle binnenkomende e-mail wordt eerst gecontroleerd op schadelijke virussen, scripts en andere gevaren. Indien deze aanwezig zijn, worden deze automatisch verwijderd en krijgen systeembeheer en de ontvanger daar een bericht van.

Officiële opdrachten mogen niet per e-mail verstrekt worden. Dit geschiedt met de traditionele standaardbrief. In de disclaimer van een e-mail staat vermeld dat het bericht in verband met het ontbreken van een rechtsgeldige handtekening geen rechtsgeldig karakter kent.

10.8.5 Systemen voor bedrijfsinformatie

Voor de elektronische kantoorsystemen is een nog niet vastgesteld beleid in gebruik.
Met betrekking tot elektronische kantoorsystemen zijn er geen aanvullende zaken noodzakelijk.

10.9 Diensten voor e-commerce

Sinds oktober 2001 wordt binnen de gemeente gebruik gemaakt van e-mailfaciliteiten. Voor het gebruik van e-mail is er een protocol opgesteld.

10.9.1 E-commerce

10.9.2 Onlinetransacties

10.9.3 Openbare beschikbare informatie

De gemeente beschikt over een eigen website. Deze website wordt extern gehost. Doordat hosting bij een externe partij plaats vindt, hoeft de gemeente niet direct te voorzien in een regeling waardoor 24-uurs continuïteit wordt gewaarborgd van de website. Via de website is geen directe toegang mogelijk tot de systemen.

10.10 Controle

10.10.1 Aanmaken audit-logbestanden

10.10.2 Controle op systeemgebruik

Er vindt geen monitoring van het systeemgebruik plaats. Medewerkers kunnen enkel toepassingen gebruiken en informatie raadplegen waartoe zij expliciet geautoriseerd zijn.

10.10.3 Bescherming van informatie in logbestanden

De netwerkbesturingssysteem (Novell Server) biedt geen mogelijkheden om uitzonderingen vast te leggen in een logboek (zgn. audittrail). Ook bij belangrijke applicaties ontbreekt deze functionaliteit.

10.10.4 Logbestanden van administrators en operators

Er worden logboeken bijgehouden van de werkzaamheden die op de systemen uitgevoerd worden.

Deze logboeken worden eenmaal per kwartaal gecontroleerd. En er wordt gerapporteerd aan het hoofd van de afdeling I&A.

10.10.5 Registratie van storingen

Alle soorten meldingen (hard- en software, gebruiker en systeembeheer, intern en extern) zijn in 1 systeem ondergebracht. Dit ene systeem is nu het programma TOPdesk.

10.10.6 Synchronisatie van systeemklokken

11. Toegangsbeveiliging

11.1 Bedrijfseisen ten aanzien van toegangsbeheersing

De toepassingen kennen een aantal groepen van gebruikers, die ieder specifieke eisen om toegang tot informatie stellen.

Gebruikers krijgen niet meer informatie dan nodig is voor de uitoefening van de functie. Een applicatiebeheerder krijgt het gehele pakket tot zijn beschikking.

Rekening wordt gehouden met de diverse classificaties aan informatie. Voor toegang tot het netwerk wordt een inlogcode aangevraagd. Met deze code krijgt men toegang tot de basisuitrusting aan software.

11.1.1 Toegangsbeleid

Onder de logische toegang wordt verstaan de toegang hebben tot niet tastbare opgeslagen informatie. Hierbij dient gedacht te worden aan toegang tot informatiesystemen en databases.

11.1.1.1 Regels voor toegangsbeveiliging

Medewerkers krijgen alleen toegang tot het netwerk en onderdelen daarvan, indien dit expliciet is aangevraagd. Niet aangevraagd is geen toegang. De autorisatieformulieren worden gearchiveerd bij het hoofd afdeling I&A.

11.1.2 Huisregels en Gedragscode

Huisregels zijn een middel om de rust binnen het gebouw en de veiligheid van de werknemers te waarborgen. Bezoekers en medewerkers van het Gemeentehuis dienen de huisregels in acht te nemen. Uiteraard dienen de huisregels niet al te rigide worden toegepast. Als iemand het Gemeentehuis alleen maar bezoekt omdat het buiten stortregent dan is dat in strijd met de huisregels. Maar om iemand om die reden naar buiten te jagen is ook niet nodig.

11.2 Beheer van toegangsrechten van gebruikers

11.2.1 Registratie van gebruikers

Toegang tot het netwerk en informatiesystemen wordt door de leidinggevende aangemeld via een aanmeldingsformulier. Het formulier wordt door de leidinggevende ondertekend. Als toegang tot applicaties nodig is worden deze applicaties beschikbaar gesteld. De aanvraag wordt doorgestuurd naar de applicatiebeheerders, die afhankelijk van de gewenste rollen rechten toekennen.

Alle relevante onderdelen waarvoor een autorisatie nodig is, worden via een autorisatie/aanvraagformulier aangevraagd.

Een gebruiker kan een (tijdelijk) medewerker zijn, een stagiair of een ingehuurde kracht.

Bij ontbreken van de handtekening van de leidinggevende wordt het formulier niet in behandeling genomen. Om in geval van ziekte en/of langdurig verlof verstoringen te voorkomen, kan de leidinggevende worden vervangen door de betreffende waarnemer.

11.2.2 Beheer van speciale bevoegdheden

Alleen de systeembeheerders kunnen als administrator (hoogste niveau) op de server komen. Voor medewerkers beperkt de toegang zich tot de pc, de persoonlijke map op het

netwerk, de afdelingsmap op het netwerk en de toegewezen en geautoriseerde applicaties met bijbehorende data.

11.2.3 Beheer van gebruikerswachtwoorden

De afdeling ICT maakt naar aanleiding van een autorisatieverzoek een gebruikerscode aan, met een eenmalig te gebruiken wachtwoord. Aan deze gebruikerscode zijn op systeemniveau rechten gekoppeld die toegang tot applicaties geeft. Vervolgens verleent de applicatiebeheerder binnen de applicatie en op onderdeelniveau toegang.

Systeembeheer heeft geen inzage in de wachtwoorden van de gebruikers. De enige mogelijkheid die systeembeheer heeft om de inlogcode van een medewerker open te breken, is het wachtwoord te verwijderen en er een nieuw initieel wachtwoord toe te kennen.

11.2.3.1 Vergeten wachtwoorden

Als een gebruiker zijn wachtwoord vergeten is en drie keer een foutief wachtwoord heeft ingevuld, wordt zijn account geblokkeerd. De gebruiker moet dit melden bij zijn leidinggevende.

11.2.4 Beoordeling van toegangsrechten van gebruikers

Ieder kwartaal worden alle autorisaties gecontroleerd.
Bij onregelmatigheden vindt overleg met het afdelingshoofd plaats over:

- mogelijke gevolgen van de ongeautoriseerde toegang;
- mogelijke maatregelen ter voorkoming van herhaling.

De personen die bovengenoemde controles uitvoeren zijn respectievelijk de applicatiebeheerders, privacybeheerder BRP, de controller en het hoofd afdeling I&A. De procedure dient nog opgesteld en formeel vastgesteld te worden.

11.3 Verantwoordelijkheden van gebruikers

11.3.1 Gebruik van wachtwoorden

De gebruiker is zelf verantwoordelijk voor de inlogcode en het bijbehorende wachtwoord en is strikt persoonlijk. Mocht een derde (intern of extern) de inlogcode gebruiken en/of misbruiken, dan blijft de medewerker verantwoordelijk. Het is pertinent niet toegestaan om log-in namen en/of wachtwoorden aan anderen te verstrekken.

Inlogcodes en wachtwoorden mogen niet op notitieblaadjes bij de pc in de buurt liggen of op een white-board vermeld staan. Indien dit toch gebeurt, zal dat wachtwoord worden geblokkeerd.

11.3.2 Onbeheerde gebruikersapparatuur

Ook op andere momenten kan misbruik gemaakt worden van de gebruikerscode en het bijbehorende wachtwoord.

Zodra een gebruiker zijn werkplek verlaat, dient hij de pc te blokkeren zodat opnieuw aangemeld moet worden.

11.3.3 ‘Clear desk’- en ‘clear screen’-beleid

Het eenvoudigste medium waarop informatie zich bevindt, is papier. Iedere dag moeten de bureaus leeggeruimd zijn en papieren in een afsluitbare kast of lade opgeborgen worden. Met name vertrouwelijke documenten moeten altijd buiten handbereik worden opgeborgen. Er mogen geen gegevensdragers met persoonsgegevens onbeheerd worden achtergelaten

op algemeen toegankelijke plaatsen (bijv. bureaus, printers, faxapparaten, etc.).

11.3.3.1 Screensaver

De beeldschermen zijn voorzien van een screensaver. Na 15 minuten treedt de screensaver in werking en moet, om weer met het beeldscherm te kunnen werken, opnieuw het wachtwoord ingevoerd worden

11.4 Toegangsbeheersing voor netwerken

Iedere medewerker kan gebruik maken van de basisfunctionaliteit van een pc binnen de gehele organisatie. Alleen voor toepassing die cliënt-software nodig hebben, geldt dat deze toepassingen slechts vanaf de eigen pc (of een pc die met dezelfde toepassing werkt) te benaderen zijn.

11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten

11.4.2 Authenticatie van gebruikers bij externe verbindingen

De enige manier waarlangs derden toegang tot het systeem kan verkrijgen, is via een modem. Dit modem wordt na toestemming c.q. op verzoek van systeembeheer aangezet.

Alleen voor de systeembeheerders is het via dit modem mogelijk om in te bellen.

11.4.2.1 Node-authenticatie

Om op een systeem binnen te kunnen komen, is een gebruikersnaam en een geldig wachtwoord nodig. Deze gegevens zijn, zij het moeilijk, te kraken of via zogenaamd “snifferen” te achterhalen.

11.4.3 Identificatie van netwerkapparatuur

Een pc en de achterliggende infrastructuur kunnen pas gebruikt worden nadat een gebruiker zich heeft aangemeld op het netwerk.

11.4.4 Bescherming op afstand van poorten voor diagnose en configuratie

Diagnosepoorten zijn niet aanwezig.

11.4.4.1 Externe toegang

Het inloggen op het netwerk vanaf een computer van buiten de organisatie is mogelijk.

Beveiligde externe toegang via Gemnet, voor bijvoorbeeld de leverancier van het BRP-systeem. De externe datacommunicatie verloopt via een andere server dan waar de BRP is geïnstalleerd.

11.4.4.2 Werkplekidentificatie

Aan elke werkplek is een unieke identificatie toegekend. Via deze identificatie kan worden gelokaliseerd vanaf welke werkplek toegang is verkregen tot het netwerk.

11.4.5 Scheiding van netwerken

11.4.6 Beheersmaatregelen voor netwerkverbindingen

Gebruikers mogen alleen toegang krijgen tot die delen van het netwerk waar de te gebruiken toepassingen en gegevens staan. In de Windows-verkenner worden alleen de mappen van

de eigen pc alsmede de persoonlijke map op netwerk en de afdelingsmap weergegeven. Een gebruiker kan e-mail naar alle interne en externe adressen (individu of afdeling) sturen. De systemen zijn standaard op de volgende tijden opengesteld voor gebruik:

Maandag tot en met vrijdag	van 06.00 uur tot 20.00 uur
Donderdag	van 06.00 uur tot 22.00 uur

Medewerkers met toegang tot het netwerk buiten deze tijden zijn aangewezen bij B&W-besluit. Incidenteel overwerk kan dezelfde dag tot 16.00 uur schriftelijk (memo of e-mail) aangekondigd worden bij automatisering zodat zij een eenmalige wijziging in de openingstijd kunnen doorvoeren.

11.4.7 Beheersmaatregelen voor netwerkroutering

Iedere pc, server, switch en printer heeft een unieke identificatie binnen het netwerk. Apparatuur die ongevraagd in het netwerk wordt geplaatst, wordt niet toegelaten.

11.5 Toegangsbeveiliging voor besturingssystemen

11.5.1 Beveiligde inlogprocedures

Elke computer is beveiligd met een logische toegangsbeveiliging op het Novell netwerk.

De regels m.b.t. (vergeten) wachtwoorden staan elders in dit document beschreven.

11.5.2 Gebruikersidentificatie en –authenticatie

Iedere medewerker is te allen tijde voor zijn persoonlijke inlogcode verantwoordelijk. Het betalingsverkeer is extra beveiligd. Hiervoor dienen de geautoriseerde medewerkers hun smartcard te gebruiken.

11.5.3 Systemen voor wachtwoordbeheer

Er wordt gebruik gemaakt van de standaard-systematiek om de wachtwoorden te beheren. Iedere gebruiker moet:

- het wachtwoord binnen 59 dagen wijzigen;
- een oud wachtwoord niet herhaald gebruiken;
- direct een initieel uitgedeeld wachtwoord wijzigen in een persoonlijk wachtwoord.

Rekening houden dat blokkering optreedt na driemaal foutief aanmelden en dat de lengte van wachtwoorden minimaal 8 karakters lang is.

11.5.4 Gebruik van systeemhulpmiddelen

11.5.5 Time-out van sessies

De pc's zijn uitgerust met een Screensaver.

11.5.5.1 Aanmelden

Als algemene regel geldt dat iedere gebruiker zich maar op één pc tegelijk kan inloggen. Indien het noodzakelijk is dat een gebruiker meer aansluitingen heeft, wordt dit door de betreffende leidinggevende aangevraagd.

11.5.5.2 Afmelden

De regel is dat een gebruiker zijn pc locked als hij zijn werkplek verlaat. Als hij het gebouw verlaat moet hij zich afmelden en de pc afsluiten.

11.5.6 Beperking van verbindingstijd

11.6 Toegangsbeheersing voor toepassingen en informatie

Er is rekening gehouden met maatregelen die voortvloeien uit de Wet bescherming persoonsgegevens (Wbp).

Elke binnendienst medewerker van de gemeente heeft de beschikking over een op het netwerk aangesloten pc. Om de op de systemen opgeslagen data te beveiligen tegen ongewenste toegang, niet in de laatste plaats omdat er binnen de gemeente met privacy gevoelige gegevens van derden (bijv. van burgers) wordt gewerkt, is een vorm van beveiliging tegen ongeautoriseerde toegang verplicht.

11.6.1 Beperken van toegang tot informatie

Een medewerker verkrijgt met gebruik van de persoonlijk toegangscode en bijbehorend wachtwoord toegang tot de netwerkfaciliteiten en applicatie. Door deze combinatie zijn de rechten van de gebruiker bekend en wordt het persoonlijke menu aangeboden met daarin de geautoriseerde programma's. Toepassingen tot privacygevoelige gegevens vereisen nogmaals een aanmelding op basis van toegangscode en wachtwoord.

11.6.2 Isoleren van gevoelige systemen

Aan medewerkers worden rechten verleend (autorisaties) op basis van de werkzaamheden die zij moeten verrichten, en de afdeling waarop zij werkzaam zijn. De afdeling ICT verleent deze rechten op netwerkniveau op basis van een aanvraag van de verantwoordelijke leidinggevende van de desbetreffende afdeling. Aanvraagformulieren worden gearchiveerd.

11.7 Draagbare computers en telewerken

11.7.1 Draagbare computers en communicatievoorzieningen

De gemeente maakt gebruik van laptops en iPADs. De laptops worden veelal gebruikt ter ondersteuning, bijv. in combinatie met een beamer bij rampenbestrijding.

Het aanmelden op een laptop geschiedt op dezelfde wijze als in het netwerk (zelfde toegangscode). Bij het opstarten en afsluiten van een laptop vindt er geen synchronisatie van de bestanden plaats.

De antivirusbescherming is op alle laptop volledig geïnstalleerd en bij aanmelding in het netwerk wordt informatie over eventueel afgevangen virussen aan de centrale database doorgegeven.

11.7.2 Telewerken

Alle medewerkers kunnen via Citrix ook telewerken. Vooralsnog zijn alleen de kantoorapplicaties (Word, Excel, Powerpoint en de mail en agenda) vrijgegeven.

12. Verwerving, ontwikkeling en onderhoud van informatiesystemen

Voor dit hoofdstuk wordt vooralsnog verwezen naar het “Informatiebeveiligingsbeleid”.

12.1 Beveiligingseisen voor informatiesystemen

12.1.1 Analyse en specificatie van beveiligingseisen

12.2 Correcte verwerking in toepassingen

12.2.1 Validatie van invoergegevens

12.2.2 Beheersing van interne gegevensverwerking

12.2.3 Integriteit van berichten

12.2.4 Validatie van uitvoergegevens

12.3 Cryptografische beheersmaatregelen

12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen

12.3.2 Sleutelbeheer

12.4 Beveiliging van systeembestanden

12.4.1 Beheersing van operationele programmatuur

12.4.2 Bescherming van testdata

12.4.3 Toegangsbeheersing voor broncode en programmatuur

12.5 Beveiliging bij ontwikkelings- en ondersteuningsprocessen

12.5.1 Procedures voor wijzigingsbeheer

12.5.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem

12.5.3 Restricties op wijzigingen in programmatuurpakketten

12.5.4 Uitlekken van informatie

12.5.5 Uitbestede ontwikkeling van programmatuur

12.6 Beheer van technische kwetsbaarheden

12.6.1 Beheersing van technische kwetsbaarheden

13. Beheer van informatiebeveiligingsincidenten

13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen

Beveiligingsincidenten dienen zo snel mogelijk te worden gerapporteerd via de juiste kanalen.

Incidenten waarbij inbreuk wordt gemaakt op privacy of waarbij informatie en/of gegevens(dragers) verminkt raken, worden zo spoedig mogelijk gemeld bij het eigen afdelingshoofd. Inbreuk op de privacy van de burgers wordt tevens gemeld aan de privacybeheerder BRP.

13.1.1.1 Het rapporteren van onvolkomenheden in de software

Zodra een gebruiker onvolkomenheden in software ontdekt (dit kan zich uiten in bijvoorbeeld foutmeldingen, maar ook het presenteren van de verkeerde gegevens), dient dit aan de (in)formele applicatiebeheerder gemeld te worden. De applicatiebeheerders dienen de problemen zo gedetailleerd mogelijk te documenteren en dit bij de afdeling ICT te melden.

13.1.2 Rapportage van zwakke plekken in de beveiliging

Een enkele keer per jaar wordt melding gedaan door medewerkers die op basis van op- of aanmerkingen (vaak onbedoeld) een zwakke plek in de beveiliging bloot leggen. Het melden van vermeende zwakke plekken wordt gerapporteerd aan de beveiligingsbeheerder.

13.2 Beheer van informatiebeveiligingsincidenten en –verbeteringen

13.2.1 Verantwoordelijkheden en procedures

Bij een systeemstoring (netwerk en/of servers) dient binnen een uur zicht te zijn op een werkende oplossing. Indien dit niet haalbaar is wordt het hoofd van de afdeling I&A geïnformeerd en zo nodig de noodprocedure gestart.
Zie verder het separate Noodplan.

Bij incidenten dient er zoveel mogelijk bewijsmateriaal (schermprint etc) verzameld te worden om e.e.a. achteraf te analyseren. Aanbevolen wordt het gehele incidentenbeheer en -management verder uit te bouwen.

13.2.1.1 Agressieprotocol

Medewerkers van de gemeente kunnen te maken krijgen met agressie. Agressie bestaat in vele vormen: van verbaal geweld, dreiging met lichamelijk geweld tot daadwerkelijk geweld. Om agressie te herkennen, te voorkomen en maatregelen te treffen is de “Beleidsnotitie Agressie & Geweld” vastgesteld.

13.2.1.2 Vertrouwenspersoon

Indien medewerkers bedreigd worden of vinden dat ze onder druk gezet worden door andere personen (bijvoorbeeld criminelen) kunnen zij, als zij dit willen, dit uiten bij het hoofd afdeling P&O of de secretaris. Voor afhandeling van de zaak wordt de “Beleidsnotitie Agressie & Geweld” gevolgd.

13.2.1.3 Incidenten registratie

Indien incidenten geconstateerd worden rond de integriteit, continuïteit, exclusiviteit of controleerbaarheid van vastgelegde informatie, wordt dit gemeld bij het afdelingshoofd.

13.2.1.4 Instructies m.b.t. handelen bij een overval

Er is een is overvalinstructie. Iedere medewerkers die direct klantencontact heeft is hiervan op de hoogte.

13.2.2 Leren van informatiebeveiligingsincidenten

In een aantal gevallen zal op basis van een incident een aanpassing plaats vinden, hetzij procedureel, hetzij softwarematig. Er is nog geen mechanisme beschikbaar waarbij het mogelijk is om terug te gaan zoeken in de historie van alle meldingen die gemeentebreed zijn gedaan.

13.2.3 Verzamelen van bewijsmateriaal

Er wordt een registratie van het internetbezoek bij gehouden.
In het kader van de privacy wetgeving zijn daarin twee essentiële zaken van belang:

- de medewerker weet (door ondertekening verklaring) dat het internetbezoek geregistreerd wordt;
- de registratie vindt automatisch en anoniem plaats.

Pas bij gegronde reden kan, enkel met toestemming van de gemeentesecretaris, gericht gezocht worden en kan de registratie op naam gesteld worden ten einde bewijsmateriaal voor onrechtmatig gebruik of voor overtreding van de regels aan te tonen. Voor details inzake deze regeling wordt verwezen naar het voorbeeld reglement van de VNG.

14. Bedrijfscontinuïteitsbeheer

14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Elke organisatie kan te maken krijgen met onvoorziene calamiteiten, zoals brand, waterschade of ernstige computerstoringen. Dergelijke calamiteiten kunnen er voor zorgen dat de bedrijfsvoering moet worden onderbroken. In het ernstigste geval komt de continuïteit van een organisatie in gevaar.

14.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer

De continuïteit kan op verschillende manieren verstoord worden. Niet alleen de wijze van verstoring is van belang. Minstens zo belangrijk is het om de waarschijnlijkheid van het voorkomen van de verstoring (= risico) in te schatten. Daarnaast spelen ook mogelijke gevolgen een grote rol.

Op basis van prioriteiten zijn procedures beschreven om de risico's te beperken (maatregelen, kosten, inspanning). Voor iedere situatie is beschreven welke handelingen verricht worden, welke medewerkers erbij betrokken zijn en binnen welke termijn bepaalde aspecten uitgevoerd moeten zijn.

14.1.2 Bedrijfscontinuïteit en risicobeoordeling

Om oplossingen aan te kunnen bieden moet de oorzaak van de onderbrekingen (brand, wateroverlast etc.) gespecificeerd worden. Na het beschrijven van de gebeurtenis wordt een risicoanalyse uitgevoerd zodat vastgesteld kan worden wat de gevolgen van een onderbreking in de bedrijfsprocessen zijn. In dit proces worden altijd de proceseigenaren betrokken samen met de eigenaren van de middelen.

Let wel: processen en informatievoorziening reiken verder dan enkel automatisering!

14.1.3 Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging

Om de verstoorde processen zo snel mogelijk weer op gang te brengen/ te herstellen, moeten voor alle voorkomende risico's met prioriteit, continuïteitsplannen geschreven worden. Alle verantwoordelijkheden en procedures zoals genoemd in de continuïteitsplannen worden formeel goedgekeurd en vastgesteld door college van burgemeester en wethouders. Alle overeengekomen procedures worden gedocumenteerd. Over wijzigingen dient gerapporteerd te worden. Aangezien de omgeving waarbinnen gewerkt wordt continu in beweging is, worden de plannen periodiek getest en geactualiseerd. Regelmatig worden passende trainingen gehouden. Dit alles dient binnen het plan beschreven te worden.

De nadruk binnen deze continuïteitsplannen ligt op het zo spoedig mogelijk herstellen van de verstoorde processen. Om de continuïteit van de reguliere dienstverlening en processen te waarborgen is er een "Noodplan" vastgesteld.

14.1.4 Kader voor de bedrijfscontinuïteitsplanning

Er worden meerdere continuïteitsplannen opgeleverd. Ieder plan sec is gericht op een bepaalde soort verstoring op basis van de risicoanalyse of het zo spoedig mogelijk herstellen van een verstoord proces.

Onderdelen van de continuïteitsplannen zijn onder andere de randvoorwaarden waarbinnen

gehandeld wordt (wanneer treedt een plan inwerking), welke acties worden uitgevoerd in geval van incidenten, acties ten behoeve van uitwijk, momenten van toetsing procedures, verantwoordelijkheden, onderhoud en evaluatie.

14.1.5 Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen

Om de plannen zo dicht mogelijk bij de realiteit te houden, is het noodzakelijk om deze zeer regelmatig te testen. Bij essentiële wijzigingen op onderdelen binnen het plan wordt het plan aangepast. Tevens wordt getest of de beschrijving van de werking nog correct is. Wijzigingen die van invloed zijn, zijn o.a. wijzigingen in apparatuur of toepassing, wijzigingen in personeel (nieuwe functionaris, gewijzigde functies), andere werkwijze.

Na uitvoering van een test wordt een evaluatierapport opgesteld. Op basis van de bevindingen kan dan vervolgens de procedure of het plan bijgesteld worden. Om de actualiteit van de plannen te garanderen is het essentieel om met versiebeheer te werken.

Om na calamiteiten een goede werking te kunnen waarborgen is het noodzakelijk te zorgen voor goede back-up en herstel procedures.

14.1.5.1 Uitwijktest

Deze jaarlijkse test wordt uitgevoerd als onderdeel van de uitwijkprocedure.

De bevindingen van deze test worden gerapporteerd door de systeembeheerder aan het management.

14.1.5.2 Terugplaatsen back-up

Deze jaarlijkse test is vergelijkbaar met de uitwijktest, maar wordt uitgevoerd op het eigen computersysteem.

De bevindingen van deze test worden gerapporteerd door de systeembeheerder aan het management.

14.1.5.3 Mutatiereconstructie

Om een goed oordeel over de reconstructie te kunnen geven worden na het terugplaatsen van de back-up de mutaties gereconstrueerd. In de applicatiegerichte handboeken zijn nadere instructies beschreven.

14.1.6 Uitwijk

Er is een uitwijkovereenkomst gesloten met een externe partij.

14.1.6.1 Uitwijkplan

Het uitwijkplan (ook wel noodplan genoemd) is beschreven in een separaat document.

15. Naleving

15.1 Naleving van wettelijke voorschriften

De werkzaamheden van de gemeente vallen (uiteraard) volledig binnen wettelijke kaders.

15.1.1 Identificatie van toepasselijke wetgeving

15.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)

Om recht te doen aan de eigendomsrechten, ligt alle originele software opgeborgen op de afdeling I&A. Dit is alleen van toepassing voor de software die op fysieke informatiedragers is ontvangen. Meer en meer wordt software via internet beschikbaar gesteld.

15.1.3 Bescherming van bedrijfsdocumenten

Een groot aantal documenten kent een wettelijke bewaarplicht. Hiertoe zijn diverse archieven ingericht. De beveiliging van deze ruimten is ook in dit handboek beschreven.

De digitale gegevens zijn als data op één van de servers opgeslagen. De persoonlijke data van de gebruiker wordt ook op een van de servers opgeslagen.

15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens

De bescherming van persoonsgegevens valt in Nederland onder het juridische kader van de Wet Bescherming Persoonsgegevens (WBP). De gemeente heeft op basis van haar wettelijke verplichting daartoe een “Handboek Burgerzaken” opgesteld dat goedgekeurd is door het college van burgemeester en wethouders.

In dit handboek staan de procedures beschreven die in verschillende situaties gehanteerd worden en welke functionaris welke verantwoordelijkheid heeft.

15.1.5 Voorkomen van misbruik van IT-voorzieningen

Alle automatiseringsmiddelen (zowel apparatuur als toepassingen) die beschikbaar zijn gesteld aan de medewerkers, worden geacht te worden gebruikt voor de uitvoering van de opgedragen werkzaamheden.

15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Dit geldt met name voor de laptops en de systemen buiten de hoofdvestiging (hier heeft men geen directe controle op).

15.2 Naleving van beveiligingsbeleid en –normen en technische naleving

15.2.1 Naleving van beveiligingsbeleid en –normen

Aan het beveiligingsbeleid zal regelmatig aandacht besteed worden. In het kader van het integraal management (het afdelingshoofd is verantwoordelijk voor de middelen op de afdeling) is hier een rol voor het afdelingshoofd weggelegd.

Applicatiebeheerders toetsen regelmatig 'hun' applicatie aan het geldende beveiligingsbeleid.

Daarbij wordt rekening gehouden met de algemeen gehanteerde beveiligingsnormen en -eisen aan de veranderingsprocessen.

Het afdelingshoofd heeft in het kader van integraal management de verantwoordelijkheid op beveiligingsgebied. Hij heeft een actieve rol in de gehele evaluatie van beveiligingsbeleid, -normen en -eisen.

15.2.2 Controle op technische naleving

Een controle heeft tot doel te achterhalen of de beveiligingsmaatregelen van hardware en software op de juiste wijze zijn geïmplementeerd. Deze controle kan plaats vinden in de vorm van een audit door een externe deskundige. Tijdens deze audit worden de zwakke plekken opgespoord en wordt beoordeeld of de opgestelde procedures voldoende effectief zijn.

15.3 Overwegingen bij audits van informatiesystemen

15.3.1 Beheersmaatregelen voor audits van informatiesystemen

Een audit kan handmatig (bijv. BRP-audit) uitgevoerd worden of geautomatiseerd. Wordt een audit geautomatiseerd uitgevoerd (met behulp van (hulp)programma's) dan dienen de nodige voorzorgsmaatregelen getroffen te worden. Allereerst dient bekend te zijn in welke mate de inzet van hulpprogramma's of de audit-programmatuur de operationele processen kan verstoren. Een zorgvuldige planning is dus vereist. De grenzen van de audit dienen goed afgebakend te zijn en het management dient in te stemmen met de eisen die behaald dienen te worden.

In principe hoort een audit het operationele proces niet te verstoren. Er mag enkel in gegevens gelezen worden en absoluut niet gemuteerd worden. Van alle acties die uitgevoerd worden op systemen dient een logboek bijgehouden te worden.

15.3.2 Bescherming van hulpmiddelen voor audits van informatiesystemen

Hulpmiddelen die door de auditor gebruikt worden, vallen onder zijn verantwoordelijkheid. De gemeente kan hiervoor niet aansprakelijk gesteld worden.