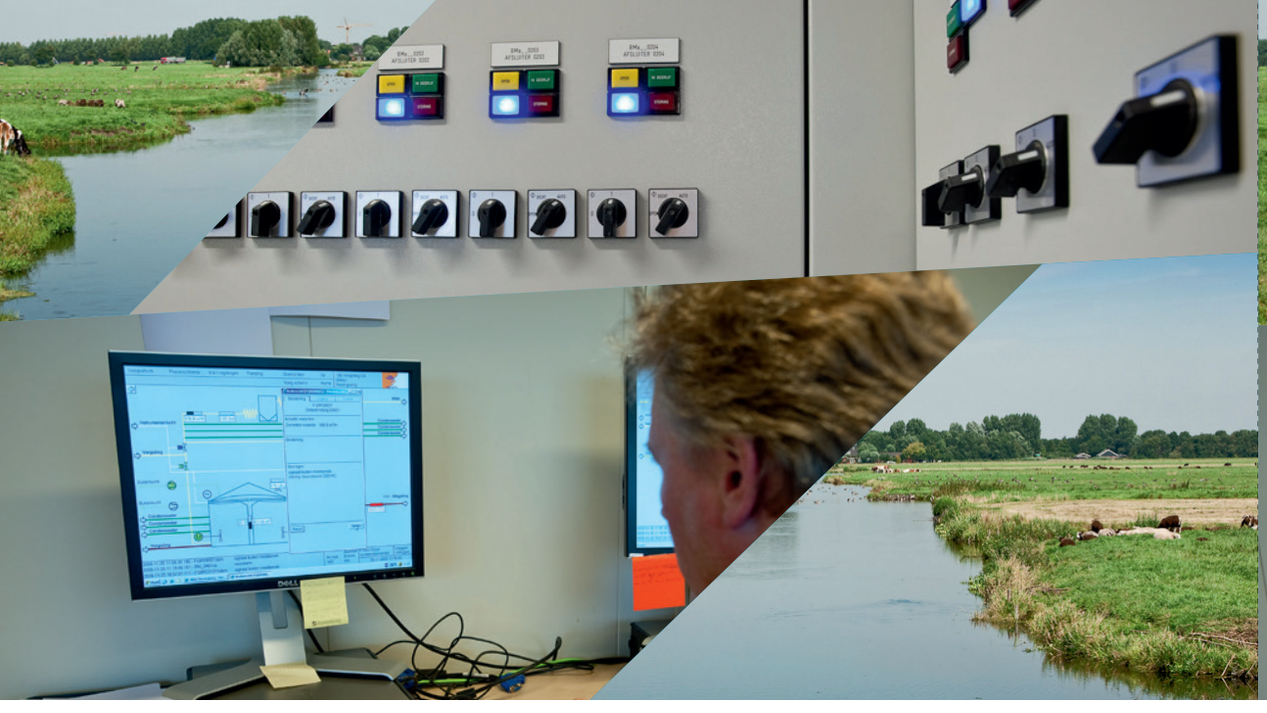


Baseline
Informatiebeveiliging Waterschappen
Strategisch en Tactisch normenkader
WS versie 1.0

UNIE VAN WATERSCHAPPEN

Baseline
Informatiebeveiliging Waterschappen

Strategisch en Tactisch normenkader
WS versie 1.0

UNIE VAN WATERSCHAPPEN

Inhoudsopgave

I Strategisch normenkader

1 Inleiding Stategisch normenkader

1 Inleiding Stategisch normenkader

1.1 Aanleiding

Na diverse incidenten rondom informatiebeveiliging en de toenemende cybercrime heeft de Tweede Kamer en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de druk opgevoerd om maatregelen te nemen die de digitale veiligheid garanderen. Het Ministerie van BZK heeft om dit te bereiken een ' Programmaraad vervolg Diginotar' en later de Taskforce Bestuur Informatieveiligheid en Dienstverlening opgericht. Ook bij de waterschappen komt het belang voor dit onderwerp steeds meer naar voren en is dit onderwerp uitgebreid besproken in de Werkgroep middelen van de Unie van Waterschappen. Deze heeft het Bestuur van de Unie van Waterschappen een aantal aanbevelingen gedaan en gevraagd om een aantal zaken centraal op te pakken. Het Bestuur van de Unie van Waterschappen heeft de volgende aanbevelingen van de Werkgroep Middelen en ingestemd om de volgende producten voor de waterschappen te realiseren:

a) het opstellen van een gezamenlijk kwaliteitsniveau van de beveiliging van fysieke objecten en digitale informatie;

b) het opstellen van een baseline informatiebeveiliging.

Met de uitwerking in de twee delen van deze baseline worden beide doelen beoogd.

1.2 Doelstelling

De baseline bevat maatregelen die algemeen voorkomende informatiebeveiligingsrisico's bij de Waterschappen afdekken. De baseline bevat een aantal minimale beveiligingsniveaus waaraan een waterschap zou moeten willen voldoen, maar is in deze versie nog niet volledig.
Voor risico's die niet door de baseline zijn afgedekt stelt het management van het waterschap aanvullende maatregelen vast.

De Baseline Informatiebeveiliging Waterschappen heeft als doel om te bewerkstelligen dat:

1. Waterschappen op een vergelijkbare manier en efficiënter te laten werken met informatiebeveiliging;
2. Waterschappen een leidraad te geven om aan alle relevante eisen op het gebied van Informatiebeveiliging te kunnen voldoen;
3. Er een eenduidig toetsingskader geboden wordt voor informatieveiligheid over alle waterschappen;
4. Waterschappen een aantoonbaar betrouwbare partner te laten zijn.

Een betrouwbare informatievoorziening is essentieel voor het goed functioneren van de processen bij waterschappen. Informatiebeveiliging is het proces dat deze betrouwbare informatievoorziening borgt.

Het opnemen van informatiebeveiliging als een van de kwaliteitscriteria voor een gezonde bedrijfsvoering is tegenwoordig niet langer een keuze, het is bittere noodzaak geworden.

1.3 Structuur

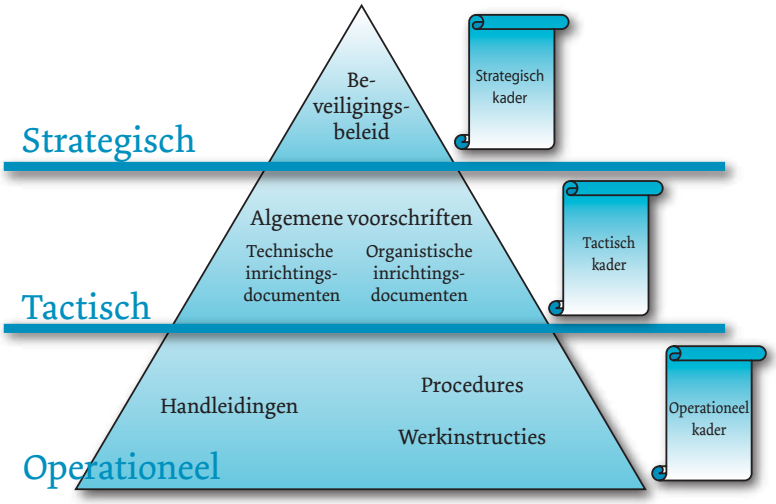
De Baseline Informatiebeveiliging Waterschappen (hierna: BIWA) bestaat uit twee [1] onderdelen:

1. BIWA – SK.

Aan het strategisch kader worden de elementen van informatiebeveiliging opgehangen. Centraal staan de organisatie van informatiebeveiliging en de verantwoording over informatiebeveiliging binnen het waterschap.

2. BIWA – TK.

Het tactisch kader beschrijft de normen en maatregelen ten behoeve van controle en risicomanagement. Het tactisch normenkader is gebaseerd op de internationale beveiligingsnorm ISO/IEC 27002:2007, de controls/ maatregelen welke als baseline gelden voor de waterschappen.

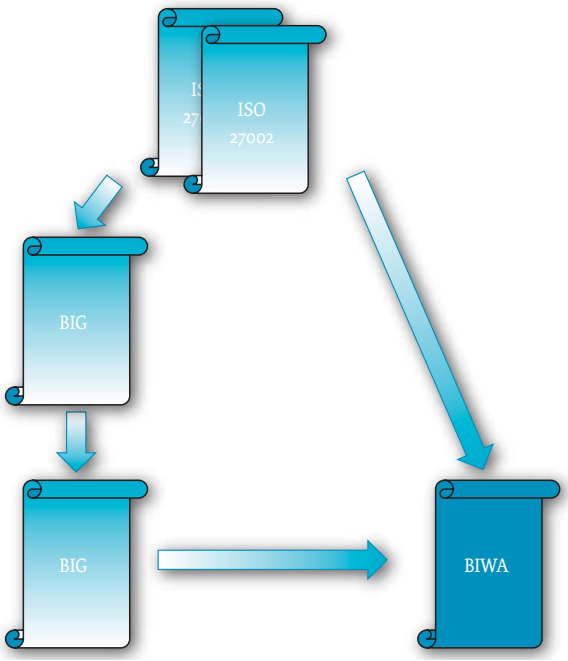


Figuur 1:
Werkingsgebied van de onderdelen van de baseline

1 Bij de gerelateerde baselines BIR en BIG is geconstateerd dat een operationeel onderdeel met implementatierichtlijnen wenselijk is. Dit zal later ook aan de BIWA worden toegevoegd.

1.4 Relatie andere baselines en ISO

De baseline bestaat uit twee delen en is gebaseerd en afgestemd op de baselines van de gemeenten (BIG) en het Rijk (BIR).Het eerste deel is een strategisch normenkader en het tweede deel en tactisch normenkader. De genoemde baselines zijn gebaseerd op de NEN-ISO/IEC 27001 en 27002 en zijn opgebouwd rondom deze normen. In het Tactisch (Normen)kader worden de maatregelen uit de NEN-ISO/IEC 27002 gebruikt en is de hoofdstukindeling gelijk. De BIG is eind maart beschikbaar gekomen en hergebruikt om de Baseline Informatieveiligheid Waterschappen op te stellen.



Figuur 2:
Relatie ISO norm en baselines van rijk (BIR), gemeenten (BIG) en waterschappen (BIWA)

De NEN-ISO/IEC 27001:2005 nl en NEN-ISO/IEC 27002:2007 nl zijn opgenomen op de 'Pas toe of leg uit'-lijst met open standaarden van het Forum Standaardisatie. De opname is een oproep aan alle (semi) overheidsorganisaties in Nederland om deze standaard te gaan gebruiken. Overheden mogen alleen afwijken (d.w.z. 'niet toepassen') ingeval van redenen van bijzonder gewicht. Overheden zijn verplicht om afwijkingen gemotiveerd vast te leggen in de administratie en zijn verplicht om zich te allen tijde over de mate van naleving te verantwoorden in het jaarverslag.

De waterschappen hebben zich aan de open standaarden geconformeerd door bestuursakkoorden.

2 Strategisch kader

2 Strategisch kader

Dit hoofdstuk biedt een strategisch kader voor informatiebeveiligingsbeleid van waterschappen en bevat beleidsuitgangspunten voor de informatiebeveiliging binnen het waterschap.

2.1 Scope

De scope van de BIWA omvat de bedrijfsfuncties, ondersteunende middelen en informatie van het waterschap in de meest brede zin van het woord. De BIWA is van toepassing op alle ruimten van een waterschapshuis en aanverwante gebouwen. Alsmede op apparatuur die door waterschapsambtenaren gebruikt worden bij de uitoefening van hun taak op diverse locaties. De Baseline heeft betrekking op de informatie die daarbinnen verwerkt wordt. Ook als informatiesystemen niet fysiek binnen het waterschap draaien of taken zijn uitbesteed aan derden is deze Baseline van toepassing.

Binnen de scope van deze baseline vallen alle op dit moment geldende normen en regels op het gebied van informatiebeveiliging die door derden aan het waterschap opgelegd zijn. Deze Baseline bevat minimaal al deze maatregelen en brengt ze met elkaar in verband.

2.2 Uitgangspunten

- Binnen de waterschappen is het Dagelijks Bestuur integraal eindverantwoordelijk voor informatiebeveiliging. Informatiebeveiliging gaat niet over ICT alleen, het gaat over informatie in alle verschijningvormen binnen de organisatie.

- De directie is verantwoordelijk voor de implementatie, toepassing en handhaving van informatiebeveiliging binnen het waterschap.

- Er wordt uitgegaan van de standaarden van de pas-toe-of-leg-uit lijst van het forum standaardisatie, de ISO 27001:2005 en ISO 27002:2007.

- Informatie moet worden behandeld volgens maatregelen die genomen zijn op basis van risicoanalyses.[2] Specifieke maatregelen moeten worden genomen voor privacygevoelige informatie op risicoklasse 2.[3]
- Onder veilig wordt verstaan: de juiste vertrouwelijkheid, beschikbaarheid en integriteit.

2 Er is, in tegenstelling tot de BIG en BIR, (nog) geen basisniveau van vertrouwelijkheid vastgesteld.

3 Informatie met vertrouwelijkheidniveau WBP-risicoklasse 2 (WBP2) en Departementaal Vertrouwelijk (DepV) komt veelvuldig voor bij de overheid. Voor waterschappen praten we hier over Vertrouwelijk. Het gaat dan bijvoorbeeld om persoonsvertrouwelijke informatie, commercieel vertrouwelijke informatie of gevoelige informatie in het kader van beleidsvorming, zogenaamde beleidsintimiteit.

- Voor de BIWA wordt het principe gehanteerd dat organisatie-onderdelen van de overheid elkaar beschouwen als vertrouwd partner en niet als onvertrouwde buitenwereld. Het gevolg hiervan is dat iedere overheidsorganisatie afzonderlijk zijn omgeving beveiligt en 'schoon' houdt en dat de andere omgevingen hierop kunnen vertrouwen. Hierbij moet controle de basis van het vertrouwen zijn (governance). Overheden moeten elkaar hierop kunnen aanspreken.

- Bij de opbouw van de BIWA wordt het principe van gelaagdheid gehanteerd. Er is een basisbeveiligingsniveau gekozen op basis van aangedragen risicoanalyses en inbreng van de waterschappen. Daar waar bepaalde toepassingen, werkomgevingen of specifieke dreigingen een hogere beveiligingsgraad of specialistische maatregelen vereisen, kunnen extra maatregelen getroffen worden bovenop het basisbeveiligingsniveau. De baseline is zo opgebouwd dat er, zonder de voor het basisniveau getroffen maatregelen aan te tasten, een verdieping bovenop gebouwd kan worden om te voldoen aan hogere of specialistische eisen.

Dit strategisch kader schrijft geen methodiek voor. De kern is het bewust komen tot betrouwbaarheidseisen en -maatregelen. Waterschappen kunnen op deze wijze kiezen voor een methode of systematiek die past bij de interne risicoanalyse methodiek en daarmee dus aansluit op het risico-denken binnen een waterschap. Daarmee is het element 'comply or explain' toegevoegd aan dit strategisch kader. In feite wordt hiermee aan het management een managementverantwoording wat betreft de informatiebeveiliging gevraagd.

Doordat dit strategisch kader integraal onderdeel is van de bedrijfsvoering sluit het aan bij de planning- en controlcyclus.

2.3 Randvoorwaarden

In de BIWA zijn de volgende randvoorwaarden op de beveiliging van de waterschappen zijn verwerkt:

1. De implementatie, uitvoering en handhaving van informatiebeveiliging valt onder verantwoordelijkheid op directie niveau en wordt gedragen door het management; (zie iso 27001: hfd5 en 27002 hfd 6.1.1);

2. Risicomanagement is uitgangspunt voor informatiebeveiliging[4];

3. Verantwoord en bewust gedrag van mensen is cruciaal voor een goede informatiebeveiliging.

4. De BIWA wordt waterschapsbreed afgesproken.

4 Hiermee wordt niet bedoeld dat daarmee deze Baseline niet van toepassing is, de Baseline bevat het basis beveiligingsniveau en er dient voor informatiesystemen te worden vastgesteld of deze baseline wel voldoende afdekt.

5. Kennis en expertise zijn essentieel voor een toekomstvaste informatiebeveiliging en moeten geborgd worden.

6. Informatiebeveiliging vereist een integrale aanpak, zowel binnen de waterschappen als voor overheidsbrede gemeenschappelijke voorzieningen.

2.4 Plaatsbepaling en Reikwijdte

Dit strategisch kader binnen de Baseline geldt voor de waterschappen waartoe gerekend worden de waterschappen met de daaronder vallende diensten.

Deze Baseline geldt voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.

Informatiebeveiliging is een lijnverantwoordelijkheid en onderdeel van de kwaliteitszorg voor organisatie- en bestuursprocessen en de ondersteunende informatiesystemen.

2.5 Beleid

Het Dagelijks Bestuur stelt het informatiebeveiligingsbeleid vast en ziet toe op uitvoering. Het beleid omvat ten minste:

1. De strategische uitgangspunten en randvoorwaarden die het waterschap hanteert ten aanzien van informatiebeveiliging, waaronder de inbedding in en afstemming op het overige beleid;
2. Het doel van het informatiebeveiligingsbeleid;
3. De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden;
4. De toewijzing van de verantwoordelijkheden op het gebied van informatiebeveiliging aan lijnmanagers;
5. De informatiebeveiligingseisen en normen die voor het waterschap van toepassing zijn;
6. De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd;
7. De bevordering van het beveiligingsbewustzijn.

2.6 Verantwoordelijkheden

Het lijnmanagement is verantwoordelijk voor de kwaliteit van de bedrijfsvoering en daarmee verantwoordelijk voor de beveiliging van informatiesystemen.

Die verantwoordelijkheid wordt verticaal in de lijn verdeeld, van organisatietop tot teamleider. Informatiebeveiliging geldt als een integraal onderdeel van de bedrijfsvoering. Zo is het lijnmanagement ook verant-

woordelijk voor informatiebeveiliging. Het begrip lijnmanagement wordt hierbij ruim opgevat. In voorkomende gevallen kan ook een afdelingshoofd of een manager van een stafafdeling onder het lijnmanagement worden verstaan.

Het lijnmanagement:

1. stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast;

2. is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;

3. controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze maatregelen worden nageleefd;

4. evalueert periodiek de betrouwbaarheidseisen en stelt deze waar nodig bij;

5. rapporteert over de implementatie van de maatregelen in de management rapportages.

Het lijnmanagement kan besluiten om (delen van) de ontwikkeling, exploitatie of het onderhoud van systemen uit te besteden. Ook in deze gevallen blijft het lijnmanagement verantwoordelijk voor de beveiliging van het individuele systeem. Het lijnmanagement communiceert de betrouwbaarheidseisen van het systeem aan de derde partij. Vanuit zijn hoedanigheid als verantwoordelijke partij, controleert het lijnmanagement of de werkzaamheden van de derde partij het vereiste betrouwbaarheidsniveau realiseren.

Functie	Verantwoordelijkheid
Dagelijks bestuur	Stelt informatiebeveiliging beleid vast
Secretaris directeur	Management
Directeur Bedrijfsvoering	Financieel
Afdelingshoofd I(&A)	Strategisch gebruik van management informatiesystemen Verantwoordelijk voor het beveiligingsprogramma
Concern Control	Bedrijfsbrede risico's en deze risico naar een acceptabel niveau brengen Focus op het bedrijfsproces van de hele organisatie Onderhoud het beveiligingsprogramma
Informatiebeveiligings-functionaris	Borgen van informatiebeveiliging maatregelen en rapporteren over afwijkingen
Functionaris Gegevensbescherming	Bescherming van privacy gevoelige gegevens
Systeembeheer Beveiliging	Beveiliging van informatie systemen Implementatie beveiligingsbeleid
Lijnmanagement	Voor de integriteit van gegevens binnen systemen/ applicaties

2.7 Opzet, beheer en onderhoud van de Baseline

De Unie van Waterschappen is eigenaar van dit document en daarmee verantwoordelijk voor het beheer en onderhoud van de BIWA.

Dit document en de daarin opgenomen maatregelen worden periodiek op inhoud, uitvoerbaarheid, invoering en werking beoordeeld en, indien nodig, aangepast om te voorkomen dat de Baseline veroudert.

De Unie van Waterschappen geeft opdracht tot inhoudelijke toetsing en bijstelling van de Baseline.

Herziening is mede afhankelijk van wijzigingen in wetgeving, onderliggende normen, het beleid en de beheerorganisatie. Beveiligingsincidenten vormen aanwijzingen waar voor het waterschap specifieke kwetsbaarheden liggen. Voor de aanpassing van het minimumniveau wordt dan ook gebruik gemaakt van een analyse van incidenten uit de periode voorafgaand aan het vaststellen van het minimumniveau.

II Tactisch normenkader

1 Inleiding Tactisch normenkader

1 Inleiding Tactisch normenkader

1.1 Aanleiding

De steeds grotere afhankelijkheid van informatiesystemen en informatiestromen leidt tot voelbare risico's voor de continuïteit van waterschapsdienstverlening. Betrouwbare, beschikbare en correcte informatie is cruciaal voor de primaire processen en bedrijfsvoering van alle waterschappen. Na diverse incidenten rondom informatiebeveiliging bij overheidsorganisaties en de toenemende cybercrime heeft de Tweede Kamer en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de druk opgevoerd om maatregelen te nemen die de digitale veiligheid garanderen. Het Ministerie van BZK heeft om dit te bereiken een ' Programmaraad vervolg Diginotar' en later de Taskforce Bestuur Informatieveiligheid en Dienstverlening opgericht. Ook bij de waterschappen komt het belang voor dit onderwerp steeds meer naar voren en is dit onderwerp uitgebreid besproken in de Werkgroep middelen van de Unie van Waterschappen. Deze heeft het Bestuur van de Unie van Waterschappen een aantal aanbevelingen gedaan en gevraagd om een aantal zaken centraal op te pakken. Het Bestuur van de Unie van Waterschappen heeft de volgende aanbevelingen van de Werkgroep middelen en ingestemd om de volgende producten voor de waterschappen te realiseren:

a) het opstellen van een gezamenlijk kwaliteitsniveau van de beveiliging van fysieke objecten en digitale informatie;

b) het opstellen van een baseline informatiebeveiliging.

Met de uitwerking in de twee delen van deze baseline worden beide doelen beoogd.

1.2 Scope

De scope van de BIWA omvat de bedrijfsfuncties, ondersteunende middelen en informatie van het waterschap in de meest brede zin van het woord. De BIWA is van toepassing op alle ruimten van een waterschapshuis, aanverwante gebouwen en beheerde objecten als kunstwerken. Alsmede op apparatuur die door waterschapsambtenaren gebruikt worden bij de uitoefening van hun taak op diverse locaties. De Baseline heeft betrekking op de informatie die daarbinnen verwerkt wordt. Ook als informatiesystemen niet fysiek binnen het waterschap draaien of taken zijn uitbesteed aan derden is deze Baseline van toepassing.

Binnen de scope van deze baseline vallen alle op dit moment geldende normen en regels op het gebied van informatiebeveiliging die door derden aan het waterschap opgelegd zijn. Deze Baseline bevat minimaal al deze maatregelen en brengt ze met elkaar in verband.

1.3 Randvoorwaarden

Het tactisch kader beschrijft de normen en maatregelen ten behoeve van controle en risicomanagement. Het tactisch normenkader is gebaseerd op de internationale beveiligingsnorm ISO/IEC 27002:2007, de controls/ maatregelen welke als baseline gelden voor de waterschappen.

Bij het invoeren van de maatregelen van deze baseline en onderliggende ISO norm, wordt voldaan aan het minimale niveau van beveiliging. Indien gekozen wordt om maatregelen niet in te voeren moet dat worden uitgelegd, zogenaamd 'çomply or explain'.

1.4 Definitie informatiebeveiliging

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket maatregelen, gericht op het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening. Het gaat hierbij om:

- Preventieve maatregelen: het voorkomen van informatiebeveiligingsproblemen;
- Repressieve maatregelen: het beperken van schade als gevolg van informatiebeveiligingsproblemen;
- Correctieve maatregelen: de schade die is ontstaan door informatiebeveiligingsproblemen herstellen.

Onderstaand is de definitie van beschikbaarheid, integriteit en vertrouwelijkheid gegeven.

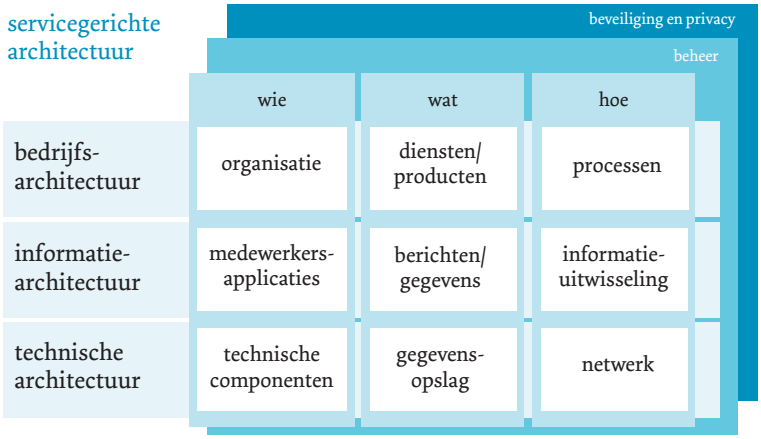
- Beschikbaarheid: waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben;
- Integriteit: het waarborgen van de juistheid, actualiteit en de volledigheid van informatie;
- Vertrouwelijkheid: het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.

In dit document wordt met de term informatiesysteem bedoeld het geheel van mensen, middelen, processen en regels dat de informatievoorziening verzorgt.

1.5 De baseline onder architectuur

De BIWA moet toegepast worden op organisatie- informatie- en technisch vlak. Architectuur zorgt voor samenhang van deze vlakken en stelt kaders voor een toekomstvaste inrichting. Daarom is informatiebeveiliging een onderdeel van de referentiearchitectuur van de waterschappen, de WILMA[1] en wordt de BIWA hierin opgenomen en beheerd.

De WILMA is afgeleid van de overheidsbrede NORA architectuur. Daarmee sluit het aan op het doel van de baseline om in elkaars netwerken van overheden te krijgen en het delen van informatie te bevorderen.



Figuur 1:
NORA raamwerk en positie van informatiebeveiliging

1.6 Eigenaarschap, beheer en onderhoud van de baseline

De Unie van Waterschappen is eigenaar van dit document en daarmee verantwoordelijk voor het beheer en onderhoud van de BIWA.

Dit document en de daarin opgenomen maatregelen worden periodiek op inhoud, uitvoerbaarheid, invoering en werking beoordeeld en, indien nodig, aangepast om te voorkomen dat de Baseline veroudert.

De Unie van Waterschappen geeft opdracht tot inhoudelijke toetsing en bijstelling van de Baseline.

Herziening is mede afhankelijk van wijzigingen in wetgeving, onderliggende normen, het beleid en de beheerorganisatie. Beveiligingsincidenten vormen aanwijzingen waar voor het waterschap specifieke kwetsbaarheden liggen. Voor de aanpassing van het minimumniveau wordt dan ook gebruik gemaakt van een analyse van incidenten uit de periode voorafgaand aan het vaststellen van het minimumniveau.

1 WILMA: Waterschaps Informatie en Logisch Model Architectuur, zie http://wilma.hetwaterschapshuis.nl

2 Leeswijzer

2 Leeswijzer

2.1 Uitgangspunt

In dit tactisch kader worden maatregelen genoemd die voor alle waterschappen nodig worden geacht om een minimaal niveau van beveiliging van informatie te behalen. Daarnaast dient elk waterschap te onderzoeken of deze maatregel volstaat voor de eigen organisatie, aan de hand van de originele ISO-norm. Indien er geen maatregel is vermeld geldt de tekst volgens de norm.

2.2 Structuur

De indeling van dit document is als volgt.

Hoofdstuk 1 – 3: Het algemene deel over de Baseline, uitleg, relaties met architectuur frameworks, hoe deze baseline moet worden gebruikt.

Hoofdstuk 4: laat zien hoe bepaald kan worden welke ICT-voorzieningen binnen de BIWA TNK vallen en voor welke ICT-voorzieningen er aanvullende maatregelen genomen moeten worden.

Hoofdstukken 5 t/m 15: bevatten hoofdbeveiligingscategorieën en subcategorieën.

Bij elke subcategorie is de doelstelling uit NEN/ISO 27002:2007 vermeld.

Elke subcategorie kent een aantal beheersmaatregelen, waarvan de nummering exact overeenkomt met NEN/ISO 27002:2007;
De doelstelling uit de ISO NEN/27002:2007 is cursief weergegeven;
De daaronder genoemde norm of implementatierichtlijn die als specifieke aanvulling op de ISO voor de waterschappen is opgenomen wordt aangeduid met Waterschap specifieke maatregel.
Indien geen tekst is opgenomen geldt de tekst van de bijbehorende implementatierichtlijn van de ISO NEN/27002:2007.

Bijlage 1: bevat een woordenlijst.
Bijlage 2: bevat een kruisverwijzing naar de belangrijkste wet- en regelgeving.

2.3 Doelgroepen

Deze baseline bevat aandachtsgebieden voor verschillende functionarissen binnen de doelgroep waterschappen. Hieronder worden voor enkele rollen de hoofdstukken genoemd die relevant zijn.

CISO, IB- adviseurs/coördinatoren en auditors

- Alle hoofdstukken

Management

- Hoofdstukken 6, 8, 10, 12, 13 en 14

De lijnmanager is verantwoordelijk voor het handhaven van de personele beveiliging met eventuele ondersteuning door Personeelszaken. Daarnaast is deze verantwoordelijk voor het uitvoeren van activiteiten in processen (algemene procesverantwoordelijkheid) op basis van de beschreven inrichting ervan. De verantwoordelijkheid voor de naleving van specifieke beveiligingsaspecten hangt af van het soort proces.

Beleidsmakers

- Hoofdstukken 4, 5, 6, 10 en 12

De beleidsmaker is verantwoordelijk voor het ontwikkelen van een veilig en werkbaar beleid. Het beleid moet goed uitvoerbaar en controleerbaar zijn.

Personeelszaken

- Hoofdstuk 8

Personeelszaken is verantwoordelijk voor werving, selectie en algemene zaken rond het functioneren van personeel, inclusief bewustwording en gedrag.

Fysieke beveiliging

- Hoofdstuk 9

Fysieke beveiliging is verantwoordelijkheid van Facilitaire zaken. Zij zijn verantwoordelijk voor de beveiliging van percelen, panden, ruimtes en installaties.

ICT-diensten en ICT-infrastructuren

- Hoofdstukken 6, 7, 9, 10, 11 en 12

De ICT-diensten en –infrastructuren, bijvoorbeeld standaard kantoorautomatisering, maar ook procesautomatisering (SCADA/ICS systemen), zijn ondersteunend aan bijna alle processen. De eisen die aan ICT-voorzieningen gesteld worden, zijn hierdoor zeer ingrijpend en bepalen voor een significant deel de inrichting van het ICT-landschap.

Applicatie-eigenaren en systeemeigenaren

- Hoofdstukken 7, 10, 11 en 12

Applicatie-eigenaren c.q. systeemeigenaren zijn verantwoordelijk voor de veilige en correcte verwerking van de relevante data binnen de applicatie. Een belangrijk onderdeel van informatiebeveiliging vormen de eindgebruikers, zij dienen kennis te hebben van de gevolgen van hun gedrag op beveiliging.

Externe leveranciers

Externe leveranciers zijn een bijzondere groep. Bij uitbesteding van diensten, systemen of taken blijft opdrachtgever / systeemeigenaar altijd zelf verantwoordelijk voor de kwaliteit en veiligheid van uitbestede zaken.

3 Implementatie van de tactische baseline

3 Implementatie van de tactische baseline

Vanuit het RIJK (BIR) en Gemeenten (BIG) zijn de volgende stappen als een leidraad bij de implementatie van de tactische baseline overgenomen:

- Benoem verantwoordelijken
- Voer een GAP-analyse uit
- Benoem Quick Wins en voer deze uit, bijvoorbeeld het beschrijven en implementeren van procedures
- Maak een integraal implementatieplan en rapporteer periodiek over voortgang van implementatie.

Zodra er een andere implementatie aanpak voor handen is zal deze worden toegevoegd

3.1 Benoem verantwoordelijken

Maatregelen moeten worden geïmplementeerd. Vaak vallen deze binnen een verantwoordelijkheidsgebied van een specifieke manager. Bijvoorbeeld:

- Benoem een informatiebeveiligingsfunctionaris, doorgaans Corporate Information Security Officer (CISO) genoemd, of wijs iemand de CISO rol toe (zie ook hoofdstuk 6).

- Toegangsbeveiliging maatregelen behoren door de facilitair manager te worden ingevoerd en gewaarborgd

- Personele maatregelen behoren bij de afdeling personeelszaken, denk hierbij aan aanname beleid, ontslag beleid, benoemen vertrouwensfuncties.

De CISO is de rol die uitgevoerd wordt om beveiliging te coördineren binnen een organisatie, waarbij de CISO bij voorkeur niet binnen de ICT-organisatie gepositioneerd wordt. Afhankelijk van de grootte van het waterschap kunnen er meer informatiebeveiligingsfunctionarissen zijn.

Betrokken rollen bij informatieveiligheid zijn:

Rol	Verantwoordelijkheid
Bestuur	Stelt informatiebeveiliging beleid vast
CEO (Chief Executieve Officer)	Management
CFO (Chief Financial Officer)	Financieel
CIO (Chief Information Officer)	Strategisch gebruik van management informatiesystemen Verantwoordelijk beveiligingsprogramma
CSO (Chief Security Officer)	Bedrijfsbrede risico's en deze risico naar een acceptabel niveau brengen Focus op het bedrijfsproces van de hele organisatie Onderhoud het beveiligingsprogramma
CISO (Corporate Information Security Officer)	Focus op IT systemen en infrastructuur
CPO (Chief Pivacy Officer)	Bescherming van privacy gevoelige gegevens
Systeembeheer Beveiliging	Beveiliging van informatie systemen Implementatie beveilingsbeleid
Lijnmanagement	Voor de integriteit van gegevens binnen systemen/ applicaties

3.2 Voer een GAP analyse uit

De GAP-analyse geeft als instrument antwoord op vragen als: "Waar zijn we nu" en "Waar willen we heen". Met het gebruiken van de baseline weet het waterschap nog niet wat er gedaan moet worden om de baseline ingevoerd te krijgen. Door middel van de GAP-analyse kan het waterschap vaststellen welke baseline-maatregelen al ingevoerd zijn, en belangrijker, welke maatregelen uit deze baseline nog niet ingevoerd zijn.

Met het gevonden resultaat kan vervolgens planmatig worden omgegaan en kunnen de actiehouders beginnen met het invoeren van maatregelen en hierover ook periodiek in de management rapportages over rapporteren.

Onderzoek welke maatregelen al genomen zijn en geef per maatregel aan:

- of er iets over beschreven is en, zo ja, waar dat opgelegd is (opzet)
- of de verantwoordelijken bekend zijn met de maatregel (bestaan)

3.3 Quick wins

Na het uitvoeren van de GAP-analyse is aan te raden te beginnen met quick wins; maatregelen die op korte termijn toegevoegde waarde opleveren voor een organisatie of maatregelen die aansluiten bij actuele speerpunten.

3.4 Maak een implementatieplan en rapporteer over voortgang van implementatie

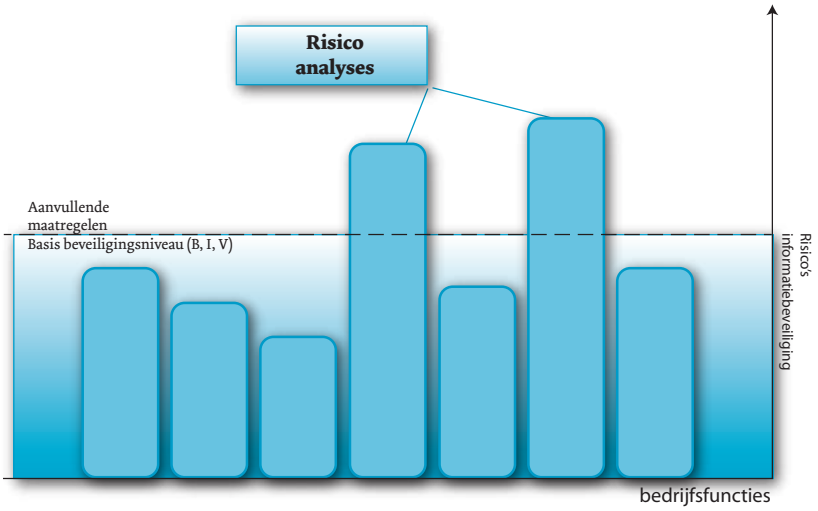
Maak een plan om te komen tot implementatie van deze baseline, rekening houdend met de resultaten van de uitgevoerde GAP-analyse en stuur op de voortgang. Laat rapporteren over deze voortgang door de benoemde verantwoordelijken om specifieke maatregelen in te voeren.

In overeenstemming met artikel 13.2.1 punt 2 dient de beheersing van deze planning opgenomen te worden in de P&C-cyclus en jaarlijks geëvalueerd te worden.

4 Risico beoordeling en risico afweging

4 Risico beoordeling en risico afweging

Het basisniveau voor informatiebeveiliging (baseline) bestaat uit een set maatregelen die in elke situatie voor elk bedrijfsonderdeel van toepassing is en die een standaard risiconiveau afdekt tegen geïdentificeerde dreigingen. Als dat niveau voldoende is – zoals bij standaard kantoorautomatiseringtoepassingen – dan is het niet nodig een risicoanalyse uit te voeren. Pas wanneer duidelijk is dat meer beveiliging vereist is, zullen aanvullende maatregelen noodzakelijk zijn. Voor het definiëren van deze maatregelen wordt een risicoanalyse uitgevoerd. In onderstaande figuur is de positionering van een baseline gevisualiseerd.



Figuur 2:
baseline positionering

Binnen het vakgebied informatiebeveiliging wordt onderscheid gemaakt tussen beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. De BIWA sluit hierbij aan.

Beschikbaarheid

De BIWA definieert een basis-set aan eisen voor beschikbaarheid voor de infrastructuur van de waterschappen en voor de informatie-uitwisseling tussen de waterschappen. Deze set van eisen dient als basis voor het maken van afspraken over de beschikbaarheid tussen de eigenaar van het informatiesysteem en de (diensten)leverancier. Dit houdt in dat voor de beschikbaarheid van de informatievoorziening er een minimale set van normen wordt opgesteld waarbij per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

Integriteit

De integriteit op het IT vlak valt normaliter in twee delen uiteen: de integriteit van datacommunicatie en opslag enerzijds (d.w.z. niet gerelateerd aan het proces zelf), en de integriteit van de informatie in de applicaties (d.w.z. gerelateerd aan het proces zelf). Integriteit gekoppeld aan de applicatie is altijd situatieafhankelijk en afhankelijk van de eisen van een specifiek proces. Voor de functionele integriteit van de informatievoorziening wordt er een minimale set van normen opgesteld waarbij er per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

Vertrouwelijkheid

De BIWA beschrijft de maatregelen die nodig zijn voor het basisvertrouwelijkheidsniveau (Waterschap) Vertrouwelijk en WBP risicoklasse 2.

5 Beveiligingsbeleid

5 Beveiligingsbeleid

5.1 Informatiebeveiligingsbeleid

Doelstelling
Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-)partners en er mede voor zorgt dat de kritieke bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden.

5.1.1 Beleidsdocumenten voor informatiebeveiliging

Een document met informatiebeveiligingsbeleid behoort door het hoogste management te worden goedgekeurd en gepubliceerd. Het document dient tevens kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.

Waterschap specifieke maatregel
1. Er is beleid voor informatiebeveiliging door het Dagelijks Bestuur vastgesteld, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritieke bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten.

5.1.2 Beoordeling van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.

Waterschap specifieke maatregel
1. Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. Zie ook 6.1.8.1.

6 Organisatie van de Informatiebeveiliging

6 Organisatie van de Informatiebeveiliging

6.1 Interne organisatie

Doelstelling
Beheren van de informatiebeveiliging binnen de organisatie.

6.1.1 Betrokkenheid van het Dagelijks Bestuur en Directie bij informatiebeveiliging

Het hoogste management behoort actief informatiebeveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.

Waterschap specifieke maatregel
Het Dagelijks Bestuur waarborgt dat de informatiebeveiligingsdoelstellingen worden vastgesteld, voldoen aan de kaders zoals gesteld in dit document en zijn geïntegreerd in de relevante processen. Dit gebeurt door één keer per jaar opzet, bestaan en werking van de Informatiebeveiligingsmaatregelen te bespreken in het overleg van het Dagelijks Bestuur en hiervan verslag te doen.

6.1.2 Coördinatie van informatiebeveiliging

Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit verschillende delen van de organisatie met relevante rollen en functies.

Waterschap specifieke maatregel
1 De rollen van Chief Information Security Officer (CISO) en het lijnmanagement zijn beschreven.

a. De CISO rapporteert aan de directie.
b. De CISO bevordert en adviseert gevraagd en ongevraagd over de beveiliging van het waterschap, verzorgt rapportages over de status, controleert of m.b.t. de beveiliging van het waterschap de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de informatiebeveiliging van het waterschap.

6.1.3 Toewijzing van verantwoordelijkheden bij informatiebeveiliging

Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.

6.1.4 Goedkeuringsproces voor ICT-voorzieningen

Er behoort een goedkeuringsproces voor nieuwe Informatievoorzieningen te worden vastgesteld en geïmplementeerd.

Waterschap specifieke maatregel

1. Er is een goedkeuringsproces voor zowel nieuwe informatievoorzieningen als wijzigingen in informatievoorzieningen.

6.1.5 Geheimhoudingsovereenkomst

Eisen voor vertrouwelijkheid of voor een geheimhoudingsovereenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie behoren te worden vastgesteld en regelmatig te worden beoordeeld.

Waterschap specifieke maatregel

1. Nieuwe medewerkers dienen bij in dienst treden de ambtseed af te leggen, respectievelijk een geheimhoudingsverklaring te tekenen. Dit geldt ook indien het een externe medewerker betreft.

6.1.6 Contact met overheidsinstanties

Er behoren geschikte contacten met relevante overheidsinstanties te worden onderhouden.

6.1.7 Contact met speciale belangengroepen

Er behoren geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties te worden onderhouden.

6.1.8 Beoordeling van het informatiebeveiligingsbeleid

De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheersdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich wijzigingen voordoen in de implementatie van de beveiliging.

Waterschap specifieke maatregel

1. Het informatiebeveiligingsbeleid wordt minimaal één keer in de drie jaar geëvalueerd en desgewenst bijgesteld. Zie ook 5.1.2.
2. Periodieke beveiligingsaudits worden uitgevoerd in opdracht van directie.
3. Over het functioneren van de informatiebeveiliging wordt, conform de P&C cyclus, jaarlijks gerapporteerd aan het lijnmanagement.

6.2 Externe Partijen

Doelstelling
Beveiligen van de informatie en ICT-voorzieningen van de organisatie handhaven waartoe externe partijen toegang hebben of die door externe partijen worden verwerkt of beheerd, of die naar externe partijen wordt gecommuniceerd.

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

De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend.

Waterschap specifieke maatregel

1. Informatiebeveiliging is aantoonbaar, op basis van een risicoafweging, meegewogen bij het besluit een externe partij wel of niet in te schakelen.
2. Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang, fysiek, netwerk of tot gegevens, de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.
3. Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie (bijv. risicoklasse II van WBP of de vertrouwelijkheidklasse) heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn.
4. Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthentiseerde en geautoriseerde toegang vastgesteld wordt.
5. Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkerovereenkomst (conform WBP artikel 14) afgesloten.
6. Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd. (zie ook 6.2.3.3). Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.
7. Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd.

6.2.2 Beveiliging beoordelen in de omgang met klanten

Alle geïdentificeerde beveiligingseisen behoren te worden beoordeeld voordat klanten toegang wordt verleend tot de informatie of bedrijfsmiddelen van de organisatie.

Waterschap specifieke maatregel

1. Alle noodzakelijke beveiligingseisen worden op basis van een risicoafweging vastgesteld en geïmplementeerd, voordat aan gebruikers toegang tot informatie op bedrijfsmiddelen wordt verleend.

6.2.3 Beveiliging behandelen in overeenkomsten met een derde partij

In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen, behoren alle relevante beveiligingseisen te zijn opgenomen.

Waterschap specifieke maatregel

1. De maatregelen behorend bij 6.2.1 zijn voorafgaand aan het afsluiten van het contract gedefinieerd en geïmplementeerd
2. Uitbesteding (ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin o.a. intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow (broncodedeponering) en reviews geregeld worden.
3. In contracten met externe partijen is vastgelegd hoe men om dient te gaan met wijzigingen en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast door de wijzigingen.
4. In contracten met externe partijen is vastgelegd hoe wordt omgegaan met geheimhouding en de geheimhoudingsverklaring.
5. Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid en integriteit.
6. In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn.
7. Als er gebruikt gemaakt wordt van onderaannemers dan gelden daar dezelfde beveiligingseisen voor als voor de contractant. De hoofdaannemer is verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken.
6. De producten, diensten en daarbij geldende randvoorwaarden, rapporten en registraties die door een derde partij worden geleverd, worden beoordeeld op het nakomen van de afspraken in de overeenkomst. Verbeteracties worden geïnitieerd wanneer onder het afgesproken niveau wordt gepresteerd.

7 Beheer van bedrijfsmiddelen

7 Beheer van bedrijfsmiddelen

7.1 Verantwoordelijkheid voor bedrijfsmiddelen

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

7.1.1 Inventarisatie van bedrijfsmiddelen

Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden.

Waterschap specifieke maatregel
Er is een actuele registratie van bedrijfsmiddelen die voor de organisatie een belang vertegenwoordigen zoals informatie(verzamelingen), software, hardware, diensten, mensen en hun kennis/vaardigheden. Van elk middel is de waarde voor de organisatie, het vereiste beschermingsniveau en de verantwoordelijke lijnmanager bekend.

7.1.2 Eigendom van bedrijfsmiddelen

Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie.Waterschap specifieke maatregel

1. Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit is een verantwoordelijke lijnmanager benoemd.

7.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen.

Waterschap specifieke maatregel

1. Gebruikers hebben kennis van de regels.
2. Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen. De toestemming kan generiek geregeld worden in het kader van de functieafspraken tussen manager en medewerker.
3. Informatiedragers worden dusdanig gebruikt dat vertrouwelijke informatie niet beschikbaar kan komen voor onbevoegde personen.

7.2 Classificatie van informatie

Doelstelling
Bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt.

Informatie behoort te worden geclassificeerd om bij het verwerken van de informatie de noodzaak, prioriteiten en verwachte graad van bescherming te kunnen aangeven.

7.2.1 Richtlijnen voor classificatie van informatie

Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.

1. Waterschap specifieke maatregelDe organisatie heeft classificatierichtlijnen opgesteld.
2. In overeenstemming met hetgeen in het WBP is vastgesteld, dient er een helder onderscheid te zijn in de herleidbare (klasse II/III) en de niet herleidbare (klasse 0 en I) gegevens.

7.2.2 Labeling en verwerking van informatie

Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.

Waterschap specifieke maatregel
1. De lijnmanager heeft maatregelen getroffen om te voorkomen dat niet-geautoriseerden kennis kunnen nemen van geclassificeerde informatie.
2. De opsteller van de informatie doet een voorstel tot classificering en brengt deze aan op de informatie. De goedkeurder van de inhoud van de informatie stelt tevens de classificering vast.

8 Personele beveiliging

8 Personele beveiliging

8.1 Voorafgaand aan het dienstverband

Doelstelling
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.

8.1.1 Rollen en verantwoordelijkheden

De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van beveiliging behoren te worden vastgesteld en gedocumenteerd overeenkomstig het beleid voor informatiebeveiliging van de organisatie.

Waterschap specifieke maatregel

1. De taken en verantwoordelijkheden van een medewerker zijn opgenomen in de functiebeschrijving en worden onderhouden. In de functiebeschrijving wordt minimaal aandacht besteed aan:
   - uitvoering van het informatiebeveiligingsbeleid
   - bescherming van bedrijfsmiddelen
   - rapportage van beveiligingsincidenten
   - expliciete vermelding van de verantwoordelijkheden voor het beveiligen van persoonsgegevens
2. Alle vaste en ingehuurde medewerkers krijgen bij hun indiensttreding hun verantwoordelijkheden ten aanzien van informatiebeveiliging ter inzage. De schriftelijk vastgestelde en voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging, welke zij bij de vervulling van hun functie hebben na te leven, worden op een toegankelijke plaats ter inzage gelegd. Overeenkomstige voorschriften maken deel uit van de contracten met externe partijen. Ook voor hen geldt de toegankelijkheid van geldende regelingen en instructies.
3. Indien een medewerker speciale verantwoordelijkheden heeft t.a.v. informatiebeveiliging dan is hem dat voor indiensttreding (of bij functiewijziging), bij voorkeur in de aanstellingsbrief of bij het afsluiten van het contract, aantoonbaar duidelijk gemaakt.
4. De algemene voorwaarden van het arbeidscontract of de aanstelling van medewerkers bevatten de wederzijdse verantwoordelijkheden ten aanzien van informatiebeveiliging. Het is aantoonbaar dat medewerkers bekend zijn met hun verantwoordelijkheden op het gebied van informatiebeveiliging.

8.1.2 Screening

Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoort te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoren evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.

Waterschap specifieke maatregel

1. Bij de aanstelling worden de gegevens die de medewerker heeft verstrekt onder andere over zijn identiteit, arbeidsverleden en scholing geverifieerd.

8.1.3 Arbeidsvoorwaarden

Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging behoren te zijn vastgelegd.

8.2 Tijdens het dienstverband

Doelstelling

Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen en het risico van een menselijke fout te verminderen.

8.2.1 Directieverantwoordelijkheid

De directie behoort van werknemers, ingehuurd personeel en externe gebruikers te eisen dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie.

Waterschap specifieke maatregel

1. De directie heeft een strategie ontwikkeld en geïmplementeerd om blijvend over specialistische kennis en vaardigheden van waterschapsambtenaren en ingehuurd personeel (onder andere die kritieke bedrijfsactiviteiten op het gebied van IB uitoefenen) te kunnen beschikken.
2. De directie bevordert dat waterschapsambtenaren, ingehuurd personeel en (waar van toepassing) externe gebruikers van interne systemen, algemene beveiligingsaspecten toepassen in hun gedrag en handelen conform vastgesteld beleid.

8.2.2 Bewustwording, opleiding en training ten aanzien van informatiebeveiliging

Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.

Waterschap specifieke maatregel

1. Alle medewerkers van de organisatie worden regelmatig attent gemaakt op het beveiligingsbeleid en de beveiligingsprocedures van de organisatie, voor zover relevant voor hun functie.

8.2.3 Disciplinaire maatregelen

Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de informatiebeveiliging hebben gepleegd.

Waterschap specifieke maatregel

1. Er is een disciplinair proces vastgelegd voor medewerkers die inbreuk maken op het informatiebeveiligingsbeleid (zie ook: SAW, hoofdstuk 7, Disciplinaire maatregelen).

8.3 Beëindiging of wijziging van het dienstverband

Doelstelling

Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers ordelijk de organisatie verlaten of hun dienstverband wijzigen.

8.3.1 Beëindiging van verantwoordelijkheden

De verantwoordelijkheden voor beëindiging of wijziging van het dienstverband behoren duidelijk te zijn vastgesteld en toegewezen.

Waterschap specifieke maatregel

1. Voor ambtenaren is in de ambtseed of belofte vastgelegd welke verplichtingen ook na beëindiging van het dienstverband of bij functiewijziging nog van kracht blijven en voor hoe lang. Voor ingehuurd personeel (zowel in dienst van een derde bedrijf als individueel) is dit contractueel vastgelegd. Indien nodig wordt een geheimhoudingsverklaring ondertekend.
2. Het lijnmanagement heeft een procedure vastgesteld voor beëindiging van dienstverband, contract of overeenkomst waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten, innemen van bedrijfsmiddelen en welke verplichtingen ook na beëindiging van het dienstverband blijven gelden.
3. Het lijnmanagement heeft een procedure vastgesteld voor verandering van functie binnen de organisatie, waarin minimaal aandacht

besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie.

8.3.2 Retournering van bedrijfsmiddelen

Alle werknemers, ingehuurd personeel en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst, of behoort na wijziging te worden aangepast.

Waterschap specifieke maatregel

1. Zie 8.3.1.3

8.3.3 Blokkering van toegangsrechten

De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en ICT-voorzieningen behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoort na wijziging te worden aangepast.

Waterschap specifieke maatregel

1. Zie 8.3.1.3

9 Fysieke beveiliging en beveiliging van de omgeving

9 Fysieke beveiliging en beveiliging van de omgeving

9.1 Beveiligde ruimten

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

9.1.1 Fysieke beveiliging van de omgeving

Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en ICT-voorzieningen bevinden.

Waterschap specifieke maatregel

1. De fysieke locaties van een waterschap en de omtrek worden ingedeeld in verschillende zoneringen.
2. Voor voorzieningen (binnen of buiten het gebouw) zijn duidelijke beveiligingsgrenzen bepaald.
3. Gebouwen bieden voldoende weerstand (bepaald op basis van een risicoafweging).
4. Voor toegang tot speciale ruimten is een doelbinding vereist, dat wil zeggen dat personen op grond van hun werkzaamheden toegang kan worden verleend. (bijvoorbeeld Beheer, BHV).

9.1.2 Fysieke toegangsbeveiliging

Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.

Waterschap specifieke maatregel

1. Toegang tot gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
2. De beveiligingszones en toegangsbeveiliging daarvan zijn ingericht conform het toegangsbeleid.
3. De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afhankelijk van de zone van een bepaald toegangsmiddel.
4. De uitgifte van toegangsmiddelen wordt geregistreerd.
5. Niet uitgegeven toegangsmiddelen worden opgeborgen in een beveiligd opbergmiddel.
6. Apparatuur en bekabeling buiten computerruimtes moeten aan dezelfde beveiligingseisen voldoen als apparatuur daarbinnen.
7. Er vindt minimaal één keer per half jaar een periodieke controle/evaluatie plaats op de autorisaties voor fysieke toegang.

9.1.3 Beveiliging van kantoren, ruimten en faciliteiten

Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.

Waterschap specifieke maatregel

1. Papieren documenten en mobiele gegevensdragers die vertrouwelijke informatie bevatten worden beveiligd opgeslagen.
2. Er is actief beheer van sloten en kluizen met procedures voor wijziging van combinaties door middel van een sleutelplan, ten behoeve van opslag van gerubriceerde informatie.
3. Serverruimtes, datacenters en daar aan gekoppelde bekabelingsystemen zijn ingericht in lijn met daarvoor geldende best practices.

9.1.4 Bescherming tegen bedreigingen van buitenaf

Er behoort fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten te worden ontworpen en toegepast.

Waterschap specifieke maatregel

1. Bij maatregelen is rekening gehouden met specifieke bedreigingen van aangrenzende panden of terreinen.
2. Reserve apparatuur en back-ups zijn op een zodanige afstand ondergebracht dat één en dezelfde calamiteit er niet voor kan zorgen dat zowel de hoofdlocatie als de back-up/reserve locatie niet meer toegankelijk zijn.
3. Beveiligde ruimten waarin zich bedrijfskritische apparatuur bevindt zijn voldoende beveiligd tegen wateroverlast.
4. Bij het betrekken van nieuwe gebouwen wordt een locatie gekozen waarbij rekening wordt gehouden met de kans op en de gevolgen van natuurrampen en door mensen veroorzaakte rampen.
5. Gevaarlijke of brandbare materialen zijn op een zodanige afstand van een beveiligde ruimte opgeslagen dat een calamiteit met deze materialen geen invloed heeft op de beveiligde ruimte.
6. Er is door de brandweer goedgekeurde en voor de situatie geschikte brandblusapparatuur geplaatst en aangesloten. Dit wordt jaarlijks gecontroleerd.

9.1.5 Werken in beveiligde ruimten

Er behoren richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast.

Waterschap specifieke maatregel

1. Medewerkers die zelf niet geautoriseerd zijn mogen alleen onder begeleiding van bevoegd personeel en als er een duidelijke noodzaak voor is toegang krijgen tot fysiek beveiligde ruimten waarin IT voorzieningen zijn geplaatst of waarin met vertrouwelijke informatie wordt gewerkt.

2. Beveiligde ruimten (zoals een serverruimte of kluis) waarin zich geen personen bevinden zijn afgesloten en worden regelmatig gecontroleerd.
3. Zonder expliciete toestemming mogen binnen beveiligde ruimten geen opnames (foto, video of geluid) worden gemaakt.

9.1.6 Openbare toegang en gebieden voor laden en lossen

Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, behoren te worden beheerst en indien mogelijk worden afgeschermd van IT voorzieningen, om onbevoegde toegang te voorkomen.

Waterschap specifieke maatregel

1. Er bestaat een procedure voor het omgaan met verdachte pakketten en brieven in postkamers en laad- en losruimten.

9.2 Beveiliging van apparatuur

Doelstelling

Het voorkomen van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.

9.2.1 Plaatsing en bescherming van apparatuur

Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd.

Waterschap specifieke maatregel

1. Apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier. Dit geldt minimaal voor temperatuur en luchtvochtigheid, aarding, spanningsstabiliteit en overspanningsbeveiliging.
2. Standaard accounts in apparatuur worden gewijzigd en de bijbehorende standaard leveranciers wachtwoorden worden gewijzigd bij ingebruikname van apparatuur.
3. Gebouwen zijn beveiligd tegen de gevolgen van blikseminslag.
4. Eten en drinken zijn verboden in computerruimtes.
5. Een informatiesysteem dient te voldoen aan de hoogste classificatie-eisen, conform de informatie die voor kan komen op het informatiesysteem bij het verwerken ervan. Indien dit niet mogelijk is wordt een gescheiden systeem gebruikt voor de informatieverwerking waaraan hogere eisen gesteld worden.[2]

2 Waterschappen die servervirtualisatie toepassen dienen zelf de risico afweging te maken of en hoe zij systemen willen scheiden.

9.2.2 Nutsvoorzieningen

Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.

9.2.3 Beveiliging van kabels

Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd.

9.2.4 Onderhoud van apparatuur

Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.

Waterschap specifieke maatregel

1. Reparatie en onderhoud van apparatuur (hardware) vindt op locatie plaats door - bevoegd personeel, reparatie op locatie uitsplitsen tenzij er geen data op het apparaat aanwezig of toegankelijk is.

9.2.5 Beveiliging van apparatuur buiten het terrein

Apparatuur buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie.

Waterschap specifieke maatregel

1. Alle apparatuur buiten de terreinen wordt beveiligd met fysieke beveiligingsmaatregelen zoals bijvoorbeeld sloten en cameratoezicht die zijn vastgesteld op basis van een risicoafweging.

9.2.6 Veilig verwijderen of hergebruiken van apparatuur

Alle apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd.

Waterschap specifieke maatregel

1. Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de beheersorganisatie ingeleverd. De beheerorganisatie zorgt voor een verantwoorde afvoer zodat er geen data op het apparaat aanwezig of toegankelijk is. Als dit niet kan wordt het apparaat of de informatiedrager fysiek vernietigd. Het afvoeren of vernietigen wordt per bedrijfseenheid geregistreerd op basis vna risicoafweging.[3]

3 Er zijn waterschappen die het gebruik van eigen apparatuur (BYOD) toestaan, in dat geval dient een policy ingesteld te worden die regelt dat data wordt verwijderd als de apparatuur niet meer gebruikt wordt door de medewerker.

2. Hergebruik van apparatuur buiten de organisatie is slechts toegestaan indien de informatie is verwijderd met een voldoende veilige methode.

9.2.7 Verwijdering van bedrijfseigendommen

Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.

10 Beheer van Communicatie- en Bedieningsprocessen

10 Beheer van Communicatie- en Bedieningsprocessen

10.1 Bedieningsprocedures en -verantwoordelijkheden

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

10.1.1 Gedocumenteerde bedieningsprocedures

Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.

Waterschap specifieke maatregel

1. Bedieningsprocedures bevatten informatie over opstarten, afsluiten, backup- en herstelacties, afhandelen van fouten, beheer van logs, contactpersonen, noodprocedures en speciale maatregelen voor beveiliging.
2. Er zijn procedures voor de behandeling van digitale media die ingaan op ontvangst, opslag, rubricering, toegangsbeperkingen, verzending, hergebruik en vernietiging.

10.1.2 Wijzigingsbeheer

Wijzigingen in ICT-voorzieningen en informatiesystemen behoren te worden beheerst.

Waterschap specifieke maatregel

1. In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan:
2. het administreren van significante wijzigingen
3. impactanalyse van mogelijke gevolgen van de wijzigingen
4. goedkeuringsprocedure voor wijzigingen
5. Instellingen van informatiebeveiligingsfuncties (b.v. security software) op het koppelvlak tussen vertrouwde en niet vertrouwde netwerken, worden automatisch op wijzigingen gecontroleerd.

10.1.3 Functiescheiding

Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

Waterschap specifieke maatregel

1. Niemand in een organisatie of proces mag op uitvoerend niveau rechten hebben om een gehele cyclus van handelingen in een bedrijfskritiek informatiesysteem te beheersen. Dit in verband met het risico dat hij of zij zichzelf of anderen onrechtmatig bevoordeelt of de

organisatie schade toe brengt. Dit geldt voor zowel informatieverwerking als beheeracties.
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.
3. Vóór de verwerking van gegevens die de integriteit van kritieke informatie of kritieke informatie systemen kunnen aantasten worden deze gegevens door een tweede persoon geïnspecteerd en geaccepteerd. Van de acceptatie wordt een log bijgehouden.
4. Verantwoordelijkheden voor beheer, wijziging van gegevens en bijbehorende informatiesysteemfuncties moeten eenduidig toegewezen zijn aan één specifieke (beheerders)rol.

10.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie

Faciliteiten voor ontwikkeling, testen en productie behoren te zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.

Waterschap specifieke maatregel

1. Er zijn minimaal logisch gescheiden systemen voor Ontwikkeling, Test en/of Acceptatie en Productie (OTAP). De systemen en applicaties in deze zones beïnvloeden systemen en applicaties in andere zones niet.
2. Gebruikers hebben gescheiden gebruiksprofielen voor Ontwikkeling, Test en/of Acceptatie en Productiesystemen om het risico van fouten te verminderen. Het moet duidelijk zichtbaar zijn in welk systeem gewerkt wordt.
3. Indien er een experimenteer of laboratorium omgeving is, is deze fysiek gescheiden van de productieomgeving.

10.2 Exploitatie door een derde partij

Doelstelling

Een geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij.

10.2.1 Dienstverlening

Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.

Waterschap specifieke maatregel

1. De uitbestedende partij blijft verantwoordelijk voor de betrouwbaarheid van uitbestede diensten.
2. Uitbesteding is goedgekeurd door de voor het informatiesysteem verantwoordelijke lijnmanager.

10.2.2 Controle en beoordeling van dienstverlening door een derde partij

De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.

Waterschap specifieke maatregel

1. Er worden afspraken gemaakt over de inhoud van rapportages, zoals over het melden van incidenten en autorisatiebeheer.
2. De in dienstverleningscontracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld middels audits of rapportages en gebeurt minimaal eens per jaar (voor ieder systeem).
3. Er zijn voor beide partijen eenduidige aanspreekpunten.

10.2.3 Beheer van wijzigingen in dienstverlening door een derde partij

Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, behoren te worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.

Waterschap specifieke maatregel

1. Zie 10.1.2

10.3 Systeemplanning en –acceptatie

Doelstelling

Het risico van systeemstoringen tot een minimum beperken.

10.3.1 Capaciteitsbeheer

Het gebruik van middelen behoort te worden gecontroleerd en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen, om de vereiste systeemprestaties te bewerkstelligen.

Waterschap specifieke maatregel

1. De ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en

metingen die het gebruik van een component vaststellen).
Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen.
Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheid eis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen.

2. Er worden beperkingen opgelegd aan gebruikers en systemen ten aanzien van het gebruik van gemeenschappelijke middelen, zodat een enkele gebruiker (of systeem) niet meer van deze middelen kan opeisen dan nodig is voor de uitvoering van zijn of haar taak en daarmee de beschikbaarheid van systemen voor andere gebruikers (of systemen) in gevaar kan brengen.
3. In koppelpunten met externe of onvertrouwde zones worden maatregelen getroffen om aanvallen te signaleren en hierop te reageren. Het gaat hier om aanvallen die erop gericht zijn de verwerkingscapaciteit zodanig te laten vollopen, dat onbereikbaarheid of uitval van computers het gevolg is.[4]

\

10.3.2 Systeem acceptatie

Er behoren aanvaardingscriteria te worden vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er behoort een geschikte test van het systeem of de systemen te worden uitgevoerd tijdens ontwikkeling en voorafgaand aan de acceptatie.

Waterschap specifieke maatregel

1. Van acceptatietesten wordt een log bijgehouden.
2. Er zijn acceptatiecriteria vastgesteld voor het testen van de beveiliging.

10.4 Bescherming tegen virussen en “mobile code” [5]

Doelstelling

Beschermen van de integriteit van programmatuur en informatie.

10.4.1 Maatregelen tegen virussen

Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.

4 Zie bijvoorbeeld de GovCert aanbevelingen: http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/dienstverlening/kennis-en-publicaties/whitepapers/bescherming-tegen-ddos-aanvallen/bescherming-tegen-ddos-aanvallen/govcert%3AdocumentResource/govcert%3Aresource

5 Malicious Mobile Code = kwaadaardige mobiele code: een term om allerlei slechte programma’s te beschrijven: virussen, wormen, Trojaanse paarden en rogue Internet content.

Waterschap specifieke maatregel

1. Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats.
2. Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, (automatisch) plaats.
3. In verschillende schakels van een keten binnen de infrastructuur van een organisatie wordt bij voorkeur antivirusprogrammatuur van verschillende leveranciers toegepast.
4. Er zijn maatregelen om verspreiding van virussen tegen te gaan en daarmee schade te beperken (bijv. quarantaine en compartimentering).
5. Er zijn continuïteitsplannen voor herstel na aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.
6. Op mobile devices wordt antivirus software toegepast

10.4.2 Maatregelen tegen 'mobile code'

Als gebruik van 'mobile code' is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde 'mobile code' functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden voorkomen dat onbevoegde 'mobile code' wordt uitgevoerd.

Waterschap specifieke maatregel

1. Mobile code wordt uitgevoerd in een logisch geïsoleerde omgeving (sandbox) 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 wordt aangetast.
2. Een gebruiker moet geen extra rechten kunnen toekennen aan programma's (bijv. internet browsers) die mobile code uitvoeren.

10.5 Back-up

Doelstelling

Handhaven van de integriteit en beschikbaarheid van informatie en IT voorzieningen.

10.5.1 Reservekopieën maken (back-ups)

Er behoren back-upkopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig het vastgestelde back-up beleid.

Waterschap specifieke maatregel

1. Er zijn periodiek geteste procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.
2. Back-upstrategieën zijn vastgesteld op basis van het soort gegevens (bestanden, databases, enz.), de maximaal toegestane periode waarover gegevens verloren mogen raken, en de maximaal toelaatbare back-up- en hersteltijd.
3. Van back-upactiviteiten en de verblijfplaats van de media wordt een registratie bijgehouden, met een kopie op een andere locatie. De andere locatie is zodanig gekozen dat een incident/calamiteit op de oorspronkelijke locatie niet leidt tot schade aan of toegang tot de kopie van die registratie. (zie 9.1.4.2)
4. Back-ups worden bewaard op een locatie die zodanig is gekozen dat een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-up.
5. De fysieke en logische toegang tot de back-ups, zowel van systeemschijven als van data, is zodanig geregeld dat alleen geautoriseerde personen zich toegang kunnen verschaffen tot deze back-ups.

10.6 Beheer van netwerkbeveiliging

Doelstelling

Bewerkstelligen van de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur.

10.6.1 Maatregelen voor netwerken

Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.

Waterschap specifieke maatregel

1. 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 komt.
2. Gegevensuitwisseling tussen vertrouwde en onvertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
3. Bij transport van vertrouwelijke informatie over onvertrouwde netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe 10.3.1.3.
4. Er zijn procedures voor beheer van netwerkapparatuur op afstand.

10.6.2 Beveiliging van netwerkdiensten

Beveiligingskenmerken, niveaus van dienstverlening en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.

10.7 Behandeling van media

Doelstelling

Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten.

10.7.1 Beheer van verwijderbare media

Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media.

Waterschap specifieke maatregel

1. Er zijn procedures opgesteld en geïmplementeerd voor opslag van vertrouwelijke informatie voor verwijderbare media. Voetnoot: toepassen van encryptie bij usb sticks
2. Verwijderbare media met vertrouwelijke informatie mogen niet onbeheerd worden achtergelaten op plaatsen die toegankelijk zijn zonder toegangscontrole.
3. Informatie die langer beschikbaar moet zijn dan de levensduur van de media waarop hij is opgeslagen behoort te worden gekopieerd wanneer 75% van de levensduur van het medium is verstreken.

10.7.2 Verwijdering van media

Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.

Waterschap specifieke maatregel

1. Er zijn procedures vastgesteld en in werking voor verwijderen van vertrouwelijke data en de vernietiging van verwijderbare media. Verwijderen van data wordt gedaan met een gecertificeerde methode voor wissen van data, afhankelijk van classificering van data[6] voor apparaten waar dit mogelijk is. In overige gevallen wordt de data twee keer overschreven met vaste data, één keer met random data en vervolgens wordt geverifieerd of het overschrijven is gelukt. Zie ook 9.2.6.

6 G.F. Hughes, D.M. Commins, and T. Coughlin, Disposal of disk and tape data by secure sanitization, IEEE Security and Privacy, Vol. 7, No. 4, (July/August 2009), pp. 29-34.

10.7.3 Procedures voor de behandeling van informatie

Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.

10.7.4 Beveiliging van systeemdocumentatie

Systeemdocumentatie behoort te worden beschermd tegen onbevoegde toegang.

Waterschap specifieke maatregel

1. Systeemdocumentatie die vertrouwelijke informatie bevat is niet vrij toegankelijk.
2. Wanneer de eigenaar er expliciet voor kiest om gerubriceerde systeemdocumentatie buiten het waterschap te brengen, doet hij dat niet zonder risicoafweging.

10.8 Uitwisseling van informatie

Doelstelling

Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe entiteit.

10.8.1 Beleid en procedures voor informatie-uitwisseling

Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.

Waterschap specifieke maatregel

1. Het meenemen van geclassificeerde informatie buiten het waterschap vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is.
2. Medewerkers zijn geïnstrueerd om zodanig om te gaan met (telefoon) gesprekken, e-mail, faxen, ingesproken berichten op antwoordapparaten en het gebruik van de diverse digitale berichtendiensten dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt.
3. Medewerkers zijn geïnstrueerd om zodanig om te gaan met mobiele apparatuur en verwijderbare media dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt. Hierbij wordt ten minste aandacht besteed aan het risico van adreslijsten en opgeslagen boodschappen in mobiele telefoons.
4. Medewerkers zijn geïnstrueerd om geen vertrouwelijke documenten bij de printer te laten liggen.
5. Er zijn maatregelen getroffen om het automatisch doorsturen van interne e-mail berichten naar externe e-mail adressen te voorkomen.

10.8.2 Uitwisselingsovereenkomsten

Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.

Waterschap specifieke maatregel

1. Er zijn afspraken gemaakt over de beveiliging van de uitwisseling van gegevens en software tussen organisaties waarin de maatregelen om betrouwbaarheid - waaronder traceerbaarheid en onweerlegbaarheid - van gegevens te waarborgen zijn beschreven en getoetst.
2. Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, alsmede procedures over melding van incidenten.
3. Het eigenaarschap van gegevens en programmatuur en de verantwoordelijkheid voor de gegevensbescherming, auteursrechten, licenties van programmatuur zijn vastgelegd.
4. Indien mogelijk wordt binnenkomende programmatuur (zowel op fysieke media als gedownload) gecontroleerd op ongeautoriseerde wijzigingen aan de hand van een door de leverancier via een gescheiden kanaal geleverde checksum of certificaat.

10.8.3 Fysieke media die worden getransporteerd

Media die informatie bevatten behoren te worden beschermd tegen onbevoegde toegang, misbruik of corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.

Waterschap specifieke maatregel

1. Om vertrouwelijke informatie te beschermen worden maatregelen genomen, zoals:
   - versleuteling
   - bescherming door fysieke maatregelen, zoals afgesloten containers of archief verzegeling
   - gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen
   - persoonlijke aflevering
   - opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes

10.8.4 Elektronisch berichtenuitwisseling

Informatie die een rol speelt bij elektronisch berichtenverkeer behoort op geschikte wijze te worden beschermd.

Waterschap specifieke maatregel

1. Digitale documenten binnen het waterschap waar eindgebruikers rechten aan kunnen ontlenen maken gebruik van bijvoorbeeld PKI Overheid certificaten voor tekenen en/of encryptie.
2. Er is een (spam) filter geactiveerd voor e-mail berichten.

10.8.5 Systemen voor bedrijfsinformatie

Beleid en procedures behoren te worden ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van systemen voor bedrijfsinformatie.

Waterschap specifieke maatregel

1. Er zijn richtlijnen met betrekking tot het bepalen van de risico's die het gebruik van waterschaps informatie in kantoorapplicaties met zich meebrengen en richtlijnen voor de bepaling van de beveiliging van deze informatie binnen deze kantoorapplicaties. Hierin is minimaal aandacht besteed aan de toegang tot de interne informatievoorziening, toegankelijkheid van agenda's, afscherming van documenten, privacy, beschikbaarheid, back-up en in voorkomend geval cloud diensten.

10.9 Diensten voor e-commerce

Doelstelling

Bewerkstelligen van de beveiliging van diensten voor e-commerce, en veilig gebruik ervan.

10.9.1 E-commerce

Informatie die een rol speelt bij e-commerce en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en modificatie.

Waterschap specifieke maatregel

1. Conform verplichting wordt gebruik gemaakt van en voldaan aan de eisen van de authentieke basisregistraties en aangewezen voorzieningen van de overheid gebruikt.

10.9.2 Onlinetransacties

Informatie die een rol speelt bij onlinetransacties behoort te worden beschermd om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking, onbevoegde duplicatie of weergave van berichten te voorkomen.

Waterschap specifieke maatregel

1. Een transactie wordt bevestigd (geautoriseerd) door een elektronische handtekening of een andere vorm van wettelijk geldige authenticatie.

10.9.3 Openbaar beschikbare informatie

De betrouwbaarheid van de informatie die beschikbaar wordt gesteld op een openbaar toegankelijk systeem behoort te worden beschermd om onbevoegde modificatie te voorkomen.

Waterschap specifieke maatregel

1. Er zijn procedures die waarborgen dat gepubliceerde informatie is aangeleverd door daartoe geautoriseerde medewerkers.

10.10 Controle

Doelstelling

Ontdekken van onbevoegde informatieverwerkingsactiviteiten.

10.10.1 Aanmaken audit-logbestanden

Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.

Waterschap specifieke maatregel

1. Er dient een procedure te zijn hoe wordt omgegaan met logging.
2. Van logbestanden worden rapportages gemaakt die periodiek worden beoordeeld. Deze periode dient te worden gerelateerd aan de mogelijkheid van misbruik en de schade die kan optreden. De GBA logging kan bijvoorbeeld dagelijks nagelopen worden, evenals financiële systemen, controle van het Internet gebruik kan bijvoorbeeld per maand of kwartaal.
3. Een log-regel bevat minimaal:
4. Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID
5. De gebeurtenis (zie 10.10.2.1)
6. Waar mogelijk de identiteit van het werkstation of de locatie
7. Het object waarop de handeling werd uitgevoerd
8. Het resultaat van de handeling
9. De datum en het tijdstip van de gebeurtenis
10. In een log-regel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, enz.).
11. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.
    Controle op opslag van logging: het vol lopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijv. een logserver die niet bereikbaar is).

10.10.2 Controle van systeemgebruik

Er behoren procedures te worden vastgesteld om het gebruik van IT voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.

Waterschap specifieke maatregel

1. De volgende gebeurtenissen worden in ieder geval opgenomen in de logging:
   - gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore.
   - gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases).
   - handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels.
   - beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services).
   - verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen).
   - logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren aangesloten op een Security Information and Event Management Systeem[7] waarmee meldingen en alarmoproepen aan de beheerorganisatie gegeven worden. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.

10.10.3 Bescherming van informatie in logbestanden

Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.

10.10.4 Logbestanden van administrators en operators

Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd.

10.10.5 Registratie van storingen

Storingen behoren in logbestanden te worden vastgelegd en te worden geanalyseerd en er behoren geschikte maatregelen te worden genomen.

7 Een SIEM systeem kan, afhankelijk van de context, meer of minder uitgebreid zijn. Essentieel is dat de loggegevens van beveiligingscomponenten en authenticatiemiddelen dusdanig overzichtelijk worden gepresenteerd dat belangrijke meldingen niet gemist worden.

10.10.6 Synchronisatie van systeemklokken

De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

11 Toegangsbeveiliging

11 Toegangsbeveiliging

11.1 Toegangsbeleid

Doelstelling
Beheersen van de toegang tot informatie.

Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van organisatie-eisen en beveiligingseisen voor toegang.

11.2 Beheer van toegangsrechten van gebruikers

Doelstelling
Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen.

11.2.1 Registratie van gebruikers

Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.

Waterschap specifieke maatregel

1. Gebruikers worden vooraf geïdentificeerd en geautoriseerd. Van de registratie wordt een administratie bijgehouden.
2. Op basis van een risicoafweging wordt bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.

11.2.2 Beheer van (speciale) bevoegdheden

De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.

11.2.3 Beheer van gebruikerswachtwoorden

De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.

Waterschap specifieke maatregel

1. Wachtwoorden worden nooit in originele vorm (onversleuteld) opgeslagen of verstuurd.
   - Ten aanzien van wachtwoorden geldt:
   - Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker).
   - Tijdelijke wachtwoorden of wachtwoorden die standaard in software of hardware worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord.
   - Gebruikers bevestigen de ontvangst van een wachtwoord.
   - Wachtwoorden zijn alleen bij de gebruiker bekend.
   - Wachtwoorden bestaan uit minimaal 8 karakters, waarvan tenminste 1 hoofdletter, 1 cijfer en 1 vreemd teken.
   - Wachtwoorden zijn maximaal 60 dagen geldig en mogen niet binnen 6 keer herhaald worden.

11.2.4 Beoordeling van toegangsrechten van gebruikers

Het management behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces.

Waterschap specifieke maatregel

1. Toegangsrechten van gebruikers worden periodiek, minimaal jaarlijks, geëvalueerd. Het interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau.

11.3 Verantwoordelijkheden van gebruikers

Doelstelling

Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en ICT-voorzieningen. Gebruik van wachtwoorden

11.3.1 Gebruik van wachtwoorden

Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.

Waterschap specifieke maatregel

1. Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende:
   - Wachtwoorden worden niet opgeschreven.
   - Gebruikers delen hun wachtwoord nooit met anderen.
   - Wachtwoorden mogen niet opeenvolgend zijn.
   - Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde.
   - Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijv. opgeslagen onder een functietoets of in een macro).

11.3.2 Onbeheerde gebruikersapparatuur

Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.

Waterschap specifieke maatregel

1. De gebruiker vergrendelt de werkplek tijdens afwezigheid. (zie ook : 11.5.5)

11.3.3 Clear desk en clear screen

Er behoort een 'clear desk'-beleid voor papier en verwijderbare opslagmedia en een 'clear screen'-beleid voor ICT-voorzieningen te worden ingesteld.

Waterschap specifieke maatregel

1. In het clear desk beleid staat minimaal dat de gebruiker geen vertrouwelijke informatie op het bureau mag laten liggen. Deze informatie moet altijd worden opgeborgen in een afsluitbare opbergmogelijkheid (kast, locker, bureau of kamer).
2. Bij afdrukken van gevoelige informatie wordt, wanneer mogelijk, gebruik gemaakt van de functie 'beveiligd afdrukken' (pincode verificatie).
3. Schermbeveiligingsprogrammatuur (een screensaver) maakt na een periode van inactiviteit van maximaal 15 minuten alle informatie op het beeldscherm onleesbaar en ontoegankelijk.

11.4 Toegangsbeheersing voor netwerken

Doelstelling

Het voorkomen van onbevoegde toegang tot netwerkdiensten.

11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten

Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn.

11.4.2 Authenticatie van gebruikers bij externe verbindingen

Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen.

Waterschap specifieke maatregel

1. Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.

11.4.3 Identificatie van (netwerk)apparatuur

Automatische identificatie van apparatuur behoort te worden overwogen als methode om verbindingen vanaf specifieke locaties en apparatuur te authentiseren.

Waterschap specifieke maatregel

1. Alleen geïdentificeerde en geauthentiseerde apparatuur kan worden aangesloten op een vertrouwde zone. Eigenapparatuur (BringYour-Own Device) wordt niet aangesloten op een vertrouwde zone.

11.4.4 Bescherming op afstand van poorten voor diagnose en configuraties

De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst.

Waterschap specifieke maatregel

Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst dienen te worden afgesloten.

11.4.5 Scheiding van netwerken

Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.

Waterschap specifieke maatregel

1. Werkstations worden zo ingericht dat routeren van verkeer tussen verschillende zones of netwerken niet mogelijk is.
2. De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze staan. Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.
3. Elke zone heeft een gedefinieerd beveiligingsniveau Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.
4. Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.
5. Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).

11.4.6 Beheersmaatregelen voor netwerkverbindingen

Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangsmogelijkheden voor gebruikers te worden beperkt, overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen (zie 11.1).

11.4.7 Beheersmaatregelen voor netwerkroutering

Netwerken behoren te zijn voorzien van beheersmaatregelen voor netwerkroutering, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoepassingen.

Waterschap specifieke maatregel

1. Netwerken zijn voorzien van beheersmaatregelen voor routering gebaseerd op mechanismen ter verificatie van bron en bestemmingsadressen.

11.5 Toegangsbeveiliging voor besturingssystemen

Doelstelling

Voorkomen van onbevoegde toegang tot besturingssystemen.

11.5.1 Beveiligde inlogprocedures

Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.

Waterschap specifieke maatregel

1. Toegang tot bedrijfskritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie.
2. Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.

11.5.2 Gebruikersindentificatie en –authenticatie

Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.

Waterschap specifieke maatregel

1. Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.
2. Bij het intern gebruik van IT voorzieningen worden gebruikers minimaal geauthenticeerd op basis van wachtwoorden.
3. Applicaties mogen niet onnodig en niet langer dan noodzakelijk onder een systeemaccount (een privileged user zoals administrator of root) draaien. Direct na het uitvoeren van handelingen waar hogere rechten voor nodig zijn, wordt weer teruggeschakeld naar het niveau van een gewone gebruiker (een unprivileged user).

11.5.3 Systemen voor wachtwoordenbeheer

Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

Waterschap specifieke maatregel

1. Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (o.a. voldoende sterke wachtwoorden[8], regelmatige wijziging, directe wijziging van initieel wachtwoord).
2. Wachtwoorden hebben een geldigheidsduur zoals beschreven bij 11.2.3. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.
3. Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd.
4. De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende:
   - Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd.
   - Ter voorkoming van typefouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure.

11.5.4 Gebruik van systeemhulpmiddelen

Het gebruik van hulpprogrammatuur waarmee systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd behoort te worden beperkt en behoort strikt te worden beheerst.

11.5.5 Time-out van sessies

Inactieve sessies behoren na een vastgestelde periode van inactiviteit te worden uitgeschakeld.

Waterschap specifieke maatregel

1. De periode van inactiviteit van het gebruik van een informatiesysteem is vastgesteld op maximaal 15 minuten. Daarna wordt de sessie afgebroken.
2. Bij remote desktop sessies geldt dat na maximaal 15 minuten inactiviteit de sessie verbroken wordt.

11.5.6 Beperking van verbindingstijd

De verbindingstijd behoort te worden beperkt als aanvullende beveiliging voor toepassingen met een verhoogd risico.

8 Een voldoende sterk wachtwoord is een wachtwoord waarvan de entropie hoog is, deze is afhankelijk van de lengte en het aantal mogelijke tekens. Zie ook 'The true costs of unusable password policies', en Gartner research note G00124970 (http://www.indevis.de/dokumente/gartner_passwords_breakpoint.pdf).

Waterschap specifieke maatregel

1. De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis een wijzigingsverzoek of storingsmelding.

11.6 Toegangsbeheersing voor toepassingen en informatie

Doelstelling

Voorkomen van onbevoegde toegang tot informatie in toepassingssystemen.

11.6.1 Beperken van toegang tot informatie

Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid.

11.6.2 Isoleren van gevoelige systemen

Gevoelige systemen behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben.

Waterschap specifieke maatregel

1. Bedrijfskritieke systemen behoren een eigen vast toegewezen (geïsoleerde) computeromgeving te hebben. Isoleren kan worden bereikt door fysieke of logische methoden.

11.7 Draagbare computers en telewerken

Doelstelling

Waarborgen van informatiebeveiliging bij het gebruik van alle vormen van draagbare computers en faciliteiten voor telewerken.

11.7.1 Draagbare computers en communicatievoorzieningen

Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.

Waterschap specifieke maatregel

1. Het mobiele apparaat is zo ingericht dat geen bedrijfsinformatie wordt opgeslagen ("zero footprint"). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, geldt: een mobiel apparaat (zoals een handheld computer, tablet, smartphone, PDA) biedt de mogelijkheid om de toegang te beschermen d.m.v. een wachtwoord en versleuteling van die gegevens.
   Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats.

2. Er zijnvoorzieningen om de actualiteit van anti-malware programmatuur op mobiele apparaten te garanderen.
   Bij melding van verlies of diefstal wordt de communicatiemogelijkheid met de centrale applicaties afgesloten.

11.7.2 Telewerken

Er behoort beleid, operationele plannen en procedures voor telewerken te worden ontwikkeld en geïmplementeerd.

Waterschap specifieke maatregel

1. Er wordt een beleid met gedragsregels en een geschikte implementatie van de techniek opgesteld t.a.v. telewerken.
2. Er wordt beleid vastgesteld met daarin de uitwerking welke systemen niet en welke systemen wel vanuit de thuiswerkplek of andere telewerkvoorzieningen mogen worden geraadpleegd.
3. De telewerkvoorzieningen zijn waar mogelijk zo ingericht dat op de werkplek (thuis of op een andere locatie) geen bedrijfsinformatie wordt opgeslagen (“zero footprint”) en mogelijke malware vanaf de werkplek niet in het vertrouwde deel terecht kan komen.
4. Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats.

12 Verwerving, ontwikkeling en onderhoud van Informatiesystemen

12 Verwerving, ontwikkeling en onderhoud van Informatiesystemen

12.1 Beveiligingseisen voor informatiesystemen

Doelstelling
Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

12.1.1 Analyse en specificatie van beveiligingseisen

In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.

Waterschap specifieke maatregel

1. In projecten worden een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.
2. In standaarden voor analyse, ontwikkeling en testen van informatiesystemen wordt structureel aandacht besteed aan beveiligingsaspecten.
3. Bij aanschaf van producten wordt een proces gevolgd waarbij beveiliging een onderdeel is van de specificatie.
4. Waar het gaat om beveiligingsrelevante producten wordt de keuze voor een bepaald product verantwoord onderbouwd.
5. Er is expliciet aandacht voor leveranciers accounts, hardcoded wachtwoorden en mogelijke 'achterdeurtjes'.

12.2 Correcte verwerking in toepassingen

Doelstelling
Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen.

12.2.1 Validatie van invoergegevens

Gegevens die worden ingevoerd in toepassingen behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn.

Waterschap specifieke maatregel

1. Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, toevoegen van parameters en inconsistentie van gegevens.

12.2.2 Beheersing van interne gegevensverwerking

Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken.

Waterschap specifieke maatregel

1. Stapelen van fouten wordt voorkomen door toepassing van 'noodstop' mechanismen.
2. Verwerkingen zijn bij voorkeur herstelbaar zodat bij het optreden van fouten en/of wegraken van informatie dit hersteld kan worden door het opnieuw verwerken van de informatie.

12.2.3 Integriteit van berichten

Er behoren eisen te worden vastgesteld, en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.

12.2.4 Validatie van uitvoergegevens

Gegevensuitvoer uit een toepassing behoort te worden gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en geschikt is gezien de omstandigheden.

Waterschap specifieke maatregel

1. De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).
2. Bij uitvoer van gegevens wordt gegarandeerd dat deze met het juiste niveau van vertrouwelijkheid beschikbaar gesteld worden (bijv. beveiligd printen).
3. Alleen gegevens die noodzakelijk zijn voor de doeleinden van de gebruiker worden uitgevoerd (need-to-know).

12.3 Cryptografische beheersmaatregelen

Doelstelling

Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen.

12.3.1 Beleid voor het gebruik van cryptografische-beheersmaatregelen

Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.

Waterschap specifieke maatregel

1. De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.
2. Bij de inzet van cryptografische producten volgt een afweging van de risico's aangaande locaties, processen en gebruikers.
3. De cryptografische beveiligingsvoorzieningen waarin de cryptografische algoritmen zijn opgenomen zijn ook informatiesystemen en voldoen ook aan de geldende beveiligingscriteria.

12.3.2 Sleutelbeheer

Er behoort sleutelbeheer te zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.

Waterschap specifieke maatregel

1. In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.
2. De geldigheidsduur van cryptografische sleutels wordt bepaald aan de hand van de beoogde toepassing en is vastgelegd in het cryptografisch beleid.
3. De vertrouwelijkheid van cryptografische sleutels dient te zijn gewaarborgd tijdens generatie, gebruik, transport en opslag van de sleutels.
4. Er is een procedure vastgesteld waarin is bepaald hoe wordt omgegaan met gecompromitteerde sleutels.
5. Bij gebruik van overheidsdiensten die dat vereisen is sleutelmanagement ingericht volgens PKI Overheid.

12.4 Beveiliging van systeembestanden

Doelstelling

Beveiliging van systeembestanden bewerkstelligen.

12.4.1 Beheersing van operationele programmatuur

Er behoren procedures te zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen.

Waterschap specifieke maatregel

1. Alleen geautoriseerd personeel kan functies en software installeren of activeren.
2. Programmatuur behoort pas te worden geïnstalleerd op een productieomgeving na een succesvolle test en acceptatie.
3. Geïnstalleerde programmatuur, configuraties en documentatie worden bijgehouden in een configuratiedatabase.
4. Er worden alleen door de externe of interne leverancier onderhouden (versies van) software gebruikt.
5. Van updates wordt een log bijgehouden.
6. Er is een rollbackstrategie.

12.4.2 Bescherming van testdata

Testgegevens behoren zorgvuldig te worden gekozen, beschermd en beheerst.

Waterschap specifieke maatregel

1. Het gebruik van kopieën van operationele data voor testdoeleinden moet worden vermeden. Indien noodzakelijk, worden geanonimiseerde gegevens gebruikt welke na de test zorgvuldig worden verwijderd.

12.4.3 Toegangsbeheersing voor broncode van programmatuur

De toegang tot broncode van programmatuur behoort te worden beperkt.

Waterschap specifieke maatregel

1. De toegang tot broncode wordt zoveel mogelijk beperkt om de code tegen onbedoelde wijzigingen te beschermen. Alleen geautoriseerde personen hebben toegang.
2. Broncode staat op aparte (logische) systemen.

12.5 Beveiliging bij ontwikkelings- en ondersteuningsprocessen

Doelstelling

Beveiliging van toepassingsprogrammatuur en -informatie handhaven.

12.5.1 Procedures voor wijzigingsbeheer

De implementatie van wijzigingen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer.

12.5.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem

Bij wijzigingen in besturingssystemen behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.

Waterschap specifieke maatregel

1. Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen.

12.5.3 Restricties op wijzigingen in programmatuurpakketten

Wijzigingen in programmatuurpakketten behoren te worden ontmoedigd, te worden beperkt tot noodzakelijke wijzigingen, en alle wijzigingen behoren strikt te worden beheerst.

Waterschap specifieke maatregel

1. Bij het instellen van besturingsprogrammatuur en programmapakketten wordt uitgegaan van de aanwijzingen van de leverancier.

12.5.4 Uitlekken van informatie

Er behoort te worden voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken.

Waterschap specifieke maatregel

1. Er dient een proces te zijn om te melden dat (persoons) informatie is uitgelekt. (zie 13.1.1)

12.5.5 Uitbestede ontwikkeling van programmatuur

Uitbestede ontwikkeling van programmatuur behoort onder supervisie te staan van en te worden gecontroleerd door de organisatie.

Waterschap specifieke maatregel

1. Uitbestede ontwikkeling van programmatuur komt tot stand onder supervisie en verantwoordelijkheid van de uitbestedende organisatie. Er worden maatregelen getroffen om de kwaliteit en vertrouwelijkheid te borgen (bijv. stellen van veiligheidseisen, regelen van beschikbaarheid en eigendomsrecht van de code, certificatie, kwaliteitsaudits, testen en aansprakelijkheidsregelingen).

12.6 Beheer van technische kwetsbaarheden

Doelstelling

Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.

12.6.1 Beheersing van technische kwetsbaarheden

Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.

Waterschap specifieke maatregel

1. Er is een proces ingericht voor het beheer van technische kwetsbaarheden; dit omvat minimaal het melden van incidenten aan het centrale aanspreekpunt voor incidenten bij de waterschappen, periodieke penetratietests, risicoanalyses van kwetsbaarheden en patching.
2. Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de

laatste updates (patches) in zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de leverancier.

3. Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).
4. Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde.
5. Indien nog geen patch beschikbaar is dient gehandeld te worden volgens het advies van het centrale aanspreekpunt voor informatiebeveiligingbij de waterschappen, de Informatiebeveiligingsdienst of een andere CERT zoals het NCSC.

13 Beheer van Informatiebeveiligingsincidenten

13 Beheer van Informatiebeveiligingsincidenten

13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

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

13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen

Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.

Waterschap specifieke maatregel

1. Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld.
2. Er is een procedure waarin wordt beschreven hoe met een aangemeld beveiligingsincident wordt omgegaan.
3. Er is een procedure voor communicatie met het centrale aanspreekpunt voor incidenten bij de waterschappen.
4. Er is een contactpersoon aangewezen voor het rapporteren van beveiligingsincidenten. Voor integriteitsschendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt.
5. Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan het centrale aanspreekpunt voor incidenten bij de waterschappen.
6. Vermissing of diefstal van apparatuur of media die gegevens van het waterschap kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.
7. Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De CISO bekijkt periodiek – bij voorkeur maandelijks - een samenvatting van de informatie.

13.1.2 Rapportage van zwakke plekken in de beveiliging

Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en –diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren.

Waterschap specifieke maatregel

1. Er is een procedure om eenvoudig en snel beveiligingsincidenten en zwakke plekken in de beveiliging te melden.

13.2 Beheer van informatiebeveiligingsincidenten en verbeteringen

Doelstelling
Bewerkstelligen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.

13.2.1 Verantwoordelijkheden en procedures

Er behoren verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.

Waterschap specifieke maatregel

1. Er zijn procedures voor rapportage van gebeurtenissen en escalatie. Alle medewerkers behoren op de hoogte te zijn van deze procedures.

13.2.2 Leren van informatiebeveiligingsincidenten

Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd.

Waterschap specifieke maatregel

1. De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren. (PDCA Cyclus).

13.2.3 Verzamelen van bewijsmateriaal

Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

Waterschap specifieke maatregel

1. Er is een procedure voor het verzamelen van bewijsmateriaal vastgelegd.

14 Bedrijfscontinuïteitsbeheer

14 Bedrijfscontinuïteitsbeheer

14.1 Informatiebeveiligingsaspecten van bedrijfscontinuiteïtsbeheer

Doelstelling

Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritieke bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

14.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer

Er behoort een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering.

Waterschap specifieke maatregel

1. Er worden plannen opgesteld voor de jaarlijkse bewustwording-, training- en testactiviteiten.

14.1.2 Bedrijfscontinuïteit en risicobeoordeling

Gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden, behoren te worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatiebeveiliging.

Waterschap specifieke maatregel

1. Gebeurtenissen worden geïdentificeerd die kunnen leiden tot discontinuïteit in het bedrijfsproces. De waarschijnlijkheid en de gevolgen van de discontinuïteit worden in kaart gebracht in termen van tijd, schade en herstelperiode.

14.1.3 Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging

Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vooraf afgesproken niveau en binnen in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritieke bedrijfsprocessen.

Waterschap specifieke maatregel

1. In de continuïteitsplannen wordt minimaal aandacht besteed aan:
   - Identificatie van essentiële procedures voor bedrijfscontinuïteit.
   - Wie het plan mag activeren en wanneer, maar ook wanneer er weer gecontroleerd teruggaan wordt.
   - Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie).
   - Prioriteiten en volgorde van herstel en reconstructie.
   - Documentatie van systemen en processen.
   - Kennis en kundigheid van personeel om de processen weer op te starten.

14.1.4 Kader voor de bedrijfscontinuïteitsplanning

Er behoort een enkelvoudig kader voor bedrijfscontinuïteitsplannen te worden gehandhaafd om te bewerkstelligen dat alle plannen consistent zijn, om eisen voor informatiebeveiliging op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud.

14.1.5 Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen

Bedrijfscontinuïteitsplannen behoren regelmatig te worden getest en geüpdate, om te bewerkstelligen dat ze actueel en doeltreffend blijven.

Waterschap specifieke maatregel

1. Er worden minimaal jaarlijks oefeningen en/of testen gehouden om de bedrijfscontinuïteitsplannen en mate van gereedheid van de organisatie te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.

15 Naleving

15 Naleving

15.1 Naleving van wettelijke voorschriften

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

15.1.1 Identificatie van toepasselijke wetgeving
Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden voor elk informatiesysteem en voor de organisatie.

15.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights)
Er behoren geschikte procedures te worden geïmplementeerd om te bewerkstelligen dat wordt voldaan aan de wettelijke en regelgevende eisen en contractuele verplichtingen voor het gebruik van materiaal waarop intellectuele eigendomsrechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendomsrechten berusten.

Waterschap specifieke maatregel
1. Er is toezicht op het naleven van wettelijke verplichtingen m.b.t. intellectueel eigendom, auteursrechten en gebruiksrechten.

15.1.3 Bescherming van bedrijfsdocumenten
Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.

15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens
De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen. [9]

15.1.5 Voorkomen van misbruik van IT voorzieningen
Gebruikers behoren ervan te worden weerhouden IT voorzieningen te gebruiken voor onbevoegde doeleinden.

9 Zie artikel 12 WBP

Waterschap specifieke maatregel

1. Er is een beleid met betrekking tot het gebruik van IT voorzieningen door gebruikers. Dit beleid is bekendgemaakt en op de goede werking ervan wordt toegezien.

15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Cryptografische beheersmaatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt.

1. Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen. Zie ook 12.3.

15.2 Naleving van beveiligingsbeleid en -normen en technische naleving

Doelstelling

Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.

15.2.1 Naleving van beveiligingsbeleid en -normen

Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.

Waterschap specifieke maatregel

1. Het lijnmanagement is verantwoordelijk voor uitvoering en beveiligingsprocedures, en toetsing daarop (o.a. jaarlijkse in control verklaring). Conform het BIWA (strategisch kader) zorgt de CISO, namens de secretaris-directeur, voor het toezicht op de uitvoering van het beveiligingsbeleid. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door of vanwege de CISO dan wel door interne of externe auditteams.
2. In de P&C cyclus wordt gerapporteerd over informatiebeveiliging aan de hand van het in control statement.

15.2.2 Controle op technische naleving

Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen.

Waterschap specifieke maatregel

1. Informatiesystemen worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijv. kwetsbaarheidsanalyses en penetratietesten. Zie ook 12.6.1.1.

15.3 Overwegingen bij audits van informatiesystemen

Doelstelling
Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren.

15.3.1 Beheersmaatregelen voor audits van informatiesystemen

Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, behoren zorgvuldig te worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken.

15.3.2 Bescherming van hulpmiddelen voor audits van informatiesystemen

Toegang tot hulpmiddelen voor audits van informatiesystemen behoort te worden beschermd om mogelijk misbruik of compromitteren te voorkomen.

Bijlage A Documentenbeheer
Strategisch en Tactisch normenkader

Bijlage A Documentenbeheer Strategisch en Tactisch normenkader

Documentbeheer Strategisch normenkader

Documenthistorie

Datum	Versie	Auteur	Opmerkingen
03-05-13	0.01		
13-05-13	0.1		
16-05-13	0.2		
27-05-13	0.3		
10-06-13	0.4		
14-06-13	0.9		

Goedkeuring

Datum	Versie	Akkoord door	Opmerkingen
21-06-13	0.9	Werkgroep middelen	

Meer informatie	
Het Waterschapshuis/UvW	informatiebeveiliging@hetwaterschapshuis.nl

Bronnen Strategisch normenkader

Titel	Auteur	Jaar	Omschrijving
13-0313 Baseline informatiebeveiliging Gemeenten (SNK) strategisch normenkader 0.99b VNG/KING-IBD		2013	
Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten mei 2013 versie 1.0 IBD	VNG/KING-IBD	2013	
NEN-ISO/IEC-27001 NEN-ISO/IEC-27002	NEN	2005 2007	De code voor informatiebeveiliging
Informatiebeveiligingsbeleid Rijn Oost		2011	Beleidsdocument Rijn-Oost waterschappen en Lococensus-Tricijn
WBP		2000	Wet Bescherming Persoonsgegevens
Wet GBA		1994	Wet Gemeentelijke Basisadministratie Persoonsgegevens
NORA Dossier Informatiebeveiliging		2010	De Nederlandse Overheid Referentie Architectuur
WILMA	Het Waterschapshuis	2011	Waterschaps-Informatie en Logisch Model Architectuur
VIR		2007	Besluit Voorschrift Informatiebeveiliging Rijksdienst
VIR-BI		2012	Besluit Voorschrift Informatiebeveiliging Rijksdienst-Bijzondere Informatie

Documentbeheer Tactisch normenkader

Documenthistorie

Datum	Versie	Auteur	Opmerkingen
03-05-13	0.01		
06-05-13	0.02		
27-05-13	0.3		
10-06-13	0.4		
14-06-13	0.9		

Goedkeuring

Datum	Versie	Akkoord door	Opmerkingen
21-06-13	0.9	Werkgroep middelen	

Meer informatie

Het Waterschapshuis/UvW informatiebeveiliging@hetwaterschapshuis.nl

Het tactisch kader van de Baseline Informatiebeveiliging voor Waterschappen (BIWA) is geheel gestructureerd volgens NEN/ISO 27001, bijlage A en NEN/ISO 27002. Met klem wordt vermeld dat het tactisch kader BIWA deze normen niet vervangt. De overheid is conform de voorschriften van het college standaardisatie, verplicht om aan ISO 27001 en ISO 27002 te voldoen.
NEN/ISO 27001 en 27002 beschrijven details voor implementatie, zogenaamde implementatierichtlijnen, en eisen voor wat betreft de procesinrichting (o.a. het ISMS uit NEN/ISO 27001). Die documenten geven dus de details voor toepassing en moeten naast de BIWA aangeschaft en gebruikt worden.

Bronnen Tactisch normenkader

Titel	Auteur	Jaar	Omschrijving
13-0313 Baseline informatiebeveiliging Gemeenten (TNK) tactisch normenkader 0.99b	VNG/KING-IBD	2013	
Baseline Informatiebeveiliging Rijksdienst - Tactisch Normenkader (TNK)	MinBZK	2012	
NEN-ISO/IEC-27001 NEN-ISO/IEC-27002	NEN	2005 2007	De code voor informatiebeveiliging
Informatiebeveiligingsbeleid Rijn Oost	Rijn-Oost	2011	Beleidsdocument Rijn-Oost waterschappen en Lococensus-Tricijn
WBP		2000	Wet bescherming Persoonsgegevens
Wet GBA		1994	Wet Gemeentelijke Basisadministratie Persoonsgegevens
NORA Dossier Informatiebeveiliging		2010	De Nederlandse Overheid Referentie Architectuur
WILMA	Het Waterschapshuis	2011	Waterschaps-Informatie en Logisch Model Architectuur
VIR		2007	Besluit Voorschrift Informatiebeveiliging Rijksdienst
VIR-BI		2012	Besluit Voorschrift Informatiebeveiliging Rijksdienst-Bijzondere Informatie

Bijlage B Begrippen

Bijlage B Begrippen

Audit trail	Vastlegging van de complete keten van opeenvolgende wijzigingen op een object in een bepaalde periode.
A&K analyse	Een analyse methode om de afhankelijkheden en kwetsbaarheden in kaart te brengen.
Basis beveiligingsniveau	Het geheel van maatregelen van beveiliging dat wordt bereikt door het implementeren en toepassen van de normen zoals geformuleerd in de Code voor Informatiebeveiliging, Business Continuïty Management en WBP risicoklasse 2 en waaraan de NORA een nadere uitwerking geeft, onder meer door normen voor ICT-voorzieningen.
Bedrijfsmiddel	Elk middel waarin of waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten en ICT-voorzieningen kan worden verkregen: een bedrijfsproces, een gedefinieerde groep activiteiten, een gebouw, een apparaat, een ICT-voorziening of een gedefinieerde groep gegevens.
Beschikbaarheid	De waarborg dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
Beveiliging	Het brede begrip van informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, Business Continuïty Management (BCM), ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke veiligheid en integriteit.
Beveiligingsincident	Het manifest worden van een beveiligingsrisico (dreiging, oorzaak) als gevolg van een overtreding van beveiligingsregel, bijv. onbevoegde toegang tot ICT-voorzieningen.
Beveiligingsinstellingen	In ICT-voorzieningen kunnen in veel gevallen functionaliteiten die invloed hebben op beveiliging geactiveerd, gewijzigd of uitgeschakeld worden door het opgeven van parameterwaarden.

Clear Desk	Anders dan Clean Desk, waarbij het bureau helemaal leeg is, betekent Clear Desk dat er geen vertrouwelijke informatie op het bureau ligt.
Controleerbaarheid	De mate waarin de werkelijkheid of representaties daarvan toetsbaar zijn, dat wil zeggen te vergelijken met andere 'werkelijkheden of representaties daarvan' zodat objectieve oordeelsvorming mogelijk wordt.
Elektronische handtekening	Een elektronische handtekening is een methode voor het bevestigen van de juistheid van digitale informatie door middel van technieken van de asymmetrische cryptografie. De elektronische handtekening bestaat uit twee algoritmen: een om te bevestigen dat de informatie niet door derden veranderd is, de ander om de identiteit te bevestigen van degene die de informatie "ondertekent". De technieken worden toegepast met behulp van een PKI.
Filtering	Het gecontroleerd doorlaten van gegevens op het grensvlak tussen zones in een netwerk.
Firewall	Het geheel van software- en eventueel ook hardwarevoorzieningen dat voorkomt dat ongewenst verkeer van de ene netwerkzone terecht komt in de andere, teneinde de veiligheid in de laatstgenoemde te verhogen.
Hardening	Overbodige functies in besturingssystemen uitschakelen en/of van het systeem verwijderen en zodanige waarden toekennen aan beveiligingsinstellingen dat een maximale beveiliging ontstaat.
IB-functie	Een geheel van automatische informatiebeveiligingsverwerkingen die logisch met elkaar samenhangen.
ICT-voorzieningen	Applicaties en technische infrastructuur, of wel het geheel van ICT-voorzieningen.
In control statement	Binnen de gebruikelijke Planning en Control cyclus moet door het DB een in control statement worden afgegeven over het BIWA. De in control verklaring moet inzicht geven aan welke BIWA normen wordt voldaan en voor welke BIWA normen een uitzondering is gedefinieerd.

Informatiebeveiliging	Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
Integriteit	Het waarborgen van de juistheid en volledigheid en tijdigheid van informatie en de verwerking ervan. Als de tijdigheid van gegevens bepaald wordt door omstandigheden buiten het systeem, kan deze vanzelfsprekend niet als integriteitseis voor het systeem gesteld worden.
Logging	Vastlegging van systeemhandelingen.
Malware	Software met ongewenste functies, zoals virussen en trojans.
Media	Verzameling van middelen om informatie beschikbaar te stellen, zoals op het (beeld) scherm, spraak synthesizer, braille apparaat, en/of op te slaan, zoals papier, harddisk, of verwisselbare media (zie aldaar).
Mobile code	Code afkomstig van een ander systeem die lokaal uitgevoerd wordt, bijv. Javascript, Flash of Silverlight.
Onvertrouwd	Geen zekerheid over het beveiligingsniveau of zekerheid over het lager dan vereiste beveiligingsniveau
Onweerlegbaarheid	Het niet kunnen ontkennen iets te hebben gedaan (bijvoorbeeld een bericht te hebben ontvangen dan wel te hebben verstuurd).
Patch	Klein onderdeel van software dat de leverancier van software uitgeeft om fouten in door hem vervaardigde software te repareren
Query	Bevraging in een vraagtaal, die op basis van gebruikersvriendelijke en krachtige commando's selecties en berekeningen op bestanden kan uitvoeren, in eerste instantie alleen voor raadpleegdoeleinden.

Technische infrastructuur	Het geheel van ICT-voorzieningen voor generiek gebruik, zoals servers, firewalls, netwerkapparatuur, besturingssystemen voor netwerken en servers, database management systemen en beheer- en beveiligingstools, inclusief bijbehorende systeembestanden.
Two-factor authenticatie	Two-factor authenticatie vereist het gebruik van twee van de drie volgende authenticatiemethoden: • Iets dat de gebruiker weet (b.v. password, PIN); • Iets dat de gebruiker heeft (b.v. toegangspas, sleutel); en • Iets dat de gebruiker is (b.v. biometrische eigenschap zoals een vingerafdruk).
Vertrouwd	In overeenstemming met een door een bevoegde autoriteit vastgesteld beveiligingsniveau. Bijvoorbeeld vertrouwde zones of vertrouwde netwerken zoals in 10.6.1.2 en 10.6.1.3.
Vertrouwelijkheid	Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
Vertrouwelijke informatie	Informatie die niet algemeen bekend mag worden (bron: van Dale) In het kader van de BIWA worden maatregelen beschreven die voldoen voor de behandeling van gerubriceerde informatie tot en met vertrouwelijk en persoonsvertrouwelijke informatie van risicoklassen1 en 2 zoals gedefinieerd de toelichting op de WBP: A&V23[1]. Indien Risicoklasse 3 van toepassing is zullen aanvullende maatregelen genomen moeten worden.
Verwijderbare media	Opslagmiddelen die los van apparatuur kunnen worden verwijderd en meegenomen. Zoals CD-ROM, USB stick, verwijderbare schijven, tapes of gedrukte media.
Zone	De logische verzameling van ICT-voorzieningen met hetzelfde beveiligingsniveau, die via beveiligde koppelvlakken gegevens kunnen uitwisselen

Bijlage C Mapping BIWA

Bijlage C Mapping BIWA

In dit hoofdstuk is de mapping opgenomen naar basisregistraties GBA en BAG, WBP en NCSC richtlijnen voor ICS/SCADA systemen.

Sectie	SubSectie	Gebied	Omschrijving	GBA (+basisregistraties)	BAG	WBP	NCSC ICS/SCADA
5	1	1	Beleidsdocument voor informatiebeveiliging	X		X	X
5	1	2	Beoordeling van het informatiebeveiligingbeleid	X		X	X
6	1	1	Betrokkenheid van het College bij informatiebeveiliging	X		X	X
6	1	2	Coördinatie van informatiebeveiliging	X		X	X
6	1	3	Toewijzing van verantwoordelijkheden voor informatiebeveiliging	X		X	X
6	1	4	Goedkeuringsproces voor ICT-voorzieningen	X		X	X
6	1	5	Geheimhoudingsovereenkomst	X		X	X
6	1	6	Contact met overheidsinstanties				X
6	1	7	Contact met speciale belangengroepen				X
6	1	8	Onafhankelijke beoordeling van informatiebeveiliging	X		X	X
6	2	1	Identificatie van risico's die betrekking hebben op externe partijen	X		X	X
6	2	2	Beveiliging behandelen in de omgang met klanten				X
6	2	3	Beveiliging behandelen in overeenkomsten met een derde partij	X		X	X
7	1	1	Inventarisatie van bedrijfsmiddelen	X		X	X
7	1	2	Eigendom van bedrijfsmiddelen	X		X	X
7	1	3	Aanvaardbaar gebruik van bedrijfsmiddelen	X		X	X
7	2	1	Richtlijnen voor het classificeren			X	X
7	2	2	Labeling en verwerking van informatie			X	X
8	1	1	Rollen en verantwoordelijkheden	X		X	X
8	1	2	Screening	X		X	X
8	1	3	Arbeidsvoorwaarden	X		X	X

Sectie	SubSectie	Gebied	Omschrijving	GBA (+basisregistraties)	BAG	WBP	NCSC ICS/SCADA
8	2	1	Directieverantwoordelijkheid	X		X	X
8	2	2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	X		X	X
8	2	3	Disciplinaire maatregelen	X		X	X
8	3	1	Beëindiging van verantwoordelijkheden	X		X	X
8	3	2	Retournering van bedrijfsmiddelen	X		X	X
8	3	3	Blokkering van toegangsrechten	X		X	X
9	1	1	Fysieke beveiliging van de omgeving	X		X	X
9	1	2	Fysieke toegangsbeveiliging	X		X	X
9	1	3	Beveiliging van kantoren, ruimten en faciliteiten	X		X	X
9	1	4	Bescherming tegen bedreigingen van buitenaf	X		X	X
9	1	5	Werken in beveiligde ruimten	X		X	X
9	1	6	Openbare toegang en gebieden voor laden en lossen				X
9	2	1	Plaatsing en bescherming van apparatuur	X		X	X
9	2	2	Nutsvoorzieningen	X		X	X
9	2	3	Beveiliging van kabels				X
9	2	4	Onderhoud van apparatuur	X		X	X
9	2	5	Beveiliging van apparatuur buiten het terrein	X		X	X
9	2	6	Veilig verwijderen en hergebruiken van apparatuur	X		X	X
9	2	7	Verwijdering van bedrijfseigendommen	X		X	X
10	1	1	Gedocumenteerde bedieningsprocedures	X		X	X
10	1	2	Wijzigingsbeheer	X		X	X
10	1	3	Functiescheiding	X		X	X
10	1	4	Scheiding van faciliteiten voor ontwikkeling, testen en productie				X
10	2	1	Dienstverlening	X		X	X
10	2	2	Controle en beoordeling van dienstverlening door een derde partij	X		X	X
10	2	3	Beheer van wijzigingen in dienstverlening door een derde partij	X		X	X

Sectie	SubSectie	Gebied	Omschrijving	GBA (+basisregistraties)	BAG	WBP	NCSC ICS/SCADA
10	3	1	Capaciteitsbeheer	X		X	X
10	3	2	Systeemacceptatie	X		X	X
10	4	1	Maatregelen tegen virussen	X		X	X
10	4	2	Maatregelen tegen 'mobile code'	X		X	X
10	5	1	Reservekopieën maken (back-ups)	X		X	X
10	6	1	Maatregelen voor netwerken	X		X	X
10	6	2	Beveiliging van netwerkdiensten	X		X	X
10	7	1	Beheer van verwijderbare media	X		X	X
10	7	2	Verwijdering van media	X		X	X
10	7	3	Procedures voor de behandeling van informatie	X		X	X
10	7	4	Beveiliging van systeemdocumentatie	X		X	X
10	8	1	Beleid en procedures voor informatie-uitwisseling	X		X	X
10	8	2	Uitwisselingsovereenkomsten	X		X	X
10	8	3	Fysieke media die worden getransporteerd	X		X	X
10	8	4	Elektronische berichtuitwisseling	X		X	X
10	8	5	Systemen voor bedrijfsinformatie	X		X	X
10	9	1	E-commerce				X
10	9	2	Online transacties	X		X	X
10	9	3	Openbaar beschikbare informatie	X		X	X
10	10	1	Aanmaken auditlogbestanden	X		X	X
10	10	2	Controle van systeemgebruik	X		X	X
10	10	3	Bescherming van informatie in logbestanden	X		X	X
10	10	4	Logbestanden van administrators en operators	X		X	X
10	10	5	Registratie van storingen	X		X	X
10	10	6	Synchronisatie van systeemklokken				X
11	1	1	Toegangsbeleid	X		X	X
11	2	1	Registratie van gebruikers	X		X	X
11	2	2	Beheer van speciale bevoegdheden	X		X	X
11	2	3	Beheer van gebruikerswachtwoorden	X		X	X

Sectie	SubSectie	Gebied	Omschrijving	GBA (+basisregistraties)	BAG	WBP	NCSC ICS/SCADA
11	2	4	Beoordeling van toegangsrechten van gebruikers	X		X	X
11	3	1	Gebruik van wachtwoorden	X		X	X
11	3	2	Onbeheerde gebruikersapparatuur	X		X	X
11	3	3	'Clear desk'- en 'clear screen'-beleid	X		X	X
11	4	1	Beleid ten aanzien van het gebruik van netwerkdiensten	X		X	X
11	4	2	Authenticatie van gebruikers bij externe verbindingen.	X		X	X
11	4	3	Identificatie van (netwerk)apparatuur	X		X	X
11	4	4	Bescherming op afstand van poorten voor diagnose en configuratie	X		X	X
11	4	5	Scheiding van netwerken	X		X	X
11	4	6	Beheersmaatregelen voor netwerkverbindingen	X		X	X
11	4	7	Beheersmaatregelen voor netwerkroutering	X		X	X
11	5	1	Beveiligde inlogprocedures	X		X	X
11	5	2	Gebruikersidentificatie en -authenticatie	X		X	X
11	5	3	Systemen voor wachtwoordbeheer	X		X	X
11	5	4	Gebruik van systeemhulpmiddelen	X		X	X
11	5	5	Time-out van sessies	X		X	X
11	5	6	Beperking van verbindingstijd	X		X	X
11	6	1	Beperking van toegang tot informatie	X		X	X
11	6	2	Isolatie van gevoelige systemen	X		X	X
11	7	1	Draagbare comitputers en communicatievoorzieningen	X		X	X
11	7	2	Telewerken	X		X	X
12	1	1	Analyse en specificatie van beveiligingseisen	X		X	X
12	2	1	Validatie van invoergegevens	X		X	X
12	2	2	Beheersing van interne gegevensverwerking	X	X	X	X
12	2	3	Integriteit van berichten	X	X	X	X
12	2	4	Validatie van uitvoergegevens	X		X	X

Sectie	SubSectie	Gebied	Omschrijving	GBA (+basisregistraties)	BAG	WBP	NCSC ICS/SCADA
12	3	1	Beleid voor het gebruik van cryptografische beheersmaatregelen	X		X	X
12	3	2	Sleutelbeheer	X		X	X
12	4	1	Beheersing van operationele software	X		X	X
12	4	2	Bescherming van test data				X
12	4	3	Toegangsbeheersing voor broncode van programmatuur				X
12	5	1	Procedures voor wijzigingsbeheer			X	X
12	5	2	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem			X	X
12	5	3	Restricties op wijzigingen in programmatuurpakketten				X
12	5	4	Uitlekken van informatie	X		X	X
12	5	5	Uitbestede ontwikkeling van programmatuur				X
12	6	1	Beheersing van technische kwetsbaarheden	X		X	X
13	1	1	Rapportage van informatiebeveiligingsgebeurtenissen	X		X	X
13	1	2	Rapportage van zwakke plekken in de beveiliging	X		X	X
13	2	1	Verantwoordelijkheden en procedures	X		X	X
13	2	2	Leren van informatiebeveiligingsincidenten	X		X	X
13	2	3	Verzamelen van bewijsmateriaal	X		X	X
14	1	1	Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer	X	X	X	X
14	1	2	Bedrijfscontinuïteit en risicobeoordeling	X	X	X	X
14	1	3	Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging	X	X	X	X
14	1	4	Kader voor de bedrijfscontinuïteitsplanning	X	X	X	X
14	1	5	Testen, onderhoud en herbeoordelen van continuïteitsplannen	X	X	X	X
15	1	1	Identificatie van toepasselijke wetgeving	X		X	X

Sectie	SubSectie	Gebied	Omschrijving	GBA (+basisregistraties)	BAG	WBP	NCSC ICS/SCADA
15	1	2	Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)				X
15	1	3	Bescherming van bedrijfsdocumenten	X		X	X
15	1	4	Bescherming van gegevens en geheimhouding van persoonsgegevens	X		X	X
15	1	5	Voorkoming van misbruik van ICT-voorzieningen	X		X	X
15	1	6	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	X		X	X
15	2	1	Naleving van beveiligingsbeleid en -normen	X		X	X
15	2	2	Controle op technische naleving	X		X	X
15	3	1	Beheersmaatregelen voor audits van informatiesystemen	X		X	X
15	3	2	Bescherming van hulpmiddelen voor audits van informatiesystemen	X		X	X

Colofon

Uitgave
Unie van Waterschappen
Koningskade 40
2596 AA Den Haag
Postbus 93218
2509 AE Den Haag
www.uvw.nl

Oktober 2013

Deze publicatie wordt ook aangeboden via
www.uvw.nl

Drukwerkproductie
Opmeer drukkerij bv

Oplage
250 ex.