UBRivierenland

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 272

2 april 2021

Officiële uitgave van de gemeenschappelijke regeling Uitvoeringsorganisatie Breedbandnetwerk Rivierenland

Beleidsregel van het algemeen bestuur van het openbaar lichaam Uitvoeringsorganisatie Breedbandnetwerk Rivierenland houdende regels omtrent het informatiebeveiligingsbeleid

Deel 1: Beleidskaders informatiebeveiliging

1. Inleiding

Als UBRivierenland kunnen we niet om informatiebeveiliging heen. Informatiesystemen vormen immers het zenuwstelsel van onze organisatie en van de (keten)partners waarmee we zaken doen. Deze systemen kunnen alleen goed functioneren wanneer we de beveiliging ervan op orde hebben, dat wil zeggen: wanneer wij ervoor zorgen dat de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie gewaarborgd is en blijft.

2. Definities en belang van informatiebeveiliging

De kwaliteit van de informatievoorziening wordt voornamelijk gedefinieerd in termen van **beschikbaarheid, integriteit en vertrouwelijkheid**. Om de gegevens en informatiesystemen waarover we beschikken, op deze gebieden te kunnen beschermen is het noodzakelijk informatiebeveiligingsbeleid te hebben. We beschouwen informatiebeveiliging als het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen de organisatie.
Hierbij worden deze termen als volgt gedefinieerd:

- **Beschikbaarheid** betekent dat informatie(systemen) beschikbaar zijn op de juiste momenten. Zo kan UBRivierenland de continuïteit van de dienstverlening richting burgers en bedrijven te garanderen. En hebben burgers en bedrijven toegang tot de hen relevante informatie.
- **Integriteit** betekent het waarborgen van de correctheid en de volledigheid van de informatieverwerking. Voor een efficiënte en effectieve bedrijfsvoering is het voor UBRivierenland van belang dat de correcte informatie tijdig aanwezig is in de systemen. Maar ook dat zelfs na een bepaalde periode de correctheid en de volledigheid van informatie eenvoudig gecontroleerd kan worden (=controleerbaarheid).
- **Vertrouwelijkheid** betekent dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn. Voor UBRivierenland is het van belang dat vertrouwelijke informatie zoals de persoonsgegevens van burgers en gegevens van bedrijven niet toegankelijk is voor onbevoegden.

Dit informatiebeveiligingsbeleid richt zich niet alleen op de geautomatiseerde gegevensverwerking door middel van ICT-voorzieningen, maar uitdrukkelijk ook op de bescherming van niet geautomatiseerde gegevens (zoals fysieke documenten) en bedrijfseigendommen.

3. Doelstelling van informatiebeveiliging

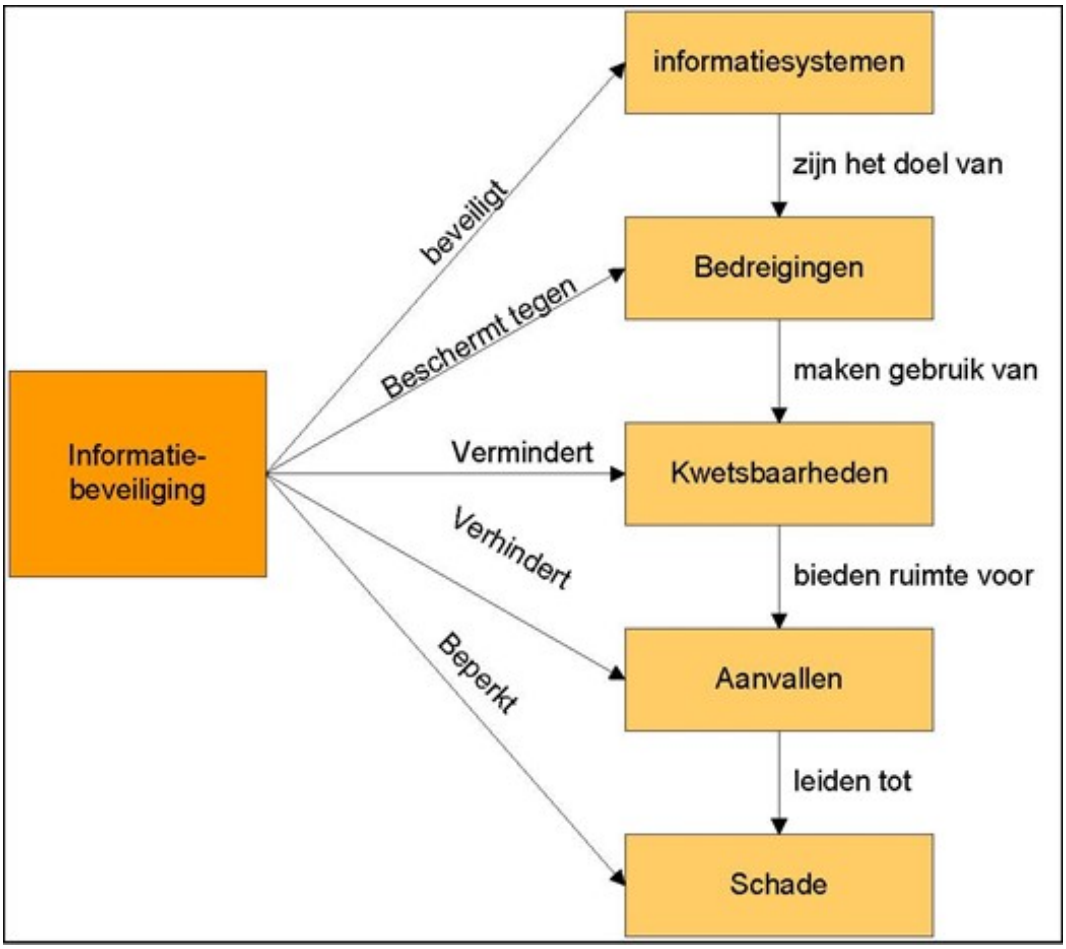
Dit document is de leidraad voor de aansturing en coördinatie van de verschillende beveiligingsprocessen binnen UBRivierenland. Het uiteindelijke doel is het inrichten van een set van beveiligingsmaatregelen, gericht op risicobeheersing. De risicobronnen waar de informatie en informatievoorziening van UBRivierenland aan zijn blootgesteld komen onder andere voort uit:

- de door de organisatie gewenste functionaliteit.
- de gebruikers van informatiesystemen.
- de kwetsbaarheden van de infrastructuur.
- externe oorzaken (bijvoorbeeld ongeoorloofd gebruik, vernieling inbraak).
- externe oorzaken (bijvoorbeeld technische calamiteiten zoals brand en lekkage).

Het doel van informatiebeveiliging binnen UBRivierenland is om te allen tijde een adequate set van maatregelen te hebben getroffen om de risico's die de hiervoor genoemde risicobronnen met zich meebrengen te beperken c.q. de gevolgschade te beperken. Niet alleen het treffen van fysieke, procedurele, organisatorische en technische maatregelen is van belang, ook de controle op naleving is essentieel. Hierbij wordt rekening gehouden met het volwassenheidsniveau van de organisatie en de beschikbare middelen.

Zonder goede informatie kunnen we niet werken, want de primaire en ondersteunende processen van UBRivierenland zijn in hoge mate afhankelijk van een adequate informatievoorziening en betrouwbare informatiesystemen. Zonder beveiligde informatie kan UBRivierenland bloot staan aan imagoschade. Met andere woorden informatie is voor ons een belangrijk bedrijfsmiddel dat op gepaste wijze beschermd moet worden.

Dit informatiebeveiligingsbeleid is er op gericht de beschikbaarheid, de integriteit en de vertrouwelijkheid van de (geautomatiseerde) gegevensverwerking binnen UBRivierenland en de (geautomatiseerde) uitwisseling van gegevens tussen UBRivierenland en derden te waarborgen. Om die beheersbare en betrouwbare informatievoorziening te realiseren is het van belang een aantal gemeenschappelijke uitgangspunten te hanteren en deze uit te dragen.



Het informatiebeveiligingsbeleid heeft als doel om de betrouwbare werking van de (geautomatiseerde) uitwisseling van informatie van UBRivierenland inzichtelijk te maken en daar waar nodig maatregelen aan te geven tegen een brede waaier van bedreigingen waaronder verstoringen en inbreuken en zo de continuïteit van UBRivierenland op dit gebied te verzekeren en maximaal bij te dragen tot goede resultaten.

Het informatiebeveiligingsbeleid moet steunen op een lagenmodel (zie volgend hoofdstuk) waar verschillende maatregelen complementair aan elkaar zijn. De veiligheid die bereikt kan worden met technische middelen is slechts één van de lagen. Deze middelen moeten aangevuld worden met een doeltreffend managementsysteem en met de noodzakelijk processen. Cruciaal voor een goede informatiebeveiliging is de deelname van alle medewerkers binnen UBRivierenland.

Informatieveiligheid wordt bereikt door de implementatie van een reeks beleidsmaatregelen of controles (hardware en software functies, processen, procedures, organisatie structuren). Deze moeten uitgewerkt worden om de veiligheidsdoelstellingen van UBRivierenland in te vullen.

4. Organisatie van informatiebeveiliging

- Binnen UBRivierenland is een beheerkader vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.
- Het informatiebeveiligingsbeleid is door het Dagelijks Bestuur vastgesteld en wordt door het Management Team (MT) van UBRivierenland uitgevoerd, waarbij beveiligingsrollen zijn toegewezen.

- De implementatie van de beveiligingsmaatregelen binnen UBRivierenland worden namens het MT door de Chief Information Security Officer (CISO) gecoördineerd en beoordeeld
- De implementatie van de beveiligingsmaatregelen binnen UBRivierenland worden namens het MT door de Chief Information Security Officer (CISO) gecoördineerd en beoordeeld.
- Omdat de IT-voorzieningen continu onderhevig zijn aan veranderingen, is Informatiebeveiliging binnen UBRivierenland een continu (verbeter)proces.
- Het informatiebeveiligingsproces doorloopt de zogenaamde Deming Cyclus die de fases Plan, Do, Check en Act bevat.
- De correcte uitvoering van informatiebeveiliging wordt minimaal jaarlijks door een externe partij beoordeeld.

Ten aanzien van risico's die voort komen uit de risicoanalyse heeft UBRivierenland per risico één van de volgende strategieën gekozen om deze te verkleinen:
- Treat the risk (reduceren): verkleinen van het risico door middel van het nemen van informatiebeveiligingsmaatregelen.
- Take the risk (accepteren): het risico is zo klein dat de gevolgen acceptabel zijn.
- Terminate the risk (vermijden): wanneer er een groot risico bestaat voor een bedrijfsactiviteit die weinig tot geen toegevoegde waarde heeft dan wordt deze bedrijfsactiviteit indien mogelijk gestaakt.
- Transfer the risk (delen/overdragen): overhevelen van het risico naar een derde partij door middel van uitbesteding of het afsluiten van verzekeringen.

Het informatiebeveiligingsbeleid is opgebouwd in drie niveaus.

Op het hoogste niveau wordt het informatiebeveiligingsbeleid gedefinieerd. De uitgangspunten in dit beleid worden beïnvloed door algemeen geldende standaarden en normen alsmede de wettelijke bepalingen waaraan UBRivierenland onderhevig is. Daarnaast wordt het beleid ingevuld op basis van randvoorwaarden zoals het algemene bedrijfsbeleid en mogelijke geldende externe normen. Het gaat hier om algemeen geldende richtlijnen, niet om op specifieke informatiesystemen gerichte maatregelen.

Op het tweede niveau worden de beveiligingsmaatregelen beschreven als uitwerking van de doelstellingen in het informatiebeveiligingsbeleid. Het gaat hierbij om zowel organisatorische als om technische beveiligingsmaatregelen. Deze kunnen gedefinieerd zijn voor de informatiebeveiliging in het algemeen of voor specifieke informatiesystemen.

Op het laagste niveau zijn de procedures en werkinstructies gedefinieerd die bestaan uit dagelijkse beheersactiviteiten met betrekking tot de informatiebeveiliging.

Het is van essentieel belang te realiseren dat het informatiebeveiligingsbeleid in algemene termen uitspraken doet over beveiligingsaspecten. Het geeft via richtlijnen dwingend richting aan de implementatie van een adequaat beveiligingsniveau voor alle (geautomatiseerde) informatie. Maatregelen op systeemniveau komen in het beleid niet aan de orde.

Subjecten van het informatiebeveiligingsbeleid
Alle personeelsleden in dienst van UBRivierenland en alle externe inhuurkrachten dienen overeenkomstig het beveiligingsbeleid te handelen en zijn dus verantwoordelijk voor het toepassen van het beveiligingsbeleid binnen hun verantwoordelijkheidsgebied.

Objecten van het informatiebeveiligingsbeleid
Het beveiligingsbeleid geldt voor alle informatie, hetzij mondeling, hetzij geschreven, geprint of elektronisch opgeslagen, die eigendom is van, in bewaring is bij of gebruikt wordt van UBRivierenland. Het beveiligingsbeleid geldt ook voor alle dragers gebruikt in het creëren, verwerken, versturen sorteren, gebruiken of controleren van gegevens en informatie.

5. Taken, bevoegdheden en verantwoordelijkheden
Binnen UBRivierenland worden de volgende functies ten aanzien van informatiebeveiliging onderscheiden:

Het Dagelijks Bestuur van UBRivierenland is eindverantwoordelijk voor alle informatiebeveiligingsaangelegenheden. Het **Managementteam (MT)** ondersteunt informatiebeveiliging door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.

De **Chief Information Security Officer (CISO)** gecoördineerd en beoordeeld namens het MT de implementatie van de beveiligingsmaatregelen binnen UBRivierenland.

De **Coördinatoren** van elk team van UBRivierenland zijn verantwoordelijk voor de beveiliging en voor de kwaliteit van de informatie en informatiesystemen voor eigen gebruik en de aan anderen (intern en extern) geleverde informatie en informatiediensten.

Daarnaast hebben (eigen en ingehuurde) **medewerkers**, oftewel gebruikers van informatie en informatiesystemen van UBRivierenland een eigen verantwoordelijkheid. Men is verplicht, zich te houden aan de verstrekte richtlijnen aangaande de omgang met informatie, informatieverwerking en desbetreffende bedrijfsmiddelen. Niet naleving kan (disciplinaire) consequenties hebben.

6. Doelgroepen

Informatiebeveiliging en daarmee ook dit informatiebeveiligingsbeleid geldt voor alle medewerkers en externe inhuur van UBRivierenland. Kortom allen die te maken hebben met het verwerken van informatie. Het informatiebeveiligingsbeleid heeft als functie richting te geven aan informatiebeveiliging. Daarom worden in dit beleid de grondhouding en de basisprincipes van UBRivierenland ten aanzien van informatiebeveiliging beschreven.

Dit document is tevens gericht op alle overige belanghebbenden van UBRivierenland, zoals burgers, bedrijven en leveranciers van goederen en diensten om op die manier duidelijk te maken wat de basisprincipes en eisen zijn ten aanzien van informatiebeveiliging.

Indien bij samenwerking met derden sprake is van uitwisseling van informatie, waarvan UBRivierenland eigenaar of beheerder is, dient informatiebeveiliging een onderdeel te zijn de samenwerkingsovereenkomst en mag deze niet strijdig zijn met het informatiebeveiligingsbeleid van UBRivierenland.

Het informatiebeveiligingsbeleid is locatie onafhankelijk. Indien een medewerker, zakelijke relatie of leverancier of derde zich op een locatie bevindt buiten de kantooromgeving van UBRivierenland, maar wel met informatie of informatievoorziening (denk aan onderhoud in het veld, thuiswerken en/of webmail) van UBRivierenland werkt, dient men zich ook aan dit beleid te houden.

7. Van toepassing zijnde wet-en regelgeving

Behalve de interne eisen die UBRivierenland aan informatiebeveiliging stelt, zijn er wettelijke eisen gesteld aan de beveiliging van gegevens en informatiesystemen. Voorbeelden hiervan zijn te vinden in:

- Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.
- UBRivierenland dient volgens deze wet ervoor zorg te dragen dat persoonsgegevens van burgers, bedrijven, medewerkers, leveranciers en overige belanghebbenden worden beschermd tegen onrechtmatige verwerking van of onbevoegde toegang tot deze gegevens.
- De Wet Computercriminaliteit II. Deze wet gaan in op computer gerelateerde strafbare handelingen. UBRivierenland dient door middel van adequate informatiebeveiligingsmaatregelen ervoor te zorgen dat deze wet door medewerkers van UBRivierenland of door derden waarvoor UBRivierenland verantwoordelijk is niet wordt overtreden.
- Daarnaast zijn er voor gemeentelijke taken specifieke vereisten van de Wet GBA, de wet BAG, de richtlijnen voor SUWInet, etc.
- Maar ook het Burgerlijk Wetboek, de Telecommunicatiewet, de Auteurswet, de Wet op de Jaarrekening, de Archiefwet en het Wetboek van Strafvordering, etc.... bevatten in het algemeen een resultaatverplichting tot een passend niveau van informatiebeveiliging.

8. Gebruikte normen en standaarden

Binnen UBRivierenland wordt de Code voor Informatiebeveiliging (NEN- ISO/IEC 27002:2013) als norm gehanteerd voor het implementeren van informatiebeveiliging.

9. Relaties met overige documentatie

Het informatiebeveiligingsbeleid wordt door middel van een informatiebeveiligingsplan geoperationaliseerd. Dit betekent dat de concrete uitvoering van dit beleid door middel van het implementeren van informatiebeveiligingsmaatregelen is beschreven in het informatiebeveiligingsplan. In het informatiebeveiligingsplan wordt beschreven welke maatregelen ingevoerd moeten worden, op welke manier, door wie en binnen welk tijdsbestek. Indien van toepassing worden activiteiten uit het informatiebeveiligingsplan verder uitgewerkt in afzonderlijke projectplannen.

10. Benodigde middelen

UBRivierenland stelt ieder jaar een begroting op, waarin de benodigde middelen voor informatiebeveiliging beschikbaar worden gesteld. Het budget wordt beschikbaar gesteld aan de hand van de in het informatiebeveiligingsplan gedefinieerde activiteiten.

Deel 2: doelstellingen en beleidsuitgangspunten voor informatiebeveiliging

In deel 2 wordt per beveiligingscategorie uit de Code voor Informatiebeveiliging uiteengezet wat voor UBRivierenland de doelstelling en de uitgangspunten zijn voor de te treffen maatregelen.

1. Beveiligingsbeleid

Informatiebeveiligingsbeleid

Doelstelling:
Het borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de wetgeving en er voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden.

Beleidsdocumenten voor informatiebeveiliging:
Het MT van UBRivierenland geeft richting aan en biedt ondersteuning voor informatiebeveiliging in overeenstemming met de bedrijfsmatige eisen en relevante wetten en voorschriften.

Het informatiebeveiligingsbeleid is door het hoogste management goedgekeurd, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten. Het informatieveiligheidsbeleid is bekend bij alle medewerkers en relevante externe partijen.

Beoordeling van het informatiebeveiligingsbeleid:
- Het informatiebeveiligingsbeleid wordt periodiek (2 x per jaar) of zodra zich belangrijke wijzigingen voordoen geactualiseerd.
- Er worden periodiek (minimaal 1 keer per jaar) beveiligingsaudits uitgevoerd.
- Er wordt jaarlijks gerapporteerd over het functioneren van informatiebeveiliging aan het Dagelijks Bestuur.

2. Organisatie van informatiebeveiliging

Interne organisatie

Doelstelling:
De continuïteit van informatiebeveiliging in UBRivierenland is geborgd in de organisatie en in de processen.

Uitgangspunten:
- Het Dagelijks Bestuur van UBRivierenland stelt een beheerkader vast om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.
- Het Dagelijks Bestuur van UBRivierenland stelt het informatiebeveiligingsbeleid vast.
- De uitvoering van het informatieveiligheidsbeleid is bij het MT belegd.
- De CISO coördineert en beoordeelt namens het MT de implementatie van de beveiliging binnen de organisatie.

Externe partijen

Doelstelling:
De conformiteit van het regionaal informatiebeveiligingsbeleid met externe partijen is geborgd middels leveranciersmanagement en de daarbij behorende contracten, SLA's en eventuele verwerkersovereenkomsten.

Uitgangspunten:

- Informatiebeveiliging is aantoonbaar meegewogen bij het besluit een externe partij wel of niet in te schakelen.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe partij moet hebben om de in het

contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthentiseerde en geautoriseerde toegang vastgesteld wordt.
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een verwerkersovereenkomst afgesloten.
- 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

3. Beheer van bedrijfsmiddelen

Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling:
De bedrijfsmiddelen van UBRivierenland zijn adequaat beschermd.

Uitgangspunten:
- Alle bedrijfsmiddelen [1] zijn verantwoord en aan een 'eigenaar' toegewezen.
- Voor alle bedrijfsmiddelen is vastgelegd wie verantwoordelijk is voor het handhaven van geschikte beheersmaatregelen. Deze verantwoordelijkheid kan zijn gemandateerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.
- Er zijn regels voor acceptabel gebruik van bedrijfsmiddelen (met name internet, e-mail en mobiele apparatuur).
- Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.
- Informatiedragers worden dusdanig gebruikt dat vertrouwelijke informatie niet beschikbaar kan komen voor onbevoegde personen.

4 Classificatie van informatie

Doelstelling:
Alle informatie heeft een passend beschermingsniveau.

Uitgangspunten:
- Informatie binnen UBRivierenland is geclassificeerd om bij het verwerken van deze informatie de noodzaak, prioriteiten en graad van beveiliging aan te geven.
- Informatie is geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.
- Er zijn samenhangende procedures voor de labeling en de verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.
- UBRivierenland beschikt over een informatie classificatieschema dat wordt gebruikt om adequate niveaus van bescherming te definiëren en de noodzaak voor verwerkingsmaatregelen te communiceren.
- De proceseigenaar heeft maatregelen getroffen om te voorkomen dat niet- geautoriseerde toegang tot informatie krijgen.
- Papieren documenten en mobiele gegevensdragers die vertrouwelijke informatie bevatten worden beveiligd opgeslagen, tenzij de vertrouwelijke informatie op de mobiele gegevensdrager voldoende versleuteld is.

5. Beveiliging van personeel

Voorafgaand aan het dienstverband

Doelstelling:

1) Onder bedrijfsmiddelen worden o.a. verstaan, apparatuur zoals: PC's, laptops, tablets, smartphones, en servers, maar ook applicaties Key2Finance, Afas, Corsa, Tim, etc.

Werknemers, in te huren personeel en gebruikers van externe partijen kennen en begrijpen hun verantwoordelijkheden waardoor het risico op diefstal, fraude of misbruik van faciliteiten vermindert.

Uitgangspunten:
- De verantwoordelijkheid voor (informatie)beveiliging is voorafgaand aan het dienstverband vastgelegd in de integriteitsclausule en opgenomen in ambtseed.
- Kandidaten, in te huren personeel en gebruikers van externe partijen worden op, door P&O bepaalde, passende wijze gescreend.
- Alle werknemers, in te huren personeel en gebruikers van externe partijen die IT-voorzieningen gebruiken worden geïnformeerd over het algemeen geldend beveiligingsbeleid en over hun beveiligingsrollen en verantwoordelijkheden.

Tijdens het dienstverband

Doelstelling:
Alle werknemers, in te huren personeel en gebruikers van externe partijen zijn zich bewust van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheden en zijn toegerust om het beveiligingsbeleid van UBRivierenland in hun dagelijkse werkzaamheden uit te voeren en het risico van een menselijke fout te verminderen.

Uitgangspunten:
- Alle werknemers, al het ingehuurde personeel en alle externe medewerkers beschikken over een passend niveau van bewustwording, opleiding en training in beveiligingsprocedures en het juiste gebruik van IT- voorzieningen om mogelijke beveiligingsrisico's te minimaliseren.
- UBRivierenland kent een gestructureerd proces voor het omgaan met beveiligingsinbreuken.

Beëindiging of wijziging van dienstverband

Doelstelling:
Zorgen dat werknemers, in te huren personeel en gebruikers van externe partijen UBRivierenland volgens de richtlijnen verlaten of hun dienstverband wijzigen.

Uitgangspunten:
- UBRivierenland kent een proces om te waarborgen dat alle apparatuur wordt teruggegeven en dat alle toegangsrechten worden ingetrokken wanneer een werknemer, ingehuurde medewerker of externe gebruiker de organisatie verlaat.
- Bij verandering van rol of functie binnen UBRivierenland wordt specifiek gekeken naar de consequenties hiervan voor autorisaties en verantwoordelijkheden in het kader van informatieveiligheid.

6 Fysieke beveiliging en beveiliging van de omgeving

Beveiligde ruimten

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

Fysieke beveiliging van het gebouw

Er zijn toegangsbeveiligingen aangebracht om ruimten te beschermen waar zich informatie en ICT-voorzieningen bevinden.

- Het bedrijfsgebouw van UBRivierenland en haar omgeving worden ingedeeld in verschillende zones.

  Deze zones bestaan uit:
  - Zone 0: de omgeving en het gebouw
  - Zone 1: de wachtruimten en de spreekkamers
  - Zone 2: de werkruimten
  - Zone 3: de ICT-ruimte/archief

- Voor iedere zone zijn duidelijke beveiligingsgrenzen bepaald.
- Toegang tot het gebouw en zones binnen het gebouw zijn met tags geregeld.

- Er is dagelijks bewaking die het gebouw controleert en afsluit. Er is een inbraakalarm gekoppeld aan de alarmcentrale.
- De ingehuurde bewakingsdienst is vooraf geverifieerd op de wettelijke eisen gesteld in de Wet Particuliere Beveiligingsorganisaties en Recherchebureaus. Deze verificatie wordt jaarlijks herhaald.

Fysieke toegangsbeveiliging

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

- Toegang tot gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
- Beveiligde zones zijn toegankelijk met een tag voor geautoriseerd personeel. Hiervan wordt een automatische registratie bijhouden in de logfile.
- Voor toegang tot speciale ruimten is een doelbinding vereist, dat wil zeggen dat personen op grond van hun werkzaamheden toegang kan worden verleend.

Beveiliging van kantoren, ruimten en faciliteiten

- De serverruimtes en het archief zijn alleen toegankelijk met een tag voor geautoriseerd personeel. Hiervan wordt een automatische registratie bijgehouden in de logfile.
- Apparatuur en bekabeling in kabelverdeelruimtes en patchruimtes voldoen aan dezelfde eisen t.a.v. toegangsbeveiliging zoals die worden gesteld aan computerruimtes.
- Serverruimtes, datacenters en daar aan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende best practices.
- De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering.
- De uitgifte van toegangsmiddelen wordt geregistreerd.
- Niet uitgegeven toegangsmiddelen worden opgeborgen in een beveiligd opbergmiddel.
- 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.
- Er vindt één keer per half jaar een periodieke controle/evaluatie plaats op de autorisaties voor fysieke toegang.

Bescherming tegen bedreigingen van buitenaf

- 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.
- Beveiligde ruimten waarin zich bedrijfskritische apparatuur bevindt zijn voldoende beveiligd tegen wateroverlast.
- 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.
- Er is door de brandweer goedgekeurde en voor de situatie geschikte brandblusapparatuur geplaatst en aangesloten. Dit wordt jaarlijks gecontroleerd.

Werken in beveiligde ruimten

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

- 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
- Beveiligde ruimten (zoals een serverruimte of kluis) waarin zich geen personen bevinden zijn afgesloten en worden regelmatig gecontroleerd.

Beveiliging van apparatuur

Doelstelling:
Het voorkomen van onderbrekingen van de bedrijfsactiviteiten en het voorkomen van schade aan, of verlies of diefstal van apparatuur.

Uitgangspunten:

- Alle apparatuur van UBRivierenland is beschermd tegen fysieke bedreigingen en gevaren van buitenaf, zodat het risico van toegang door onbevoegden tot informatie wordt verminderd en de apparatuur wordt beschermd tegen verlies of schade en de gevolgen van diefstal.
- Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.
- Apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om er voor te zorgen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven, voordat de apparatuur wordt verwijderd.
- Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.

7. Beheer van communicatie-en bedieningsprocessen

Bedieningsprocedures en verantwoordelijkheden

Doelstelling:
Het waarborgen van een correcte en veilige bediening van IT-voorzieningen.

Uitgangspunten:
- UBRivierenland heeft verantwoordelijkheden en procedures vastgesteld voor beheer en bediening van alle IT-voorzieningen. Hieronder vallen ook bedieningsinstructies en handleidingen.
- Waar van toepassing wordt functiescheiding toegepast om het risico van nalatigheid of opzettelijk misbruik van informatiesystemen te verminderen.

Beheer van de dienstverlening door een derde partij

Doelstelling:
Het implementeren en bijhouden van een passend niveau van informatiebeveiliging bij dienstverlening door een derde partij.

Uitgangspunten:
- UBRivierenland controleert de implementatie van overeenkomsten met derden, bewaakt naleving van de overeenkomsten en beheert wijzigingen om te waarborgen dat de geleverde diensten aan alle eisen betreffende informatiebeveiliging voldoen die met de derde partij zijn overeengekomen.

Beheer van wijzigingen

Doelstelling:
Het risico van systeem verstoringen tot een minimum beperken.

Uitgangspunten:
- UBRivierenland treft bij wijzigingen de nodige voorbereidingen om voldoende menscapaciteit en beschikbaarheid van IT-middelen te waarborgen.
- UBRivierenland heeft de operationele eisen aan nieuwe systemen vastgesteld gedocumenteerd en getest voordat deze systemen worden geaccepteerd en in gebruik worden genomen

Bescherming tegen virussen en kwaadaardige programmatuur

Doelstelling:
Beschermen van de integriteit van programmatuur en informatie.

Uitgangspunten:
- UBRivierenland heeft maatregelen getroffen voor de detectie en preventie en terminatie van de verspreiding van virussen en andere kwaadaardige programmatuur.

Back-up en recovery

Doelstelling:
Handhaven van de integriteit en beschikbaarheid van informatie en IT- voorzieningen.

Uitgangspunten:
- UBRivierenland heeft routineprocedures vastgesteld voor het uitvoeren van de overeengekomen back-up en recovery strategie.

Beheer van netwerkbeveiliging

Doelstelling:
Zorg dragen voor de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur.

Uitgangspunten:
- UBRivierenland heeft maatregelen getroffen voor de beveiliging van het interne netwerk.

Behandeling van media

Doelstelling:
Voorkomen van onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten.

Uitgangspunten:
- UBRivierenland heeft passende maatregelen getroffen om documenten, opslagmedia (bijvoorbeeld schijven, tapes, USB-sticks), en systeemdocumentatie te beschermen tegen onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging.

Uitwisseling van informatie

Doelstelling:
Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld met derden.

Uitgangspunten:
- UBRivierenland heeft procedures vastgesteld ter bescherming van informatie en fysieke media die informatie bevatten die wordt getransporteerd.

Diensten voor online transacties

Doelstelling:
Zorgen voor de beveiliging van diensten voor online transacties en veilig gebruik ervan.

Uitgangspunten:
- UBRivierenland zorgt voor passende beveiligingsmaatregelen die gepaard gaan met diensten voor online transacties.
- UBRivierenland zorgt voor passende beveiligingsmaatregelen die betrekking hebben op de integriteit en beschikbaarheid van online transacties.

Controle

Doelstelling:
Ontdekken van onbevoegde informatieverwerkingsactiviteiten.

Uitgangspunten:
- UBRivierenland controleert haar systemen en registreert informatiebeveiligingsgebeurtenissen. Hiertoe wordt gebruik gemaakt van logbestanden en storingsregistraties.
- UBRivierenland voldoet aan alle relevante wettelijke eisen die van toepassing zijn op haar controle en registratie-activiteiten.

8. Toegangsbeveiliging

Beheer van toegangsrechten van gebruikers

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

Uitgangspunten:
- Toegang tot informatie, IT-voorzieningen en bedrijfsprocessen wordt bij UBRivierenland beheerst op grond van autorisatiematrix.
- UBRivierenland heeft procedures vastgesteld voor de beheersing van toewijzing van toegangsrechten tot informatiesystemen en –diensten

- UBRivierenland heeft speciale aandacht besteed aan het toewijzen van speciale toegangsrechten waarmee gebruikers de normale beveiliging van het systeem kunnen passeren.

Verantwoordelijkheden van gebruikers

Doelstelling:
Voorkomen van onbevoegde toegang door gebruikers en beschadiging of diefstal van informatie en IT-voorzieningen.

Uitgangspunten:
- UBRivierenland informeert haar medewerkers over hun verantwoordelijkheid voor toegangsbeveiliging, vooral met betrekking tot het gebruik van wachtwoorden.
- UBRivierenland kent een 'clear-desk' en 'clear-screen'-beleid om het risico van ongeoorloofde toegang of schade aan papieren, media en IT-voorzieningen te verminderen.

Mobiele apparaten en telewerken

Doelstelling:
Het zorgen voor een passende mate van informatiebeveiliging bij het gebruik van mobiele apparaten en faciliteiten voor telewerken.

Uitgangspunten:
- De vereiste bescherming bij UBRivierenland is in overeenstemming met de risico's die verbonden zijn aan deze manier van werken.

9. Inkoop, onderhoud en ontwikkeling van informatiesystemen

Beveiligingseisen aan informatiesystemen

Doelstelling:
Zorgen dat informatiebeveiliging integraal deel uitmaakt van nieuw te ontwikkelen informatiesystemen.

Uitgangspunten:
- UBRivierenland heeft maatregelen getroffen die waarborgen dat beveiligingseisen voorafgaand aan de ontwikkeling en/of implementatie van informatiesystemen worden vastgesteld en overeengekomen.
- Tijdens de specificatie van eisen voor een project worden de van toepassing zijnde beveiligingseisen overeengekomen en gedocumenteerd als onderdeel van de randvoorwaarden rondom het nieuwe informatiesysteem.

Correcte verwerking in programmatuur

Doelstelling:
Voorkomen van fouten, verlies, onbevoegde wijziging of misbruik van informatie in programmatuur.

Uitgangspunten:
- In programmatuur zijn geschikte beheermaatregelen ingebouwd, waaronder validatie van invoergegevens, interne verwerking en uitvoergegevens.
- Indien nodig zijn, bij systemen waarop gevoelige, waardevolle of kritische informatie wordt verwerkt, aanvullende beheersmaatregelen getroffen op basis van de beveiligingseisen en een risicobeoordeling.

Cryptografische beheersmaatregelen

Doelstelling:
Beschermen van de vertrouwelijkheid, authenticiteit en integriteit van informatie met behulp van cryptografische middelen.

Uitgangspunten:
- Wanneer de vertrouwelijkheid van de gegevens binnen een (te ontwikkelen) informatiesysteem dit vereist, wordt er gebruik gemaakt van cryptografische toepassingen om de gegevens te beschermen tegen onbevoegde wijziging of inzage.

Beveiliging van systeembestanden

Doelstelling:
Zorgen voor de beveiliging van systeembestanden.

Uitgangspunten:
- De broncode en systeembestanden van applicaties van UBRivierenland zijn beschermd tegen inzage door onbevoegden, beschadiging en diefstal.

Beheer van technische kwetsbaarheden

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

Uitgangspunten:
- UBRivierenland heeft het beheer van technische kwetsbaarheden op een doeltreffende, systematische en herhaalbare wijze geïmplementeerd (software patchen).

Uitlekken van informatie

Doelstelling:
Voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken.

Uitgangspunten:
- UBRivierenland probeert lekken van informatie te voorkomen door onbevoegde netwerktoegang te voorkomen,
- UBRivierenland combineert dit met beleid en procedures om het bewustzijn te stimuleren en tegelijkertijd misbruik van informatiediensten door personeel te ontmoedigen.

10. Beheersen van informatiebeveiligingsincidenten

Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

Doelstelling:
Zorgen dat informatiebeveiligingsgebeurtenissen en zwakheden geregistreerd worden en dat tijdig corrigerende maatregelen worden getroffen.

Uitgangspunten:
- UBRivierenland heeft een procedure opgesteld voor rapportage van gebeurtenissen en escalatie.
- Alle medewerkers, in te huren personeel en gebruikers van externe partijen zijn van deze procedure op de hoogte en zijn zich bewust van hun verplichting alle beveiligingsgebeurtenissen en zwakke plekken zo snel mogelijk te rapporteren aan de aangewezen contactpersoon.

Beheer van informatiebeveiligingsincidenten en -verbeteringen

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

Uitgangspunten:
- UBRivierenland heeft een procedure opgesteld voor het doeltreffend behandelen van informatiebeveiligingsgebeurtenissen en zwakke plekken, zodra ze zijn gerapporteerd.
- UBRivierenland heeft een proces van continue verbetering ingericht voor het reageren op, controleren, beoordelen en beheer van informatiebeveiligingsincidenten.

11. Continuïteitsbeheer

Informatiebeveiligingsaspecten van continuïteitsbeheer

Doelstelling:
Onderbrekingen van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen tegen de gevolgen van calamiteiten[2] en om voor tijdig herstel te zorgen.

2) Onder calamiteit wordt verstaan een omvangrijke storing in informatiesystemen of rampen.

Uitgangspunten:
- De definitie van een calamiteit is duidelijk binnen de gehele organisatie.
- Calamiteiten welke de gegevenswerking kunnen bedreigen zijn geïdentificeerd.
- UBRivierenland beschikt over een continuïteitsplan waarin is beschreven welke stappen genomen dienen te worden om de continuïteit van de gegevensverwerking te waarborgen in geval van een calamiteit.
- Het calamiteitenplan wordt periodiek getest.
- De meest bedrijfskritische informatiesystemen die de primaire bedrijfsprocessen ondersteunen kennen een uitwijkplan en zijn opgenomen in genoemd continuïteitsplan.

12. Naleving

Naleving van beveiligingsbeleid en –normen en technische naleving

Doelstelling:
Zorgen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.
Uitgangspunten:
- Informatiesystemen worden regelmatig beoordeeld op naleving van beveiligingsnormen en standaarden.
- Dergelijke beoordelingen worden uitgevoerd op basis van het beveiligingsbeleid
- Technische platforms en informatiesystemen worden beoordeeld op naleving van toepasselijke normen voor de implementatie van de beveiliging en gedocumenteerde beveiligingsmaatregelen.

Zorgvuldigheid bij audits van informatiesystemen

Doelstelling:
Zorgvuldigheid bewaken bij audits van informatiesystemen en minimaliseren van eventuele verstoringen als gevolg van audits.

Uitgangspunten:
UBRivierenland heeft beheersmaatregelen getroffen om productiesystemen te beveiligen tijdens de uitvoering van audits.

Bescherming van (vertrouwelijke) bedrijfsinformatie en bedrijfsdocumenten

Doelstelling:
Belangrijke informatie en/of registraties behoren te worden beschermd tegen verlies, vernietiging, ontvreemding en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen, projectmatige en bedrijfsmatige eisen (lees: auditability).

Uitgangspunten:
UBRivierenland heeft een (privacy) beleid voor bescherming van vertrouwelijke gegevens ontwikkeld en ingevoerd. Dit beleid is gecommuniceerd naar alle personen die betrokken zijn bij het werken met vertrouwelijke gegevens. Naleving van dit beleid en alle relevante wetgeving voor gegevensbescherming en regelgeving vereist een passende structuur voor beheer en beveiliging. Er is een functionaris aangewezen die belast is met de bescherming van gegevens. Deze functionaris biedt ondersteuning aan managers, gebruikers en dienstverlenende bedrijven met betrekking tot hun individuele verantwoordelijkheden en de specifieke procedures die behoren te worden gevolgd. Het toewijzen van verantwoordelijkheid voor het verwerken van vertrouwelijke informatie en het waarborgen dat medewerkers zich bewust zijn van de uitgangpunten van bescherming van gegevens is uitgevoerd in overeenstemming met de relevante wet-en regelgeving. Er zijn passende technische en organisatorische maatregelen geïmplementeerd om dergelijke vertrouwelijke gegevens te beschermen (lees: bescherming van forensisch bewijs).