provincie limburg

Beleid Informatiebeveiliging Provincie Limburg

1. Inleiding

1.1. Strategisch informatiebeleid Provincie Limburg

Om de ambities ten aanzien van onze Limburgse opgaves waar te maken is het essentieel om de juiste informatie en data te gebruiken én te delen met partners in de regio. Dit brengt echter risico's met zich mee.

De afgelopen jaren zijn diverse organisaties in het nieuws geweest in verband met incidenten op het gebied van informatieveiligheid. De bedrijfsprocessen van de Provincie Limburg worden gevoed met talloze gegevens, informatie en kennis met als resultaat (beleids-) informatie, besluitvorming en uitvoering. Verstoringen van deze processen als gevolg van niet-beschikbaarheid, onjuiste informatie of gelekte informatie kunnen vergaande gevolgen hebben voor het democratisch proces.

We hebben als organisatie het doel om informatie als een betrouwbare productiefactor te gebruiken. Dit is een verantwoordelijkheid van de hele organisatie, waarbij het cluster Organisatie en Informatie de kaders schept en ondersteunt middels de rol van Concern Information Security Officer (CISO). Om ons doel te bereiken is het cruciaal dat we onze beveiliging op het gewenste niveau houden. Voor dit gewenste niveau hanteren we een internationale normering (ISO27001) en de Baseline Informatieveiligheid Overheid (BIO) als uitgangspunt. Op basis hiervan komen we tot een set van maatregelen waarmee informatiebeveiligingsrisico's tot een acceptabel niveau worden beperkt.

- *We implementeren en volgen standaarden en best practices.*
- *We zijn eind 2022 gereed voor certificering voor de ISO 27001-norm.*
- *We versterken actief het interne bewustzijn van medewerkers.*
- *We bouwen samen met ketenpartners aan kennis.*
- *We bouwen de monitoring en rapportagestructuur uit.*

Hiervoor implementeren en volgen we ook de komende jaren standaarden en best practices. Belangrijk onderdeel hierbij vormt de verdere professionalisering van ons (informatieveiligheids-)risicomanagement proces. Conform interprovinciale afspraak streeft de Provincie Limburg er naar om eind 2022 gereed zijn om te certificeren voor de ISO27001-norm. Daarnaast zetten we onze inspanningen voort, gericht op het verder versterken van het interne bewustzijn van onze medewerkers m.b.t. informatieveiligheid binnen (en buiten) de eigen werkomgeving. Met het groeiende belang van samenwerkingen waarbij het delen van data en informatie centraal staat, verwachten wij ook van onze (keten-)partners en leveranciers dat zij hun informatieveiligheid en privacy goed op orde hebben (voldoen aan de ISO27001/BIO en AVG of hiermee vergelijkbaar).

Tot slot zal ook de monitoring en rapportagestructuur verder uitgebouwd worden, waardoor we sneller en adequater actie kunnen ondernemen op eventuele (beveiligings-)incidenten. Provinciale Staten zullen, zoals sinds 2018 al gebeurt, jaarlijks in het eerste kwartaal schriftelijk geïnformeerd worden over de belangrijkste ontwikkelingen en activiteiten op dit gebied van het achterliggende jaar.

1.2. Het belang van informatieveiligheid

Vrijwel alle binnen de provinciale organisatie te onderscheiden bedrijfsprocessen zijn informatie-verwerkend van aard. Bij alle dagelijkse activiteiten wordt gebruik gemaakt van een scala aan informatie: niet alleen informatie over diverse beleidsonderwerpen, maar ook informatie over bedrijven, burgers, statenleden, leveranciers en werknemers; informatie die vertrouwelijk en privacygevoelig is.

Verlies, misbruik en/of “beschadiging” van informatie kan niet alleen gevaar opleveren voor de continuïteit van de bedrijfsvoering van de Provincie Limburg, maar kan o.a. ook de volgende consequenties met zich meebrengen:

- inbreuk op het vertrouwen in de Provincie Limburg van bijvoorbeeld burgers, bedrijven, instellingen, leveranciers en medewerkers;
- overtreding van wet- en regelgeving;
- (financiële) schade in relatie tot de hiervoor genoemde risico’s;
- imagoschade.

In dit verband kunnen diverse bedreigingen onderscheiden worden, o.a.: fraude, verkeerde invoer of verminking van informatie door hackers of virussen, inbraak, diefstal of vernieling, verlies van informatie, verspreiding van nep-informatie, storingen in apparatuur of programmatuur, calamiteiten (brand, wateroverlast, stroomstoring, e.d.).

Deze bedreigingen en de daaruit voortvloeiende risico’s hebben nog een extra dimensie gekregen door de explosieve groei van (elektronische) gegevensuitwisseling tussen mensen en organisaties, onder andere gestimuleerd door e-dienstverlening. Het beheersen van deze risico’s en daarmee ook het implementeren van geschikte maatregelen vereist zorgvuldige planning en aandacht vanuit een daartoe ingericht informatiebeveiligingsproces. Ook door de toename van het gebruik van social media, nieuwe manieren om informatie met elkaar te delen en het gebruik van smartphones en tablets worden extra eisen gesteld aan de informatieveiligheid.

De Provincie Limburg neemt ook op het gebied van informatievoorziening steeds meer een rol als (keten)partner op zich. Hierdoor kan de informatievoorziening niet meer als op zichzelf staand worden beschouwd, maar zal de informatievoorziening veel meer vanuit een ketenbenadering moeten worden opgepakt en beveiligd.

1.3. Het begrip Informatieveiligheid

Informatieveiligheid heeft betrekking op het garanderen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Het proces informatiebeveiliging geeft invulling aan de informatieveiligheid.

Onder informatiebeveiliging wordt verstaan: “Het definiëren, implementeren, onderhouden, handhaven en evalueren van een samenhangend stelsel van maatregelen gericht op het waarborgen van de beschikbaarheid, de integriteit, vertrouwelijkheid en controleerbaarheid van de (handmatige en geautomatiseerde) informatievoorziening”.

Beschikbaarheid:	*Het waarborgen dat alleen geautoriseerde gebruikers toegang hebben tot informatie en dat de benodigde bedrijfsmiddelen voorhanden zijn.*
Integriteit:	*Het waarborgen van de juistheid, de volledigheid en tijdigheid van informatie en verwerking.*
Vertrouwelijkheid:	*Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.*
Controleerbaarheid:	*Het waarborgen dat achteraf onweerlegbaar de toegang tot informatie en transacties gecontroleerd kan worden.*

1.4. Actualiteit

Met het belang van informatiebeveiliging worden bedrijven, overheid en particulieren vrijwel dagelijks geconfronteerd. Regelmatig verschijnen artikelen in de media met betrekking tot bedrijven en instellingen die getroffen worden door ransomware-aanvallen en datalekken. Steeds meer bedrijven en instellingen worden geconfronteerd met substantiële investeringen om de informatievoorziening op een hoger niveau te brengen en te houden.
Ook de Provincie Limburg neemt passende maatregelen om het risico op schade als gevolg van cyberdreigingen tot een acceptabel niveau te beperken.

In 9 trends in cybersecurity voor 2022 | WINMAG Pro wordt het volgende aangegeven: *"Het jaar 2021 kende een grote toename van het aantal cyberaanvallen, met wekelijks 446 getroffen bedrijven in Nederland, een stijging van maar liefst 86 procent ten opzichte van vorig jaar. Volgens het Cyber Security Predictions rapport van Check Point zet deze trend ook in 2022 door. Het rapport voorspelt dat cybercriminelen de pandemie blijven misbruiken en inventiever worden. In 2022 zullen aanvallers bijvoorbeeld misbruik maken van deepfakes, cryptocurrency en mobiele wallets".*

Het Cybersecuritybeeld Nederland[1] (CSBN), een uitgave van het Nationaal Cyber Security Centrum (NCSC), biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de weerbaarheid en risico's. Het accent ligt daarbij op de nationale veiligheid. Digitalisering biedt kansen, maar leent zich ook voor allerlei vormen van misbruik en is kwetsbaar voor uitval. Het CSBN is primair bedoeld voor strategie- en beleidsvorming op nationaal niveau (governance). Het geeft tevens een beeld van mogelijke risico's die ook voor Provincie Limburg van toepassing zijn.

Begin 2022 heeft de Zuidelijke Rekenkamer een vervolgonderzoek uitgevoerd naar de informatiebeveiliging van de Provincie Limburg. Uitgangspunt hierbij was de toets van de opvolging van de aanbevelingen uit het onderzoek van 2018. De resultaten van dit vervolgonderzoek zijn meegenomen als uitgangspunt voor het voorliggende informatiebeveiligingsbeleid.

Het informatiebeveiligingsbeleid heeft een directe relatie met het privacybeleid, in de zin dat het privacybeleid eisen stelt aan de informatieveiligheid en het proces van informatiebeveiliging.

[1] Het Cybersecuritybeeld Nederland 2021 is beschikbaar via https://www.ncsc.nl/onderwerpen/cyber-security-beeld-nederland. Het NCSC is onderdeel van het ministerie van Justitie en Veiligheid.

Overheidsbreed wordt ingezet op de baseline informatiebeveiliging overheid (BIO), die van toepassing is op de gehele overheid. Inmiddels hebben alle overheidsorganisaties zich geconformeerd aan deze baseline. Binnen het managementsysteem voor informatiebeveiliging (ISMS) wordt de compliancy t.o.v. de BIO gemonitord en wordt daar waar nodig bijgeschakeld.

1.5. Beleidsdocument

In het onderhavige document is het informatiebeveiligingsbeleid van de Provincie Limburg verwoord. Dit document is congruent met de informatie opgenomen in de beschrijving van het ISMS conform de ISO27001-standaard.

Het informatiebeveiligingsbeleid van de Provincie Limburg wordt vastgesteld door het College van Gedeputeerde Staten. De routing hiernaartoe verloopt via het CIO-overleg en het Directieteam-overleg. Het informatiebeveiligingsbeleid wordt a.d.h.v. de directiebeoordeling jaarlijks herijkt en daar waar nodig aangepast.

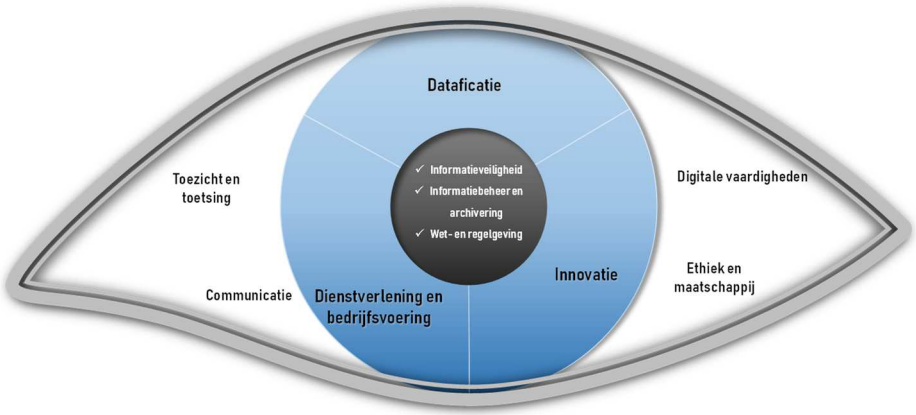
Het informatiebeveiligingsbeleid geeft de kaders aan waarbinnen de set aan informatiebeveiligings-maatregelen op basis van de ISO27002 en de Baseline Informatiebeveiliging Overheid (BIO) vorm krijgen. De sturing (governance) van de inrichting van deze maatregelen vindt plaats op basis van de PDCA-cyclus (ISMS).

2. Doelstelling en beleidsuitgangspunten informatiebeveiliging

2.1. Visie

De Provincie Limburg is een intensieve informatieverwerkende organisatie: nagenoeg alle producten en diensten die geleverd worden, bestaan uit informatie. Daarmee is dat een verbindende factor binnen de Provincie Limburg en tussen de Provincie Limburg en burgers, ondernemers en ketenpartners. Door de toename van gegevens en informatie is het aantal keuzemogelijkheden en het aantal keuze- en beslismomenten toegenomen. Tegelijkertijd is de tijd om te beslissen korter geworden. Het managen van gegevens en informatie als bedrijfsmiddel betekent dan ook dat, naast grondstoffen, arbeid en kapitaal, informatie gezien moet worden als het vierde bedrijfsmiddel. De betekenis van informatie (met de daaronder liggende gegevens) is zó cruciaal voor het succesvol functioneren van de organisatie dat er net zo mee omgegaan moet worden als met de traditionele productiemiddelen/bedrijfsmiddelen.

Het Strategisch Informatiebeleid Limburg (SIBL) positioneert informatie als strategisch bedrijfsmiddel dat randvoorwaardelijk is om de proces- en ketengerichte organisatie die de Provincie Limburg wil zijn optimaal te kunnen laten functioneren. Informatiebeveiliging vormt, samen met informatiebeheer en archivering en wet- en regelgeving, de basis van het uitvoeringsplan van het SIBL:



Het strategisch informatiebeleid spreekt van een visie die luidt: 'Wij digitaliseren en stellen daarbij de menselijke maat centraal. Dit doen we vanuit een open en lerende organisatie met ruimte voor innovatie, waarbij onze Limburgse maatschappelijke opgaven verbindend, eigentijds en verantwoord ondersteund worden'
Op basis hiervan wordt de volgende visie op informatiebeveiliging afgeleid:

Visie informatiebeveiliging

Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de Provincie Limburg. Burgers, bedrijven en instellingen kunnen erop vertrouwen dat met de aan de Provincie Limburg toevertrouwde informatie zorgvuldig wordt omgegaan.

2.2. Missie

Informatiebeveiliging is een continu proces om de risico's met betrekking tot de beschikbaarheid, integriteit en vertrouwelijkheid van informatie tot een acceptabel niveau te reduceren. Controleerbaarheid speelt een steeds prominentere rol in de informatiebeveiliging. Hierbij gaat het enerzijds om het onweerlegbaar kunnen aantonen wie welke gegevens heeft verwerkt en wie welke transactie heeft uitgevoerd. Anderzijds gaat het om de aantoonbaarheid van het bestaan én de werking van maatregelen om risico's die de Provincie Limburg in het kader van de informatieverwerking loopt, te mitigeren.

Missie informatiebeveiliging

Provincie Limburg zet in op het verhogen van de informatieveiligheid en verdere professionalisering van de informatiebeveiligingsfunctie binnen de organisatie. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn.

2.3. Doelstelling

Informatie komt in veel vormen voor (geschreven op papier, elektronisch opgeslagen, per post of via elektronische media verzonden, in gesproken vorm of in beeld). Het is een bedrijfsmiddel dat net als andere bedrijfsmiddelen van waarde is voor de Provincie Limburg en op een passende manier beveiligd dient te zijn. Informatiebeveiliging is geen doel op zich maar een integraal onderdeel van de bedrijfsprocessen en informatievoorziening van de Provincie Limburg.

Doelstelling

Het doel van informatiebeveiliging is het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie, die gebruikt worden binnen bedrijfsprocessen en informatiesystemen van de Provincie Limburg, door het opstellen, implementeren en onderhouden van een stelsel van maatregelen m.b.t. informatieveiligheid.

Hierbij wordt rekening gehouden met de te stellen eisen vanuit wet- en regelgeving, contractuele verplichtingen alsmede de resultaten van een globale risicoanalyse en eventuele beveiligingsincidenten die zich in de praktijk hebben voorgedaan. Het stelsel van maatregelen is gebaseerd op de ISO27002 en wordt aangevuld vanuit de BIO en eigen risicoanalyses.
Dit informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om de informatie van de Provincie Limburg te beschermen en te waarborgen, zodat de Provincie Limburg voldoet aan relevante wet- en regelgeving. De Provincie Limburg streeft er naar om ‘in control’ te zijn en daarover op passende wijze verantwoording af te leggen.

2.4. Beleidsuitgangspunten

Naast de hieronder opgenomen beleidsuitgangspunten zijn een aantal uitgangspunten verwoord in afzonderlijke beleidsdocumenten en als bijlage toegevoegd.

1. We zien informatie als strategisch bedrijfsmiddel
   Informatie is een bedrijfsmiddel dat net als andere bedrijfsmiddelen van waarde is voor de Provincie Limburg en op een passende manier beveiligd dient te zijn. Hierbij gaat het met name om de beschikbaarheid, de integriteit en de vertrouwelijkheid van de informatie. Aan de hand van classificatie wordt het beveiligingsniveau zichtbaar gemaakt en worden passende maatregelen getroffen. Informatie in combinatie met een toepassing (applicatie/informatiesysteem) heeft een eigenaar. De eigenaar is verantwoordelijk voor het autorisatiebeheer, het correct gebruik en de kwaliteit van de gegevens en het systeem. Hierbij vindt ondersteuning plaats vanuit het cluster Organisatie en Informatie en/of de leverancier van de toepassing.

2. We voldoen aan wet- en regelgeving

Op de informatieverwerking is wet- en regelgeving van toepassing. De Provincie Limburg respecteert deze wet- en regelgeving en zal, daar waar nodig, maatregelen treffen om aan de betreffende wet- en regelgeving te voldoen. Vanuit aanpalend beleid (o.a. het privacybeleid) kunnen aanvullende informatiebeveiligingsmaatregelen worden gevraagd.

3. We kiezen voor een risicogebaseerde aanpak
   De maatregelen die worden voorgesteld in ISO27002 en de BIO zijn gebaseerd zijn op een algemene risicoanalyse voor resp. de provincies en de overheid. Dit resulteert in een baseline, die bestaat uit een set van maatregelen die ervoor zorgen dat de risico's tot een aanvaardbaar niveau worden beperkt. Daarbij kan het zijn dat de Provincie Limburg besluit, op basis van een eigen risicoanalyse, om extra maatregelen uit te voeren. De maatregelen die de Provincie Limburg in het kader van informatiebeveiliging neemt, zijn gebaseerd op de basisset aan maatregelen en aanvullende risicoanalyses die periodiek worden uitgevoerd.

4. Ons personeel is bewust bekwaam op het gebied van informatieveiligheid
   Het verwerken van gegevens tot informatie vindt primair plaats door de medewerkers van de Provincie Limburg. Het is essentieel dat de medewerkers zich bewust zijn van de risico's van het gebruik van analoge en digitale gegevensdragers. Met digitale gegevensdragers worden applicaties en bestanden bedoeld die op de infrastructuur van de Provincie Limburg of extern zijn opgeslagen. Bewustwording informatieveiligheid heeft continu aandacht. De medewerkers worden hierbij actief betrokken.

5. Onze leveranciers conformeren zich aan ons informatiebeveiligingsbeleid
   Van leveranciers wordt verwacht dat zij bijdragen aan de uitvoering van het informatie-beveiligingsbeleid van de Provincie Limburg. Gewaarborgd wordt dat geleverde producten en diensten **niet** in strijd zijn met het informatiebeveiligingsbeleid van de Provincie Limburg en specifiek de hieraan gekoppelde wet- en regelgeving (AVG, Archiefwet e.d.).

6. We leggen verantwoording af over informatieveiligheid
   De Provincie Limburg streeft naar een actieve monitoring van het informatiebeveiligingsniveau dat, voor zover niet vertrouwelijk, openbaar is. GS informeren de Staten periodiek ten aanzien van de informatieveiligheid van de Provincie Limburg. Naast de interne rapportage (conform ISO27001) kunnen hier ook onafhankelijke onderzoeken van externe partijen hier ten grondslag liggen. De Provincie Limburg streeft er naar om met zo laag mogelijk risico zo open en transparant mogelijk te communiceren over haar informatieveiligheid.

7. We maken de informatievoorziening beheersbaar
   Het is zaak om kwetsbaarheden in de informatievoorziening zo snel mogelijk, zowel tijdens als buiten kantoortijden, in beeld te krijgen zodat tijdig adequate maatregelen getroffen kunnen worden.
   Enerzijds betekent dit dat bij de aanschaf en bij de ontwikkeling van onderdelen van de informatievoorziening rekening gehouden wordt met informatiebeveiligings- en privacyaspecten. Dit uitgangspunt wordt ook wel aangeduid als "security en privacy by design en by default".
   Anderzijds betekent dit dat de bestaande informatievoorziening continu gemonitord wordt op kwetsbaarheden binnen de digitale infrastructuur van de Provincie Limburg. In geval van

kwetsbaarheden wordt actie ondernomen om de risico's zo klein mogelijk te houden. Dit kan betekenen dat de informatievoorziening voor een bepaalde periode op een lager niveau van beschikbaarheid functioneert.
Beheersbaarheid betekent ook dat voor vrijwel dezelfde functionaliteit slechts één toepassing in gebruik is, dat die toepassing één eigenaar heeft en dat deze verantwoordelijk is voor het opruimen van de toepassing indien deze niet meer nodig is (applicatie lifecycle management).

8. We zorgen voor bedrijfscontinuïteit
   Naast vertrouwelijkheid en integriteit is beschikbaarheid een belangrijk aspect van de informatieveiligheid. De juiste informatie dient op het juiste moment en op de juiste plaats beschikbaar te zijn voor de uitvoering van het betreffende proces. Ten aanzien van de vereiste beschikbaarheid dienen afspraken gemaakt te worden met de diverse partijen die een rol spelen bij de levering van de informatievoorziening. De continuïteit van de informatievoorziening maakt integraal onderdeel uit van de bedrijfscontinuïteit.

9. We werken conform het managementproces informatiebeveiliging
   Het proces van informatiebeveiliging wordt cyclisch gestuurd vanuit een periodiek uit te voeren risicoanalyse. Vanuit het kader van de ISO27002 en de hiervan afgeleide BIO worden de te treffen maatregelen vastgesteld. Aan de hand van een PDCA-cyclus worden deze maatregelen ingevoerd, getoetst en indien nodig bijgesteld. Dit proces wordt aangeduid als Information security management system (ISMS). Onderdeel van het ISMS vormt de registratie van informatiebeveiligingsincidenten.

10. We conformeren ons aan de Baseline Informatiebeveiliging Overheid (BIO)
    De baseline bestaat uit de business impact analyse en de maatregelensets. De baseline informatiebeveiliging geeft een standaard werkwijze waarmee per bedrijfsproces of per informatiesysteem bepaald wordt welke beveiligingsmaatregelen getroffen moeten worden. De baseline informatiebeveiliging overheid (BIO) zorgt voor een uniforme werkwijze voor alle overheidsorganisaties op het gebied van informatiebeveiliging.

De onderstaande beleidsonderwerpen zijn verder uitgewerkt in gelijknamige beleidsdocumenten:

- Beleid logische toegang;
- Beleid fysieke toegang;
- Beleid veilig mobiel werken;
- Beleid cryptografie;
- Beleid logging;
- Beleid clean desk en clear screen;
- Beleid Backup en recovery;
- Beleid Informatietransport.

2.5. Reikwijdte informatiebeveiligingsbeleid

Binnen de Provincie Limburg wordt informatieveiligheid breed geïnterpreteerd en betreft het **alle** vormen van informatie. Daarmee beperkt informatieveiligheid zich **niet** tot digitale informatie. Het

informatiebeveiligingsbeleid is van toepassing op alle (informatie)diensten die de Provincie Limburg levert of afneemt van derden.
Het informatiebeveiligingsbeleid heeft betrekking op alle toepassingen die vallen onder verantwoordelijkheid van de Gedeputeerde Staten van Provincie Limburg. Dit betreft toepassingen die op locatie van de Provincie Limburg worden uitgevoerd, die extern worden gehost en die in de cloud worden afgenomen. Het informatiebeveiligingsbeleid is van toepassing op alle interne en externe afnemers van diensten van de Provincie Limburg, zoals bijvoorbeeld Statenleden, Griffie en RUD-ZL.

Informatieveiligheid heeft een duidelijke relatie met fysieke beveiliging, bedrijfscontinuïteit (business continuity) en privacy. Het informatiebeveiligingsbeleid sluit hier op aan.

2.6. Randvoorwaarden in relatie tot informatieveiligheid

De basis voor de set aan beveiligingsmaatregelen van de Provincie Limburg wordt gevormd door de ISO 27002 beheersmaatregelen en de hiervan afgeleide baseline informatiebeveiliging overheid (BIO).

Voor de Provincie Limburg gelden de wettelijke voorschriften op het gebied van informatiebeveiliging en geheimhouding. Daarnaast en in aanvulling hierop gelden de eigen specifieke regelingen. Voor wat betreft de meest relevante wet- en regelgeving gaat het in ieder geval om: AVG, WOO, Wet Computercriminaliteit III, Archiefwet 1995, Wet elektronisch berichtenverkeer, Wet hergebruik overheidsinformatie, Wet meldplicht datalekken, Auteurswet, de Telecommunicatiewet, de Databankenwet en de Regeling elektronische handtekening. Deze wet- en regelgeving is medebepalend voor de maatregelen die genomen worden in het kader van informatieveiligheid.

De clustermanager Organisatie en Informatie is door het college van Gedeputeerde Staten / Directie gemandateerd om de binnen dit informatiebeveiligingsbeleid te nemen maatregelen, voor zover deze vallen binnen het aandachtsgebied van informatievoorziening, vast te stellen en uit te voeren. Maatregelen die buiten dit aandachtsgebied vallen worden in overleg met de betreffende verantwoordelijke ter vaststelling voorgelegd binnen dat cluster. Voorbeelden hiervan zijn maatregelen in het kader van fysieke toegangsbeveiliging (cluster Facilitaire Dienstverlening), maatregelen in het kader van personeel (cluster Personeel en Organisatie) en maatregelen in het kader van privacybescherming (Algehele Juridische Zaken).

3. Organisatie van de informatiebeveiliging

Informatiebeveiliging maakt integraal onderdeel uit van alle processen van de Provincie Limburg en heeft betrekking op het treffen van maatregelen om de binnen deze processen beschikbare informatie te beschermen. Informatiebeveiliging beperkt zich daarbij niet alleen tot ICT-gerelateerde zaken.

Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met de set aan informatiebeveiligingsmaatregelen het fundament onder een betrouwbare informatievoorziening.

Informatiebeveiliging wordt enerzijds beschouwd als een op zich zelf staand proces dat, met inachtname van de hierna aangegeven verantwoordelijkheden, gericht is op het managen van de aanwezige informatiebeveiligingsrisico's binnen de provinciale organisatie. Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem (ISMS) van informatiebeveiliging. Anderzijds dient informatiebeveiliging steeds meer een integraal onderdeel te worden van de processen binnen de organisatie. Dit uit zich met name in de verantwoordelijkheid voor het uitvoeren van beveiligingsmaatregelen.

Een aantal activiteiten (tactisch/strategisch) in het kader van informatiebeveiliging worden verbijzonderd in de rol van concern information security officer (CISO). Deze rol is belegd binnen het cluster Organisatie en Informatie bij de functie senior adviseur Organisatie en Informatie. De CISO ondersteunt de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover aan de directie en GS. De CISO is lid van het interprovinciaal platform informatiebeveiliging (CIBO). Met betrekking tot zaken die betrekking hebben op privacy stemt de CISO intern af met de privacyfunctionaris en de functionaris gegevensbescherming (FG). De CISO heeft een rol bij de veranderingen binnen de organisatie op het gebied van informatievoorziening. Hiervoor neemt de CISO deel aan de "change advisory board[2]" (CAB) en is hij agendalid van het CIO-overleg.
Op uitvoerend niveau worden activiteiten op het gebied van informatiebeveiliging binnen het cluster Organisatie en Informatie uitgevoerd door individuele beheerders en de technical information security officer (TISO), die een coördinerende rol binnen het team I-Services vervult. De TISO neemt, samen met, de teammanager van I-Services, de CISO en de clustermanager deel aan het 2-wekelijkse interne informatiebeveiligingsoverleg deel.

3.1. Verantwoordelijkheden

Binnen de informatiebeveiligingsorganisatie worden een drietal rollen onderkend: de sturende rol, de vragende rol en de uitvoerende rol. Hieronder wordt ingegaan op de verantwoordelijkheden van deze rollen.

De sturende rol

- Het College van Gedeputeerde Staten is integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de Provincie Limburg.
  Het College van Gedeputeerde Staten:
  - stelt het informatiebeveiligingsbeleid vast;
  - belegt informatieveiligheid bij de portefeuillehouder bedrijfsvoering binnen het College van Gedeputeerde Staten.

- De directie van de Provincie Limburg is verantwoordelijk voor de totstandkoming en de uitvoering van het informatiebeveiligingsbeleid en wordt terzake ondersteund door het cluster Organisatie en Informatie.

[2] De change advisory board (CAB) is een intern overleg binnen het cluster Organisatie en Informatie, dat een belangrijk onderdeel vormt van het wijzigingsbeheer proces. Het CAB adviseert over niet-standaard wijzigingen en beoordeelt o.a. risico's die met het doorvoeren van deze wijzigingen gepaard gaan.

De directie:

- belegt informatieveiligheid bij de verantwoordelijke directeur voor bedrijfsvoering-CIO;
- stuurt op concern risico's;
- is verantwoordelijk voor kaderstelling op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders;
- is verantwoordelijk voor de controle of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden en wordt hierbij inhoudelijk en procesmatig ondersteund door het cluster Concern
- evalueert periodiek beleidskaders en stelt deze waar nodig bij;
- wordt hierbij ondersteund door het cluster Organisatie en Informatie.

De vragende (eigenaars) rol

- Elke clustermanager binnen de Provincie Limburg is verantwoordelijk voor de uitvoering van de processen (gegevens) binnen zijn/haar cluster en derhalve ook verantwoordelijk voor de aan deze processen gerelateerde informatiebeveiliging. Het cluster Organisatie en Informatie (i.c. de CISO) ondersteunt de clustermanager bij deze activiteiten (waaronder: risicoanalyse, business impact analyse, definiëren van aanvullende beveiligingseisen). De medewerkers spelen een belangrijke rol bij het toepassen van maatregelen op het gebied van informatiebeveiliging: samen wordt invulling gegeven aan de informatiebeveiliging.

  De clustermanagers:

  - zijn verantwoordelijk voor het vaststellen van de risico's op het gebied van informatieveiligheid voor wat betreft de processen en informatiesystemen die onder hun verantwoordelijkheid vallen (risicoanalyse);
  - zijn verantwoordelijk voor het classificeren van de gegevens en informatiesystemen die onder hun verantwoordelijkheid vallen (dataclassificatie);
  - zijn verantwoordelijk voor de keuze, de implementatie en het uitvoeren van de maatregelen die voortvloeien uit de betrouwbaarheidseisen, voor zover deze binnen het verantwoordelijkheidsgebied van de betreffende clustermanager vallen;
  - sturen op bedrijfscontinuïteit, beveiligingsbewustzijn, en naleving van regels en richtlijnen (eigen verantwoordelijkheid).

  De medewerkers:

  - hebben een eigen verantwoordelijkheid in relatie tot het onderkennen van infomatie-beveiligingsrisico's en de te treffen informatiebeveiligingsmaatregelen; samen wordt invulling gegeven aan de informatiebeveiliging.

De uitvoerende rol

- De serviceclusters binnen de Provincie Limburg (Organisatie en Informatie, Personeel en Organisatie, Facilitaire Dienstverlening, Algehele Juridische Zaken, Inkoop en Aanbestedingen) zijn verantwoordelijk voor de uitvoerende rol v.w.b. het opstellen van de relevante informatiebeveiligingsmaatregelen. Het komen tot een evenwichtige set van maatregelen, waarbij recht wordt gedaan aan de verschillende disciplines vergt een gecoördineerde afstemming tussen de clusters Organisatie en Informatie, Personeel en Organisatie, Facilitaire Dienstverlening, Algehele Juridische Zaken, Inkoop en Aanbestedingen en Concern. Deze zijn ook vertegenwoordigt in het zgn.

security board. Het security board bereidt de formele besluitvorming voor op het gebied van informatiebeveiliging.

Het cluster Organisatie en Informatie:

- is verantwoordelijk voor de beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen voor zover deze binnen het verantwoordelijkheidsgebied van het cluster Organisatie en Informatie vallen en voortvloeien uit de betrouwbaarheidseisen (classificaties);
- het cluster Organisatie en Informatie faciliteert het gebruik van de informatievoorziening binnen Provincie Limburg en een beperkt aantal externe afnemers. In het kader van de ISO27001 wordt dit gezien als de scope voor informatiebeveiliging.

De CISO:

- is verantwoordelijk voor de uitvoering van het informatiebeveiligingsproces (ISMS);
- is mede verantwoordelijk voor de uitvoering van de risicoanalyse, in nauwe samenwerking met de eigenaar van de informatievoorziening en de concernstaf;
- verzorgt monitoring en rapportage m.b.t. de informatieveiligheid;
- rapporteert over compliance aan wet- en regelgeving en algemeen beleid van de Provincie Limburg;
- stelt, samen met de stakeholders uit de organisatie het Informatiebeveiligingsbeleid op;
- stelt op basis van het vastgestelde informatiebeveiligingsbeleid de te nemen maatregelen op en stemt deze af binnen de organisatie;
- geeft beveiligingsadvies aan GS, directie en clusters;
- adviseert over informatiebeveiligingsmaatregelen die leiden tot uitvoering van activiteiten binnen de overige serviceclusters (Personeel en Organisatie, Facilitaire Dienstverlening, Algehele Juridische Zaken en Inkoop en Aanbestedingen).

Het cluster Personeel en Organisatie:

- is verantwoordelijk voor het opstellen, uitdragen en uitvoeren van maatregelen die liggen op het grensvlak tussen informatiebeveiliging en HRM.

Het cluster Facilitaire Dienstverlening:

- is verantwoordelijk voor het opstellen, uitdragen en uitvoeren van maatregelen in het kader van de fysieke informatiebeveiliging (bijvoorbeeld: fysieke toegangsbeveiliging).

Het cluster Algehele Juridische Zaken:

- is verantwoordelijk voor het adviseren over het toepassen van de relevante wet en regelgeving bij het opstellen van de maatregelen in het kader van informatiebeveiliging en privacy.

Het cluster Inkoop en Aanbestedingen:

- is verantwoordelijk voor het opstellen, uitdragen en uitvoeren van maatregelen in het kader van de inkoop en aanbesteding van ICT-diensten en middelen en het (ICT-) leveranciersmanagement.

Het cluster Concern:

- is verantwoordelijk voor de derde lijn controle m.b.t. informatiebeveiliging en de ISO27001/BIO compliancy.

4. Controle en naleving

In lijn met het managementsysteem voor informatieveiligheid vindt periodieke rapportage plaats over de belangrijkste aspecten met betrekking tot informatiebeveiliging binnen Provincie Limburg. Onderdeel van de zgn. directiebeoordeling is een jaarlijkse review van het beleid. Ook bij grote wijzigingen en n.a.v. major informatiebeveiligingsincidenten kan het informatiebeveiligingsbeleid beoordeeld worden.

5. Vaststelling

Dit beleidsdocument is vastgesteld door het directie team in de DT vergadering van dd. 4 juli 2022. Dit document wordt meegenomen in de jaarlijkse beoordeling van de beleidsdocumenten op het gebied van informatiebeveiliging.

provincie limburg

Beleid logische toegang Provincie Limburg

1. Beleidsuitgangspunten Provincie Limburg

Ten behoeve van de autorisatie voor de toegang tot applicaties en gegevens zijn in het kader van informatiebeveiliging een aantal beleidsuitgangspunten opgesteld. Het doel van dit beleid is te voorkomen dat onrechtmatig toegang verkregen wordt tot applicaties en gegevens van de Provincie Limburg.
Het beleid logische toegangsbeveiliging is van toepassing op alle applicaties, gegevens en overige componenten van de informatievoorziening waarvan de Provincie Limburg eigenaar is. Dit geldt ook wanneer de informatievoorziening niet op de infrastructuur van de Provincie Limburg wordt uitgevoerd (hosting, cloud). Ook in die gevallen is het beleid logische toegang van toepassing.

2. Uitgangspunten logische toegang

De Provincie Limburg hanteert de volgende beleidsuitgangspunten en deze zijn mede ontleend aan de BIO:

Eigenaarschap

- Iedere applicatie en gegevensverzameling heeft een eigenaar;
- De eigenaar bepaalt de toegang tot de applicatie en de rechten binnen die applicatie;
- De eigenaar is verantwoordelijk voor adequate training in het gebruik van de applicatie;
- De eigenaar bepaalt wie toegang heeft tot gegevens uit de applicatie (voor zover dit al niet gebeurt op basis van applicatierechten);
- De eigenaar van een applicatie en gegevens dient het toezicht op de uitvoering van de autorisatieprocedure goed te regelen en te documenteren. Hij neemt interne beheersmaatregelen die in overeenstemming zijn met de eisen die uit de baselinetoets BIO of risicoanalyse voortvloeien;

Authenticatie

- Iedere persoon die gebruik maakt van de infrastructuur, applicaties en gegevens is bekend;
- Alleen personen die zijn opgenomen binnen het Personeelsinformatiesysteem van de Provincie Limburg (geverifieerde identiteit en screening) komen in aanmerking voor een account voor toegang tot de informatievoorziening van de Provincie Limburg;
- Authenticatie vanuit een onveilige zone[1] vindt plaats op basis van gebruikersnaam, wachtwoord en een tweede factor;
- Het verdient de voorkeur om in alle gevallen gebruik te maken van de generieke authenticatie methodiek;[2]
- Er worden in de regel geen ‘algemene’ (ongepersonaliseerde) identiteiten gebruikt.[3]

[1] Alleen het bekabelde netwerk binnen het gouvernement wordt gezien als veilige zone, Overige netwerken worden als onveilig beschouwd.

[2] Het gaat hier om de centrale registratie van identiteiten op basis van de gegevens uit het personeels informatie systeem en de koppeling hiervan aan “rollen” t.b.v. de autorisatie voor en binnen de verschillende applicaties

[3] Uit A.9.2.1: “het gebruik van groepsidentificaties

Wachtwoorden

- Het algemene wachtwoord sluit aan op de complexiteitsvoorschriften uit de BIO(9.4.3.1).
- Het wachtwoord heeft een geldigheid van maximaal 6 maanden;
- Applicaties die geen gebruik maken van de generieke authenticatie en autorisatie methodiek conformeren zich aan de standaard voor het wachtwoord;

Autorisatie

- Op basis van functie en rol van een medewerker worden autorisaties toegekend;
- De eigenaar van de applicatie en gegevens is verantwoordelijk voor een juiste toekenning en intrekking van de autorisatie;
- Autorisaties voor applicaties worden bij voorkeur beheerd vanuit een centrale omgeving;
- De eigenaar van een applicatie wordt periodiek (minimaal 1 maal per 6 maanden), ter beoordeling van de juistheid, op de hoogte gesteld van de betreffende autorisaties;

Functiescheiding

- De beschikkende, bewarende en controlerende taken worden in beginsel nooit bij één functionaris tezamen gebracht. Indien dit toch noodzakelijk is, dan worden voor de uitvoering van deze taken door de eigenaar van de applicatie aanvullende maatregelen genomen;
- Een autorisatie voor beheeractiviteiten dient zo veel als mogelijk gescheiden te zijn van autorisaties voor de gegevens binnen een dergelijk applicatie;

Priveleged users

- Hieronder worden die interne en externe medewerkers verstaan die (tijdelijk) administrator-rechten hebben. Zij beschikken hiervoor over een persoonlijk admin-account;
- Het admin-account is toegekend aan één medewerker met de betreffende beheertaak;
- Een admin-account dient enkel gebruikt te worden bij de uitvoering van de betreffende administrator werkzaamheden. De hiervoor noodzakelijke rechten zijn toegekend aan dit account;
- Handelingen uitgevoerd met een admin-account worden gelogd;

Inhuur extern personeel

- De door Provincie Limburg ingehuurde externen vallen onverkort onder het beleid logische toegangsbeveiliging en dienen conform deze regels te handelen;
- Aan de hand van hun taken/functie/rol geeft de eigenaar van de applicatie ingehuurde externe medewerkers toegang tot de applicatie en de gegevens;

Uitbestede dienstverlening

- De ICT-dienstverlener zal een beveiligingsbeleid moeten hebben en geëffectueerde maatregelen, die zij aan de Provincie Limburg inzichtelijk maakt en die in lijn zijn met dit beleid logische toegang;

---

behoort alleen te worden toegelaten als deze om bedrijfs- of operationele redenen noodzakelijk zijn en behoort te worden goedgekeurd en gedocumenteerd;”

- De ICT-dienstverlener is verantwoordelijk voor een correcte inrichting van het eigen beveiligingsbeleid en naleving hiervan binnen de eigen organisatie.
- De ICT-dienstverlener voldoet aan de normen en eisen die gesteld zijn in het informatiebeveiligingsbeleid c.q. beleid logische toegangsbeveiliging van de Provincie Limburg;
- De ICT-dienstverlener voldoet aan de van toepassing zijnde wet- en regelgeving;
-
- De ICT-dienstverlener beschikt over een functionaris informatiebeveiliging, die verantwoordelijk is voor het informatiebeveiligingsbeleid van de ICT-dienstverlener en die contactpersoon is voor de CISO van Provincie Limburg;
- De ICT-dienstverlener beschikt over een autorisatiebeheerder voor de dagelijkse operatie die verantwoordelijk is voor een correcte inrichting van de autorisaties en die op dit gebied aanspreekpunt is voor de systeem/gegevenseigenaar binnen de Provincie Limburg;
- De ICT-dienstverlener stelt capaciteit en informatie beschikbaar t.b.v. audits op het gebied van autorisaties, die in opdracht van Provincie Limburg uitgevoerd worden.

3. Controle en naleving

In lijn met het managementsysteem voor informatieveiligheid vindt rapportage plaats over de belangrijkste aspecten van authenticatie en autorisatie binnen de provincie.

4. Vaststelling

Dit beleidsdocument is vastgesteld door het directie team in de DT vergadering van dd. 4 juli 2022. Dit document wordt meegenomen in de jaarlijkse beoordeling van de beleidsdocumenten op het gebied van informatiebeveiliging.

provincie limburg

Beleid fysieke toegang Provincie Limburg

1. Beleidsuitgangspunten Provincie Limburg

Ten behoeve van de beveiliging van informatie is er toegangsbeleid voor alle provinciale voorzieningen. Het doel van dit beleid is te voorkomen dat onbevoegden toegang krijgen tot ruimtes met informatie waar zij geen kennis van behoren te nemen dan wel dat informatie kan worden aangepast. Het toegangsbeleid spitst zich daarnaast toe op de fysieke beveiliging van kantoren, ruimten en faciliteiten.

2. Uitgangspunten fysieke toegang

De Provincie Limburg hanteert de volgende beleidsuitgangspunten en deze zijn ontleend uit de BIO:

a. Er is een zoneringsplan met daarin opgenomen de volgende zones: Openbaar, wachtruimten en spreekkamers, werkruimten, ICT-ruimte/beveiligde ruimte en een off-site backup locatie.
b. Er is een overvalplan met afspraken over aanrijroutes en contacten met de politie.
c. Er is cameratoezicht op toegangswegen, in het gebouw en beveiligde ruimtes.
d. Gebouwen bieden voldoende weerstand bij gewelddadige aanvallen zoals inbraak en vandalisme, hierbij wordt ook rekening gehouden met de omgeving.
e. De kwaliteit van de toegangsmiddelen hoort in overeenstemming te zijn met de zonering.
f. Toegang tot gebouwen of beveiligingszones is alleen mogelijk na autorisatie.
g. Voor toegang tot speciale ruimtes is doelbinding vereist. Toegang tot deze ruimtes wordt middels logging vastgelegd. Deze toegangslijsten dienen periodiek gecontroleerd te worden.
h. De provincie Limburg heeft barrières aangebracht om ruimten te beschermen waar zich ICT-voorzieningen dan wel persoonsgegevens (art. 9 en 10 AVG) en/of gevoelige gegevens bevinden (classificatie).
i. In gebouwen met beveiligde zones houdt beveiligingspersoneel toezicht op de toegang en houdt hiervan een registratie bij.
j. Er is 24 uur, 7 dagen per week bewaking met een inbraak alarm gekoppeld aan een alarmcentrale. Voor alle medewerkers die autorisatie hebben om het alarm te bedienen dient een persoonlijke code gebruikt te worden; er wordt geen gebruik gemaakt van een generieke code.
k. Medewerkers/bezoekers zonder autorisatie mogen alleen onder begeleiding van bevoegd personeel en als er een noodzaak is, toegang krijgen tot de beveiligde omgeving.
l. Zonder expliciete toestemming mogen in beveiligde ruimtes geen opnames (beeld en/of geluid) worden gemaakt.
m. Niet uitgegeven toegangsmiddelen worden beveiligd opgeborgen.
n. Toegangsmiddelen vallen primair onder de verantwoordelijkheid van het cluster Facilitaire Dienstverlening.
o. Er vindt één keer per half jaar een controle/evaluatie plaats op de autorisaties voor fysieke toegang. Voor speciale toegangsrechten is dat minimaal ieder kwartaal.
p. De huisregels voor toegangsbeleid worden bekend gesteld aan al het personeel en de bezoekers.
q. Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, zijn beheerst en afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.

3. Controle en naleving

In lijn met het managementsysteem voor informatieveiligheid vindt rapportage plaats over de belangrijkste aspecten m.b.t. fysieke toegang binnen de provincie.

4. Vaststelling

Dit beleidsdocument is vastgesteld door het directie team in de DT vergadering van dd. 4 juli 2022. Dit document wordt meegenomen in de jaarlijkse beoordeling van de beleidsdocumenten op het gebied van informatiebeveiliging.

provincie limburg

Beleid clean desk en clear screen Provincie Limburg

1. Beleidsuitgangspunten Provincie Limburg

De medewerkers van de Provincie Limburg verwerken veel (gevoelige) informatie. Deze informatie verschijnt in verschillende verschijningsvormen zoals informatie op papier, computers, laptops, telefoons, USB-sticks en tablets. Door het onbeheerd en onbeschermd achterlaten van deze informatie in persoonlijke of publieke ruimten, kunnen onbevoegden toegang krijgen tot deze informatie. Om deze reden is het belangrijk dat medewerkers van de Provincie Limburg zorgvuldig met informatie omgaan.

Het doel van dit beleid is waarborgen dat informatie waar de Provincie Limburg verantwoordelijk voor is niet (onbedoeld) in verkeerde handen komt, en het creëren van bewustzijn bij de medewerkers van de Provincie Limburg over het verantwoordelijk omgaan met informatie die aan hen is beschikbaar gesteld.

2. Uitgangspunten clean desk clear screen beleid

De Provincie Limburg hanteert de volgende beleidsuitgangspunten:

a. Vertrouwelijke of geheime informatie wordt niet onbeheerd achtergelaten, bijvoorbeeld op bureaus, printers of in vergaderruimtes;
b. Gevoelige informatie wordt veilig opgeslagen voordat de werkplek of het gebouw wordt verlaten;
c. Voor de (tijdelijke) opslag van digitale en analoge gegevensdragers worden voorzieningen (afsluitbare lockers, ladeblokken en kasten) ter beschikking gesteld;
d. Het gebruik van mobiele gegevensdragers (b.v. USB-sticks ed.) wordt ten zeerste afgeraden. Indien deze toch worden gebruikt, dienen deze veilig te worden opgeborgen voordat de werkplek wordt verlaten;
e. Bij het verlaten van de werkplek worden computers, laptops e.d. vergrendeld;
f. Het vergrendelen (met wachtwoord) van de werkplek vindt automatisch plaats na 10 minuten inactiviteit;
g. Het automatisch uitloggen vindt plaats na 120 minuten van inactiviteit;
h. Bij het verlaten van het gebouw worden computers, laptops ed. afgesloten;
i. Het bewaren van informatie vindt plaats aan de hand van de hiervoor geldende richtlijnen (besluit informatiebeheer 2022);
j. Men dient zich er van bewust te zijn dat met name in openbare ruimtes kan worden meegekeken op schermen of papieren documenten;
k. De werkplek dient schoon te worden achtergelaten. Dit geldt in het bijzonder voor flexplekken;
l. Afval wordt gescheiden bij de servicepunten weggegooid;
m. Bij de printers slingeren geen onbeheerde documenten rond.

3. Controle en naleving

Elk cluster is zelf verantwoordelijk voor een correcte naleving van dit beleid. In lijn met het managementsysteem voor informatieveiligheid vindt rapportage plaats over de belangrijkste aspecten m.b.t. clean desk en clear screen binnen de Provincie.

4. Vaststelling

Dit beleidsdocument is vastgesteld door het directieteam in de DT vergadering van dd. 4 juli 2022. Dit document wordt meegenomen in de jaarlijkse beoordeling van de beleidsdocumenten op het gebied van informatiebeveiliging.

provincie limburg

Beleid Backup Provincie Limburg

1. Doel backup Provincie Limburg

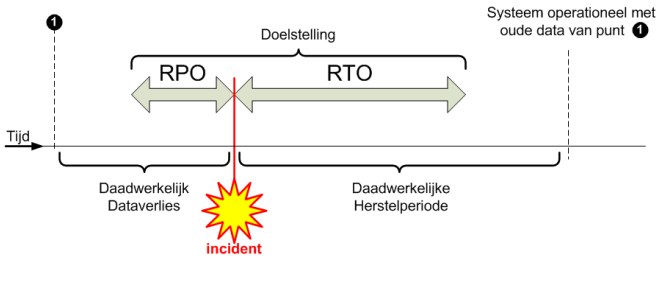
Ten behoeve van de backup van gegevens zijn in het kader van informatiebeveiliging een aantal beleidsuitgangspunten opgesteld. Het doel van dit beleid is te bewerkstelligen dat op een betrouwbare wijze backup en restore kan plaatsvinden, zodat de risico's in geval van geheel of gedeeltelijk verlies, of beschadiging van data tot een aanvaardbaar niveau kunnen worden beperkt.

2. Beleidsuitgangspunten backup

De Provincie Limburg hanteert de volgende beleidsuitgangspunten, die ontleend zijn aan de BIO en aanvullend zijn op het algemene informatiebeveiligingsbeleid van de Provincie Limburg.

a. Binnen Provincie Limburg worden een aantal type gegevens onderkend die een eigen backup-procedure hebben. Het betreft de volgend type gegevens:
   - Database omgeving (Sqlserver en Oracle);
   - Filesystemen (CFIS Common Internet File System);
   - E-mailsysteem (Exchange);
   - VMware-servers;
   - Netwerkcomponenten (CISCO).

b. Gegevensverlies
   Bij het vaststellen van de frequentie van de het uitvoeren van een backup wordt enerzijds gekeken naar de maximale tijdsperiode waarover gegevens verloren mogen raken (RPO[1]) en de maximaal toelaatbare hersteltijd (RTO[2]).



Bron: https://nl.wikipedia.org/wiki/Recovery_Time_Objective#/media/Bestand:RPO_RTO_voorbeeld_NL.png

[1] Recovery Point Objective (RPO) betekent herstelpuntdoelstelling en is het streven om te voldoen aan de afgesproken maximaal toelaatbare hoeveelheid dataverlies na een computercrash.

[2] Recovery Time Objective (RTO) betekent hersteltijddoelstelling en is het streven om te voldoen aan de afgesproken hersteltijd na een computercrash.

- Vanuit een generiek oogpunt wordt voor alle data de RPO vastgesteld op maximaal 28 uur en de maximale hersteltijd op 16 uur met een betrouwbaarheid van 85% (BIO 12.3.1.3).

c. Bescherming van backups
   - Integriteit
     Na het maken van een back-up dient een toets plaats te vinden omtrent de integriteit van de backup. Dit gebeurt bij voorkeur automatisch. Daarnaast dient de integriteit van de backup gewaarborgd te zijn. Manipulatie van de backup moet worden uitgesloten.
   - Locatie
     Bij de opslag van de backups dient rekening gehouden te worden met een fysieke scheiding tussen de verschillende versies van de backup. Bijvoorbeeld door het hebben van een primaire backup op de productie-site en een secundaire backup op een offline/offsite locatie.
   - Opslag
     De backup media kunnen in sommige gevallen hergebruikt worden. Hiervoor dient het betreffende medium in eerste instantie volledig “schoongemaakt” te zijn.

d. Herstel
   Het herstellen van een bepaalde situatie na een incident/calamiteit dient zorgvuldig plaats te vinden. Dit gebeurt a.d.h.v. een duidelijke procedurebeschrijving voor elke specifieke situatie/omgeving. Dergelijke procedures worden opgeleverd bij het in beheer nemen van de betreffende storagesystemen en de diverse toepassingen.

e. Backup- en restoretest
   De gemaakte backups dienen een hoge mate van betrouwbaarheid te hebben. Immers bij het terugzetten van een backup moet er van worden uitgegaan dat het herstellen van de betreffende gegevens ook daadwerkelijk mogelijk is. Hiervoor dient regelmatig, met in acht name van de BIO 12.3.1.5 minimaal eens per jaar, een backup- en restoretest uitgevoerd te worden. Van de uitgevoerde testen dient een verslag te worden opgesteld.

f. Vernietiging
   Opslagmedia die niet langer gebruikt worden zullen digitaal schoongemaakt worden (x aantal maal overschrijven of met behulp van specifieke software). Indien het opslagmedium in een end-of-life fase zit dan wordt dit vernietigd (inzet externe deskundigheid conform ISO/IEC 21964-1).

3. Controle en naleving

In lijn met het managementsysteem voor informatieveiligheid vindt rapportage plaats over de belangrijkste aspecten met betrekking tot backup en recovery van Provincie Limburg.

4. Vaststelling

Dit beleidsdocument is vastgesteld door het directie team in de DT-vergadering van dd. 4 juli 2022. Dit document wordt meegenomen in de jaarlijkse beoordeling van de beleidsdocumenten op het gebied van informatiebeveiliging.

provincie limburg

Beleid veilig mobiel werken Provincie Limburg

1. Doelstelling veilig mobiel werken Provincie Limburg

Ten behoeve van het tijd- en plaatsonafhankelijk werken[1] zijn in het kader van informatiebeveiliging een aantal beleidsuitgangspunten opgesteld. Het doel van dit beleid is te bewerkstelligen dat ook op een locatie buiten het Gouvernement op een veilige manier kan worden gewerkt, zodat de risico's in geval van geheel of gedeeltelijk verlies, of beschadiging van data en/of programmatuur en hardware tot een aanvaardbaar niveau kunnen worden beperkt.

2. Beleidsuitgangspunten veilig mobiel werken

De Provincie Limburg hanteert de volgende beleidsuitgangspunten, die ontleend zijn aan de BIO en aanvullend zijn op het algemene informatiebeveiligingsbeleid van de Provincie Limburg.

a. Veilig mobiel werken is alleen mogelijk als medewerkers bewust en bekwaam handelen. De Provincie Limburg informeert haar medewerkers over hun verantwoordelijkheid en draagt bij aan bewuster handelen door middel van trainingen.
   - Verantwoordelijkheid
     Elke medewerker is verantwoordelijk voor het veilig gebruik van de aan hem/haar beschikbaar gestelde mobiele apparatuur. De gebruiker wordt hierover geïnformeerd door middel van een bruikleenovereenkomst. Elke medewerker die gebruik maakt van apparatuur van de Provincie Limburg tekent een verklaring om deze verantwoordelijkheid ook juridisch vast te leggen. De helpdesk is verantwoordelijk voor het laten tekenen van de verklaringen. De getekende bruikleenovereenkomsten worden vastgelegd in het servicemanagementsysteem Topdesk.
   - Bewustzijn
     De Provincie Limburg helpt medewerkers bij het bewust veilig werken door middel van bewustwordingstrainingen en voorlichting. Elke nieuwe medewerker neemt verplicht deel aan het introductieprogramma, waarin o.a. veilig mobiel werken wordt toegelicht. Jaarlijks zijn er bewustwordingsactiviteiten waarin aandacht is voor veilig mobiel werken. In het kader van voorlichting wordt door het cluster Organisatie en Informatie informatie verstrekt via het intranet van de Provincie Limburg. In specifieke gevallen worden medewerkers rechtstreeks benaderd.
   - Gebruik privé-apparatuur
     Provinciale medewerkers maken zakelijk gebruik van namens en door de Provincie Limburg verstrekte apparatuur. Het is toegestaan om privé-apparatuur (BYOD) te koppelen aan het draadloze gastennetwerk van de Provincie Limburg. Ook vanuit een externe locatie kan gewerkt worden met apparatuur van derden. Via een browser wordt dan toegang gezocht tot de infrastructuur van de Provincie Limburg en kan een virtuele werkplek opgestart worden.

b. De Provincie Limburg maakt onderscheid tussen door de Provincie Limburg beheerde apparatuur en niet door de Provincie Limburg beheerde apparatuur. Alle apparatuur die door het cluster Organisatie en Informatie aan medewerkers van de Provincie Limburg wordt verstrekt voor de uitvoering van hun

[1] Binnen de Provincie Limburg wordt in dit kader gesproken over tijd- en plaatsbewust werken (TPBW).

taken wordt door het team I-Services, als onderdeel van het cluster Organisatie en Informatie beheerd. Niet door de Provincie Limburg beheerde apparatuur, zoals persoonlijke apparatuur (BYOD) of apparatuur van externen, worden gezien als onbeheerd (‘not trusted’).

- Uitgifte en inname
  De uitgifte en inname van apparatuur wordt uitgevoerd door de helpdesk van het cluster Organisatie en Informatie en vastgelegd in de CMDB. Zie ook de procedure in- en uitdiensttreding. Voor Statenleden van de Provincie Limburg is in het *Rechtspositiebesluit decentrale politieke ambtsdragers* de beschikbaarstelling van informatie- en communicatievoorzieningen opgenomen.

- Mobile Device Management (MDM)
  Alle smartphones en tablets die door de Provincie Limburg worden uitgegeven worden beheerd door middel van Mobile Device Management (MDM) software. Hiermee is het voor de Provincie Limburg mogelijk om minimale eisen te stellen aan de beveiliging van de smartphone en tablet zoals pincode, versleuteling en updates. Bij het uitblijven van updates op de smartphone of tablet wordt een e-mail gestuurd naar de gebruiker om hem/haar op de hoogte te stellen van de tekortkoming. Bij meer dan twee herinneringen heeft de Provincie Limburg de mogelijkheid om de smartphone of tablet af te sluiten van toegang tot de informatievoorziening van de Provincie Limburg .
  Provinciale smartphones en tablets zijn zo ingericht dat toegang wordt verkregen met een persoonlijke code en dat de gegevens op het apparaat worden versleuteld. Via het MDM-systeem is het mogelijk om de apparatuur op afstand te wissen.
  Voor provinciale laptops wordt geen ‘zero footprint’ gehanteerd. Hier wordt de lokale data versleuteld opgeslagen.

- Patching en hardening
  Updates/patches worden zo snel als mogelijk, met in achtname van de BIO 12.6.1.1, na de releasedatum doorgevoerd op de door de Provincie Limburg beheerde infrastructuur. Voorafgaand aan het doorvoeren van updates en patches worden deze eerst getest door het team I-Services van het cluster Organisatie en Informatie. Hardening van de apparatuur wordt uitgevoerd op basis van vastgelegde hardeningspolicies van de Provincie Limburg.

c. Digitale werkplek en applicaties
   Voor toegang tot provinciale applicaties en data kan gebruik worden gemaakt van een VPN-verbinding of een verbinding met de zgn. VDI-omgeving.
   Door gebruik te maken van de VDI-omgeving beschikt de medewerker over alle applicaties die ook binnen het Gouvernement beschikbaar zijn. Binnen de VDI-omgeving worden centrale updates door het cluster Organisatie en Informatie doorgevoerd, waardoor deze beschikbaar komen op alle virtuele werkplekken.
   Uitsluitend provinciale laptops kunnen vanaf een externe locatie via VPN een verbinding maken met het netwerk van de Provincie Limburg. Wanneer gebruik gemaakt wordt van een VPN-verbinding, zijn niet alle provinciale applicaties op de laptop beschikbaar. Wanneer een provinciale laptop verbonden is met het netwerk van de Provincie Limburg, wordt ook de software op die laptop automatisch bijgewerkt.

Zowel de VPN-toegang als de VDI-toegang vanaf een zgn. onveilige zone2 vindt plaats op basis van loginnaam, wachtwoord en een tweede factor.

d. Veilige verbindingen
De mobiele apparatuur en dan met name de provinciale laptops zijn zo uitgerust dat deze zowel gebruikt kunnen worden binnen het Gouvernement (veilige verbinding, bedraad) als vanaf een externe locatie. Vanaf een externe locatie wordt ingelogd met een extra 2e factor. Het draadloze netwerk van Provincie Limburg wordt in dit kader ook gezien als een onveilig netwerk.
Het is niet mogelijk om met een vreemd device (bijvoorbeeld een laptop die niet door Provincie Limburg wordt beheerd, BYOD) gebruik te maken van het bedrade netwerk binnen het Gouvernement.

3. Controle en naleving

In lijn met het managementsysteem voor informatieveiligheid vindt rapportage plaats over de belangrijkste aspecten van het veilig mobiel werken binnen de Provincie Limburg.

4. Vaststelling

Dit beleidsdocument is vastgesteld door het directie team in de DT-vergadering van dd. 4 juli 2022. Dit document wordt meegenomen in de jaarlijkse beoordeling van de beleidsdocumenten op het gebied van informatiebeveiliging.

[2] Alleen het bekabelde netwerk binnen het gouvernement wordt gezien als veilige zone, Overige netwerken worden als onveilig beschouwd.

provincie limburg

Beleid logging Provincie Limburg

1. Logging

In de ICT wordt een log gebruikt om gebeurtenissen van een bepaald proces of systeem bij te houden, ook wel loggen genoemd. Logs worden onder andere gebruikt om gebeurtenissen die belangrijk zijn voor de beveiliging, beheer of voor de analyse van verstoringen in een (log)bestand vast te leggen. Logs kunnen ook in een database of het hoofdgeheugen bewaard worden.
Het registreren van het systeemgebruik heeft tot doel om inzicht te verkrijgen in de werking en het gebruik van informatiesystemen ten behoeve van o.a. :

- capaciteitsbeheer;
- het vinden van de oorzaak van een foutieve werking van het systeem (debugging);
- incidentbeheer, onderzoek na een security incident;
- het onweerlegbaar aantonen van een (bepaalde) activiteit;
- het controleren van menselijk handelen ingeval van bedienfouten of misbruik.

2. Doelstelling logging Provincie Limburg

Ten behoeve van de beveiliging van informatie is een logging-beleid opgesteld voor alle provinciale ICT-voorzieningen. Het doel van dit beleid is duidelijke regels neer te leggen die in relatie tot logging genomen moeten worden binnen de Provincie Limburg.

3. Beleidsuitgangspunten logging

De Provincie Limburg hanteert de volgende beleidsuitgangspunten welke zijn ontleend aan de BIO en aanvullend zijn op het algemene informatiebeveiligingsbeleid van de Provincie Limburg.

Systeemactiviteiten van gebruikers, beheerders, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode, met inachtname van de BIO 9.4.4.2, te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.

a. Van logbestanden worden rapportages gemaakt die periodiek, minimaal maandelijks, worden beoordeeld.
b. Er is vastgelegd welke persoon en/of rol verantwoordelijk is voor deze beoordeling.
c. Een logregel bevat minimaal:
    - Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID
    - Informatie herleidbaar tot de gebeurtenis
    - Waar mogelijk de identiteit van het werkstation of de locatie
    - Host naam
    - Operating System (OS)
    - Naam van de toepassing
    - IP-adres(sen)
    - Locatie(s)
    - Het object waarop de handeling werd uitgevoerd

- Het resultaat van de handeling
- De datum en het tijdstip van de gebeurtenis

d. In een logregel worden in geen geval gevoelige gegevens opgenomen, zoals gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, et cetera). In de logregel mogen ook geen persoonsgegevens worden opgenomen uit systemen van de Provincie Limburg zelf (dus wel gebruikersnamen of inlog accounts).
e. Logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren bij voorkeur aangesloten op een Security Information and Event Management systeem (SIEM) danwel geschikt om op een later moment aan te sluiten op een SIEM. Met een SIEM worden (gecorreleerde) meldingen en alarmoproepen aan de beheerorganisatie gegeven. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.
f. Controle op opslag van logging: het vol lopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt ook gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijvoorbeeld een logserver die niet bereikbaar is).
g. Alle ongeautoriseerde toegangspogingen zijn beveiligingsincidenten en vereisen directe opvolging door melding aan en registratie door de helpdesk.

4. Controle van het beleid op systeemgebruik

Er zijn binnen de Provincie Limburg procedures vastgesteld om het voor komen van bepaalde gebeurtenissen i.r.t. het gebruik van ICT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld met inachtname van de BIO 12.4.3. Zoveel als mogelijk wordt systeemgebruik automatisch gelogd, als dit niet mogelijk is kan ook gebruik gemaakt worden van een logboek voor bijvoorbeeld beheerders.

De volgende gebeurtenissen worden in ieder geval opgenomen in de logs:

a. Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instellingen: uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore.
b. Gebruik van functies voor functioneel beheer, zoals het wijzigingen van configuraties en instellingen, release van nieuwe functionaliteiten, ingrepen in gegevenssets (waaronder databases).
c. Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren van gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels.
d. 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).
e. Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens het uitvoeren van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of -systemen).
f. Handelingen van gebruikers, zoals geslaagde en mislukte inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders.
g. Online transacties. Hierbij wordt minimaal gelogd:

- het bericht-ID;
- datum en tijd;
- aanroepend en verzendend systeem en -proces.

5. Bescherming van informatie in logbestanden

Logbestanden dienen te worden beschermd tegen modificatie, inzien door onbevoegden en verwijdering. De volgende beleidsregels zijn hierop van toepassing:

a. Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.
b. Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.
c. Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
d. Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
e. De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten worden zal daarbij altijd het ‘vier ogen’ principe toegepast worden.
f. De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met inachtname van de BIO 9.4.4.2 en conform de wensen van de systeemeigenaar. Bij een (vermoedelijk) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.
g. Het goed functioneren van de logging wordt continu gemonitord voor essentiële systemen.
h. Controle op opslag van de logs: het vollopen 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 (bijvoorbeeld: een logserver die niet bereikbaar is).

6. Synchronisatie van systeemklokken

De klokken van alle relevante informatiesystemen van de Provincie Limburg behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

a. Systeemklokken worden zodanig gesynchroniseerd dat altijd een betrouwbare analyse van logbestanden mogelijk is.

7. Controle en naleving

In lijn met het managementsysteem voor informatieveiligheid vindt rapportage plaats over de belangrijkste aspecten met betrekking tot de logging bij Provincie Limburg.

8. Vaststelling

Dit beleidsdocument is vastgesteld door het directie team in de DT vergadering van dd. 4 juli 2022. Dit document wordt meegenomen in de jaarlijkse beoordeling van de beleidsdocumenten op het gebied van informatiebeveiliging.

provincie limburg

Beleid informatietransport Provincie Limburg

1. Doel beleid informatietransport Provincie Limburg

Ten behoeve van het digitaal uitwisselen van informatie zijn in het kader van informatiebeveiliging een aantal beleidsuitgangspunten opgesteld. Het doel van dit beleid is te bewerkstelligen dat gegevens op een betrouwbare wijze kunnen worden uitgewisseld, zodat de risico's in geval van geheel of gedeeltelijk verlies, of beschadiging van data tot een aanvaardbaar niveau kunnen worden beperkt.

Informatietransport in dit kader heeft betrekking op het uitwisselen van gegevens tussen personen en tussen systemen. In andere gevallen gaat het om de gegevensuitwisseling tussen een persoon en een systeem en vice versa. Dit valt onder de invoer en uitvoer van een bepaald systeem.

2. Beleidsuitgangspunten informatietransport

De Provincie Limburg hanteert de volgende beleidsuitgangspunten en deze zijn ontleend aan de BIO en aanvullend zijn op het algemene informatiebeveiligingsbeleid van de Provincie Limburg.

a. Informatie-uitwisseling tussen personen
   Bij de informatie-uitwisseling tussen personen dient men rekening te houden met de aard van de gegevens die men gaat uitwisselen. Indien dit bijvoorbeeld persoonsgegevens betreft dan zal de AVG van toepassing zijn en zal gebruik moeten worden gemaakt van veilige communicatiemogelijkheden. Ook voor overige vertrouwelijke gegevens dienen maatregelen getroffen te worden, die de communicatie op een veilige manier mogelijk maakt.
   Hieronder worden een aantal producten genoemd die gebruikt worden bij het uitwisselen van informatie.

   - Email in combinatie met veilige e-mail
     Het gebruik van email wordt ondersteund middels de standaarden die verplicht zijn gesteld door het forum voor standaardisatie. Hiermee is het gebruik van de reguliere email een manier om relatief veilige te communiceren.
     Indien het vertrouwelijke informatie betreft, waaronder persoonsgegevens, dan dient gebruik gemaakt te worden van veilige e-mail. Hierbij is sprake versleuteling van het bericht en de bijlagen tot het moment dat de (geauthentiseerde) ontvanger deze opent.
     Het is niet toegestaan om privé-emailvoorzieningen te gebruiken met betrekking tot zakelijke communicatie en toepassingen.

   - Filetransfer via de transfersite of als bijlage bij veilige e-mail
     Het gebruik van de filetransfersite is bedoeld voor het uitwisselen van met name grote bestanden. Bij het gebruik van de transfersite dient, indien nodig, zelf zorggedragen te worden voor een bepaalde vorm van versleuteling.
     Grote bestanden die vertrouwelijke en mogelijk persoonsgegevens bevatten, dienen via veilige e-mail uitgewisseld te worden.

- Samenwerkomgeving
    - SharePoint
      SharePoint als toepassing zoals deze binnen Provincie Limburg wordt gebruikt, bestaat uit het product SharePoint van Microsoft in combinatie met een specifieke inrichting t.b.v. de Provincie Limburg. Deze toepassing wordt gebruikt door medewerkers van Provincie Limburg voor opslaan, archivering en samenwerken aan dossiers en documenten.
    - Webex
      Wordt gebruikt als online vergadertool. Informatie wordt hier uitgewisseld tussen personen in de vorm van gesproken tekst en gedeelde informatie via het scherm.
    - Teams
      Wordt gebruikt als online vergadertool. Informatie wordt hier uitgewisseld tussen personen in de vorm van gesproken tekst en gedeelde informatie via het scherm.
    - Pleio
      Betreft een samenwerkomgeving die door de Overheid en Provincies (samenwerkomgeving provincies BIJ12/GBO) wordt ondersteund. Na aanmelding kan hier in principe iedereen aan deelnemen. Binnen Pleio kunnen specifieke groepen worden gecreëerd die enkel toegankelijk zijn voor geautoriseerde personen.
    - Overige samenwerkomgevingen
      Daarnaast zijn er nog andere samenwerkomgevingen, online vergadertools en transfersites die aangeboden worden als “gratis” dienst of in een bepaalde abonnementsvorm. Het gebruik hiervan wordt ten zeerste ontraden. Indien dit onvermijdelijk is in verband met de samenwerking met derden, dan dient men er rekening mee te houden dat de gedeelde informatie mogelijk ook voor onbekenden toegankelijk is.
- Social media
  Voor het gebruik van social media wordt ook verwezen naar het personeelshandboek.
    - Whatsapp
      Is een veel gebruik platform om snel korte berichtjes uit te wisselen. Dit mag niet gebruikt worden voor zakelijke informatie-uitwisseling.
    - Signal
      Dit is vergelijkbaar met Whatsapp waarbij dit product wel een meer afgesloten karakter heeft. Echter ook hier geldt dat dit niet gebruikt mag worden voor zakelijke communicatie.
    - Overige social media kanalen
      Het gebruik hiervan in een zakelijke omgeving dient vermeden te worden. De Provincie Limburg gebruikt sociale kanalen voor het doen van communicatie uitingen. Dit betreft in alle gevallen openbare informatie, die ook via andere bronnen beschikbaar is.

b. Informatie-uitwisseling tussen systemen

- Enterprise Service Bus (ESB)
  Voor de informatie-uitwisseling tussen systemen wordt gebuikt gemaakt de zgn. Enterprise Service Bus (ESB). Deze wijze van communiceren maakt het mogelijk dat de communicatie veilig en gestructureerd voor de betreffende applicaties verloopt. Binnen de Provincie Limburg wordt standaard deze wijze van communiceren tussen applicaties ingezet (architectuurprincipe).

3. Controle en naleving

In lijn met het managementsysteem voor informatieveiligheid vindt rapportage plaats over de belangrijkste aspecten van informatietransport binnen de provincie.

4. Vaststelling

Dit beleidsdocument is vastgesteld door het directie team in de DT vergadering van dd. 4 juli 2022. Dit document wordt meegenomen in de jaarlijkse beoordeling van de beleidsdocumenten op het gebied van informatiebeveiliging.

provincie limburg

Beleid cryptografie Provincie Limburg

1. Doelstelling cryptografie Provincie Limburg

Ten behoeve van bescherming van gegevens wordt gebruik gemaakt van cryptografie (versleuteling van gegevens). Encryptie (versleuteling) zorgt ervoor dat derden gegevens niet kunnen lezen. Encryptie wordt gebruikt om:

- gegevens veilig uit te wisselen over een onveilig communicatiekanaal;
- de identiteit van de verzender te verifiëren (zoals digitale handtekeningen);
- gegevens veilig op te slaan;
- gegevens te vernietigen (crypto-schredding).

Naast encryptie is hashing (formeel geen encryptie) ook een cryptografische toepassing. Hashing wordt bijvoorbeeld toegepast bij de opslag van wachtwoorden, omdat dan niet het oorspronkelijke wachtwoord hoeft te worden opgeslagen, maar alleen de uitkomst van een juist ingevoerd wachtwoord. Hashing kan gebruikt worden om:

- de integriteit van gegevens te controleren;
- gegevens te controleren zonder de inhoud te kennen (zoals wachtwoordcontrole).

In het kader van het gebruik van cryptografie zijn een aantal beleidsuitgangspunten opgesteld. Het doel van dit beleid is te voorkomen dat gegevens zondermeer gebruikt kunnen worden door derden, zodat de risico's op het lekken, vervreemden en manipuleren van gegevens tot een aanvaardbaar niveau kan worden beperkt.

2. Beleidsuitgangspunten cryptografie

De Provincie Limburg hanteert voor het toepassen van cryptografie de volgende beleidsuitgangspunten, welke zijn ontleend aan de BIO en aanvullend zijn op het algemene informatiebeveiligingsbeleid van de Provincie Limburg:

a. Versleuteling van gegevens wordt steeds goedkoper en is steeds sneller te verwerken. Het versleutelen van gevoelige data heeft de voorkeur op niet versleutelen.
b. De provincie hanteert best practices op het gebied van encryptie zoals de standaarden op de pas-toe-of-leg-uit lijst en lijst open standaarden van het Forum Standaardisatie en de richtlijnen van Internet.nl en het NCSC.
c. De Provincie Limburg gebruikt alleen versleutelingen die de status "voldoende" en "goed" hebben, zoals aangegeven door het NCSC.
d. De door Provincie Limburg verstrekte middelen zoals laptop, smartphone en tablet zijn voorzien van encryptietechnieken. Medewerkers hoeven hier zelf niets op in te stellen. Datzelfde geldt voor o.a. de versleuteling van e-mail, WiFi, wachtwoorden e.d.
e. Voor de versleuteling van gegevens op middelen die medewerkers op eigen initiatief gebruiken (BYOD) is de medewerker zelf verantwoordelijk. Onder deze middelen vallen bijvoorbeeld eigen tablets, smartphones, laptops, usb-sticks e.d. Het gebruik van deze middelen voor de opslag van zakelijke informatie wordt daarom ten zeerste afgeraden.

3. Toepassing van cryptografie

De Provincie Limburg hanteert cryptografie als onderdeel van de standaarddiensten die door het cluster Organisatie en Informatie worden geboden. Het gaat bij deze standaarddiensten om zowel de opslag van data op onder meer mobiele devices als om de beveiliging van communicatie tussen systemen. Hieronder volgt een opsomming van de organisatiebrede toepassing van cryptografie.

3.1. E-mail

E-mail kan vertrouwelijke informatie bevatten. Daarnaast wil de Provincie Limburg ook de afkomst van e-mail garanderen. Belangrijk hierbij is dat, naast de afzender, ook de ontvanger de juiste beveiliging moet hanteren om echt effectief veilig te kunnen mailen.
Het verkeer tussen de mailserver en de mobiele apparaten wordt versleuteld middels TLS-encryptie op basis van veilige ciphers die regelmatig getoetst worden aan de geldende NCSC-richtlijnen.
Voor het mailen van vertrouwelijke en persoonsgegevens dient gebruik gemaakt te worden van een toepassing voor veilige e-mail. Hierbij wordt de e-mail inclusief de bijlage versleuteld en aangeboden aan de ontvanger. Deze kan de e-mail pas openen nadat hij/zij zich heeft geïdentificeerd.
Met de Belastingdienst en de Dienst Koninklijk Huis zijn specifieke afspraken gemaakt over de emailuitwisseling. Voor deze domeinen kan alleen e-mailuitwisseling plaatsvinden op basis van verplicht TLS-verkeer tussen de mailservers.
De maatregelen m.b.t. de betreffende e-mail standaarden (SPF, DKIM, DMARC, STARTTLS en DANE) gelden voor elk domein waar de Provincie Limburg eigenaar van is en vanaf waar e-mail verzonden kan worden. Voor domeinen waarvan geen e-mail van verzonden mag worden, worden de SPF-records en DMARC zo ingesteld dat de DMARC-instelling op ‘reject’ staat.

3.2. Draadloos Netwerk

Voor het draadloze netwerk van de Provincie Limburg wordt gebruik gemaakt van encryptie via WPA2 Enterprise. Het wachtwoord voor interne medewerkers is, bij uitgifte, ingesteld op de provinciale apparatuur.
Medewerkers met eigen apparatuur (BYOD) en externe gasten van instellingen die aangesloten zijn bij de Stichting GovRoam, kunnen GovRoam gebruiken voor draadloze toegang tot internet. Hiermee kunnen zgn. “not trusted devices” worden gekoppeld aan het draadloze netwerk van Provincie Limburg, waarmee deze enkel toegang krijgen tot internet. De betreffende personen dienen gebruik te maken van de inloggegevens van de eigen organisatie (GovRoam).
Externe gasten van instellingen die niet aangesloten zijn bij de Stichting GovRoam kunnen gebruik maken van een door Provincie Limburg verstrekt wachtwoord (GovGuest) om draadloze toegang te krijgen tot internet.

3.3. Internetverkeer

Alle extern beschikbare websites van de Provincie Limburg zijn voorzien van een PKI-certificaat en hierdoor beschikbaar via het HTTPS-protocol. Certificaten gelden voor zowel het root domein (zonder www) als voor het domein met www. Indien gebruik wordt gemaakt van specifieke hosts, zal dit een certificaat op hostnaam zijn. Alleen voor het voor het provinciale domein 'prvlimburg.nl’ zijn zgn. wildcard-certificaten beschikbaar. Deze worden met name gebruikt voor interne omgevingen.

De externe DNS-omgeving is voorzien van DNSSEC, waarbij het key management gedeelte in beheer is binnen het team I-Services van het cluster Organisatie en Informatie.

3.4. VPN

Medewerkers hebben de mogelijkheid om van buiten locaties van de Provincie Limburg verbinding te maken met het interne netwerk van de provincie. Medewerkers zetten daarvoor een beveiligde verbinding op door middel van VPN (Virtual Private Network).
Het VPN-verkeer van laptops wordt ontsloten middels TLS-encryptie, op basis van veilige ciphers die getoetst worden aan de geldende NCSC-richtlijnen.

3.5. Uitwisseling van bestanden

Het veilig uitwisselen van bestanden vindt bij voorkeur plaats via de voorziening voor veilige email in combinatie met “attachements”. Bij het gebruik van andere mogelijkheden zoals de eigen transfersite of producten van derden dient zelf zorg gedragen te worden voor een passend niveau van versleuteling.

3.6. Mobiele apparatuur

Opslag van gegevens op door de Provincie Limburg beheerde mobiele apparatuur (laptop, tablet en smartphone) wordt standaard versleuteld met de in het besturingssysteem aanwezige versleutelmethode.

3.7. Opslag op fileservers

Interne data op de fileservers is in de meeste gevallen niet versleuteld.

3.8. Beheer

Voor het automatiseren van beheertaken worden powershellscripts gebruikt. De cliënts staan alleen powershell script toe die ondertekend zijn door een geldig provinciaal certificaat. In alle ander gevallen wordt dit geblokkeerd door de endpoint protectie.

3.9. Elektronische handtekeningen

Voor elektronische handtekeningen met hoge betrouwbaarheidseisen wordt binnen de Provincie Limburg gebruik gemaakt van een standaardoplossing. Voor gekwalificeerde handtekeningen moet de oplossing voldoen aan de vereisten van de wet voor zowel AES (Advanced Electronic Signatures) als QES (Qualified Electronic Signatures) handtekeningen.

3.10. PKI certificaten/sleutels

De aanvraag van overheids- en public signed certificaten verloopt via de beheerportalen van de leveranciers. Het aanvragen van certificaten bij externe partijen en het uitgeven van interne certificaten wordt uitgevoerd door het cluster Organisatie en Informatie.
Voor private signed certificaten wordt gebruik gemaakt van een eigen PKI-omgeving. Deze is in beheer bij het team I-Services van het cluster Organisatie en Informatie.
Van alle websites en domeinen waar een certificaat van toepassing is, vindt binnen het team I-Services een automatische controle op de geldigheidsduur plaats.

Provincie Limburg is voor de public signed certificaten niet gebonden aan één leverancier. Als een leverancier niet meer de gewenste dienstverlening kan leveren (bijvoorbeeld bij faillissement of compromitering), dan wordt er op dat moment een andere leverancier geselecteerd en ingezet.

4. Controle en naleving

In lijn met het managementsysteem voor informatieveiligheid vindt rapportage plaats over de belangrijkste aspecten van cryptografie binnen de provincie.

5. Vaststelling

Dit beleidsdocument is vastgesteld door het directie team in de DT vergadering van dd. 4 juli 2022. Dit document wordt meegenomen in de jaarlijkse beoordeling van de beleidsdocumenten op het gebied van informatiebeveiliging