1 Goedkeuring informatiebeveiligingsbeleid en distributie

De directie behoort een beleidsdocument voor informatiebeveiliging goed te keuren, te publiceren en kenbaar te maken aan alle werknemers en relevante externe partijen.

2 Inleiding

2.1 Toelichting

Dit document beschrijft het beleid van Hecla Professional ("Hecla") met betrekking tot de beveiliging van informatie. De informatievoorziening is van essentieel belang voor de continuïteit van de bedrijfsvoering van de Hecla en haar klanten. Zowel op papier als geautomatiseerd zijn Hecla en haar klanten, bij het dagelijks werk afhankelijk van de beschikbaarheid van betrouwbare informatie. Hecla en haar informatievoorziening worden blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's tot een aanvaardbaar niveau te reduceren. Het proces van informatiebeveiliging begint met het definiëren van een beleid op dit punt. Dit beleid is vastgelegd in dit document, en vastgesteld door de directie.

2.2 Definitie van informatiebeveiliging

Informatiebeveiliging wordt als volgt gedefinieerd:
Het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen.

Informatiebeveiliging omvat een samenhangend stelsel van maatregelen. Dit betekent dat de verschillende maatregelen die samen de informatiebeveiliging vormen, niet los van elkaar worden getroffen, maar in onderlinge relatie met elkaar staan.

Het stelsel van beveiligingsmaatregelen heeft tot doel een *blijvend niveau van beveiliging* te realiseren. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn wordt gehandhaafd.

Informatiebeveiliging is gericht op het realiseren van een *optimaal niveau van beveiliging.*
Dit optimum wordt bereikt door een zorgvuldige afweging van kosten en baten.

2.3 Samenhang tussen informatiebeveiliging en privacybescherming

Bescherming van privacy richt zich op de zorgvuldige omgang met persoonsgegevens. Dit kunnen bijvoorbeeld gegevens van klanten of van medewerkers zijn. Informatiebeveiliging richt zich op de beveiliging van vertrouwelijke gegevens, waaronder persoonsgegevens. De maatregelen die in het kader van informatiebeveiliging worden getroffen, leveren dus een bijdrage aan de bescherming van privacygevoelige gegevens. Binnen Hecla is de Security Officer verantwoordelijk voor de coördinatie van alle activiteiten die betrekking hebben op informatiebeveiliging.

2.4 Samenhang tussen informatiebeveiliging en risicomanagement

Risicomanagement richt zich op het analyseren en beheersen van risico's waaraan Hecla en haar klanten bloot worden gesteld. Deze risico's kunnen betrekking hebben op velerlei terreinen, zoals financiële risico's en de beschikbaarheid en inzet van personeel. Informatiebeveiliging heeft betrekking op de risico's die samenhangen met de informatievoorziening en de omgang met vertrouwelijke informatie. De coördinatie van risicomanagement is de verantwoordelijkheid van de Security Officer van Hecla.

2.5 Doelstelling informatiebeveiligingsbeleid

Het opstellen van het informatiebeveiligingsbeleid heeft tot doel de doelstellingen en uitgangspunten m.b.t. informatiebeveiliging binnen Hecla vast te stellen en vast te leggen. Hiermee vormt het beleid de leidraad voor alle betrokkenen bij informatiebeveiliging binnen Hecla. De directie acht de doelstellingen, uitgangspunten en uitvoering van het informatiebeveiligingsbeleid een kritische succesfactor voor de continuïteit van Hecla.

2.6 Doelstelling informatiebeveiliging

Zoals in de voorgaande definitie (2.2) is verwoord, richt informatiebeveiliging zich op de volgende drie aspecten van de informatievoorziening:

- *beschikbaarheid*, de informatie moet op de gewenste momenten beschikbaar zijn;
- *integriteit*, de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
- *vertrouwelijkheid*, de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is.

Informatiebeveiliging heeft tot doel het optreden van bedreigingen die bovenstaande aspecten van de informatievoorziening kunnen schaden, te voorkomen en/of te beperken. Bedreigingen zijn er in vele vormen. Deze kunnen fysiek van aard zijn, zoals brand en wateroverlast of technisch, bijvoorbeeld in de vorm van storingen in programmatuur, apparatuur of de stroomvoorziening. Ook de mens vormt een bedreiging door onopzettelijk fouten en vergissingen te maken die de informatievoorziening verstoren of door opzettelijke kwaadaardige daden, zoals hacking, phishing, computervirussen, computerfraude, etc. De ervaring leert dat bedreigingen op dit terrein steeds vaker voorkomen en ook steeds geraffineerder van aard worden.

2.7 Werkingsgebied

Het informatiebeveiligingsbeleid is van toepassing op de hele Hecla organisatie. Het informatiebeveiligingsbeleid is ook van toepassing op de gegevensuitwisseling van Hecla met andere organisaties. Het beleid richt zich op onze eigen medewerkers, tijdelijk personeel, vrijwilligers en op personeel dat door derden wordt ingezet om diensten te verlenen aan onze organisatie.

2.8 Verantwoordelijkheid informatiebeveiligingsbeleid

De directie is eindverantwoordelijk voor het informatiebeveiligingsbeleid en heeft dit beleid op vastgesteld door middel van dit document.
De Security Officer is verantwoordelijk voor het onderhoud van het informatiebeveiligings-beleid.

2.9 Communicatie van het informatiebeveiligingsbeleid

Het is van groot belang dat het informatiebeveiligingsbeleid en de hieruit volgende principes en richtlijnen bekend zijn bij alle betrokkenen binnen Hecla. De Security Officer is verantwoordelijk voor de communicatie van het beleid. Het bevorderen van het beveiligingsbewustzijn bij management en medewerkers vormt een belangrijk aandachtspunt bij deze communicatie.

2.10 Inhoud informatiebeveiligingsbeleid

In hoofdstuk 3 zijn de uitgangspunten vastgelegd die worden gehanteerd bij de toepassing van informatiebeveiliging binnen Hecla. In hoofdstuk 4 wordt aandacht besteed aan het managementsysteem voor informatiebeveiliging. Hoofdstuk 5 beschrijft de organisatie van informatiebeveiliging bij Hecla. Hoofdstuk 6 beschrijft het Hecla informatiebeveiligingsbeleid op diverse specifieke punten.

3 Uitgangspunten informatiebeveiliging

Bij de toepassing van informatiebeveiliging binnen Hecla worden de volgende uitgangspunten gehanteerd:

1. Hecla streeft ernaar aantoonbaar te voldoen aan de norm ISO 27001 voor Informatiebeveiliging.
2. Hecla voldoet aan alle, van toepassing zijnde, wet- en regelgeving. In dit verband wordt genoemd:
   - Grondwet
   - Algemene Verordening Gegevensbescherming (AVG)
   - Auteurswet
   - Telecommunicatiewet (incl. cookiewetgeving)
   - Wet computercriminaliteit III
   - Europese Verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt EU/910/2014 (eIDAS-Verordening)
3. Informatiebeveiliging is binnen Hecla zo ingericht dat de rechten van betrokkenen (klanten van Hecla, medewerkers, bezoekers, leveranciers) die voortvloeien uit de AVG, worden gerespecteerd en kunnen worden geëffectueerd.
4. Beveiliging van informatie is een onderdeel van de integrale management-verantwoordelijkheid. Alle

onderdelen van Hecla hebben hiertoe verantwoordelijkheden voor informatiebeveiliging toegewezen en vastgelegd.

5. Wanneer Hecla samenwerkingsverbanden aangaat met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatievoorziening, wordt nadrukkelijk aandacht besteed aan informatiebeveiliging. Afspraken hierover worden schriftelijk vastgelegd en op de naleving hiervan wordt toegezien.
6. Bedrijfsmiddelen zijn volgens een gestructureerde methode geclassificeerd naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.
7. Bij de aanname, tijdens het dienstverband en in geval van ontslag van medewerkers wordt nadrukkelijk aandacht besteed aan de betrouwbaarheid van medewerkers en aan de waarborging van de vertrouwelijkheid van informatie.
8. Hecla voert een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren. Hiertoe voert de Security Officer periodiek bewustwordingscampagnes uit. Hecla biedt hiervoor de communicatiemiddelen aan.
9. Hecla beschikt over gedragsregels voor het gebruik van (algemene) informatievoorzieningen. Op de naleving van deze gedragsregels wordt toegezien.
10. Bij overtreding van de regelgeving voor informatiebeveiliging zal de directie disciplinaire maatregelen treffen.
11. Hecla heeft maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.
12. Hecla heeft maatregelen getroffen voor de beveiliging en het beheer van de operationele informatie- en communicatievoorzieningen. Maatregelen tegen allerlei vormen van kwaadaardige programmatuur (computervirussen, spam, spyware, phishing, etc.) vormen hierin een belangrijk onderdeel.
13. Hecla en haar medewerkers treffen maatregelen om te voorkomen, dat vertrouwelijke informatie in handen van derden terechtkomt.
14. Geautoriseerde medewerkers moeten ook op afstand een beveiligde toegang hebben tot de voor hun relevante productie omgevingen. Er worden geen vertrouwelijke gegevens buiten de productieomgeving opgeslagen. Onder condities kan hiervan afgeweken worden.
15. Productie omgevingen zijn gescheiden van andere omgevingen en hierin kunnen specifiek toegangsrechten worden verleend en is monitoring van de toegang mogelijk.
16. Bij de ontwikkeling en aanschaf van informatiesystemen besteden opdrachtgevers, projectleiders, ontwikkelaars en beheerders in alle fasen van het aanschaf- of ontwikkelingsproces nadrukkelijk aandacht aan informatiebeveiliging en dragen zij zorg voor de realisatie van de gestelde beveiligingseisen. Hecla heeft adequate maatregelen getroffen, waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) is gewaarborgd. Het beheren van een continuïteitsplan, het inrichten van een crisisorganisatie en het oefenen van de getroffen maatregelen vormen hiervan een onderdeel.
17. Als onderdeel van het managementsysteem voor informatiebeveiliging wordt binnen Hecla door interne en externe partijen toegezien op de naleving van het informatie- beveiligingsbeleid.
18. Hecla beschikt over middelen voor het melden en afhandelen van beveiligingsincidenten. De evaluatie van de afhandeling van beveiligingsincidenten wordt benut voor de verbetering van informatiebeveiliging.

4 Managementsysteem voor informatiebeveiliging

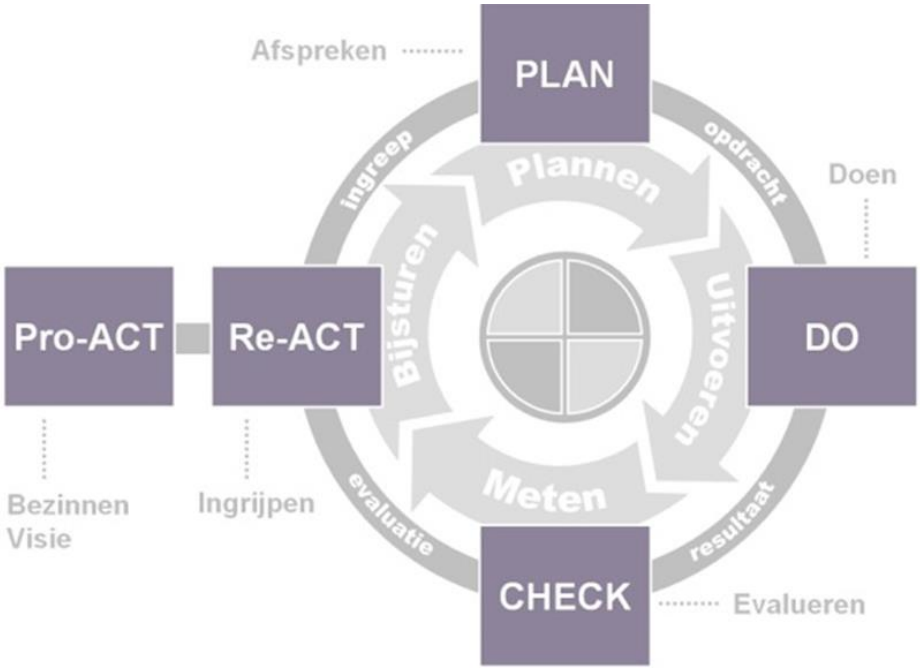
Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, na het optreden van een omvangrijk informatiebeveiligingsincident of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.

Het informatiebeveiligingsbeleid wordt iedere 2 jaar opnieuw beoordeeld en bijgewerkt indien noodzakelijk.

4.1 Overzicht managementsysteem informatiebeveiliging

Het managementsysteem voor informatiebeveiliging maakt onderdeel uit van het managementsysteem van Hecla waarin het werken volgens ISO 9001, ISO 14001, ISO 27001 en VCA is opgenomen.

Vanuit de High Level Structure van ISO is de basis van dit managementsysteem de Deming cirkel:



Plan : Beleidsvorming en Risicoanalyse
Do : Planvorming en Implementatie
Check : Monitoring, evaluatie en controle
Act : Het verbeterproces

In het document 1.0 Algemeen (hoofdstuk 4) is omschreven hoe deze Demming cirkel is geïmplementeerd bij Hecla. Informatiebeveiliging maakt integraal onderdeel uit van dit managementsysteem. Zodoende is informatiebeveiliging een continu en cyclisch proces.

5 Organisatie van de informatiebeveiliging

5.1 Directie

De directie ondersteunt informatiebeveiliging binnen Hecla actief door duidelijk richting te geven, betrokken te zijn en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.

De directie heeft de volgende taken m.b.t. informatiebeveiliging:

- De directie formuleert informatiebeveiligingsdoelstellingen;
- Het is de verantwoordelijkheid van de directie om het informatiebeveiligingsbeleid te formuleren, te beoordelen en goed te keuren;
- De directie moet zorgen voor de middelen die nodig zijn voor informatiebeveiliging;
- De directie moet plannen en programma's initiëren om het informatiebeveiligingsbewustzijn op een voldoende peil te krijgen en te houden;
- De directie moet rollen en verantwoordelijkheden voor de informatiebeveiliging in toekennen en benoemt een Security Officer;
- De directie controleert of het informatiebeveiligingsbeleid en de hieruit voortvloeiende richtlijnen en procedures worden nageleefd binnen Hecla. De Security Officer voorziet de directie van de juiste informatie om haar controlerende taak uit te kunnen oefenen.

5.2 Overleg informatiebeveiliging

De verantwoordelijke binnen de directie van Hecla en de Security Officer overleggen regelmatig bilateraal over informatiebeveiliging. In dit overleg wordt aandacht besteed aan (voortgangs-) rapportages, voorstellen voor wijzigingen van het informatiebeleid, investeringsvoorstellen voor beveiligingsmaatregelen, etc. Dit overleg wordt ieder kwartaal gehouden en vaker indien hier aanleiding voor is.

5.3 Security Officer

De Security Officer is de spin in het web m.b.t. informatiebeveiliging binnen Hecla. De Security Officer heeft de volgende taken:

- Voorbereiden van de beleidsvorming m.b.t. informatiebeveiliging;
- Coördineren van de implementatie van beveiligingsmaatregelen;
- Monitoring en controle van informatiebeveiligingsmaatregelen binnen Hecla;
- Signaleren van tekortkomingen in de naleving van het informatiebeveiligingsbeleid;
- Voorlichten en stimuleren van het beveiligingsbewustzijn bij alle betrokkenen;
- Evaluatie en advies, het adviseren van de directie over informatiebeveiliging;
- Opstellen en coördineren van een verbeterplan m.b.t. informatiebeveiliging
- Coördineren van de implementatie van beveiligingsmaatregelen
- Centraal registreren van ICT-beveiligingsincidenten
- Analyseren en beoordelen van ICT-beveiligingsincidenten
- Centraal informeren van gebruikers over (potentiële) ICT-beveiligings-incidenten;
- Coördineren van de uitvoering van preventieve en herstelacties.

De Security Officer rapporteert aan de directie.

5.4 Privacy Officer

De Privacy Officer is de spin in het web m.b.t. de bescherming van persoonsgegevens binnen Hecla. De Privacy Officer heeft de volgende taken:

- Voorbereiden van de beleidsvorming m.b.t. bescherming van persoonsgegevens en de verwerking van persoonsgegevens;
- Coördineren van de implementatie van beveiligingsmaatregelen;
- Monitoring en controle van maatregelen ten behoeve van de bescherming van persoonsgegevens binnen Hecla;
- Signaleren van tekortkomingen in de naleving van het privacybeleid;
- Voorlichten en stimuleren van het privacy bewustzijn bij alle betrokkenen;
- Evaluatie en advies, het adviseren van de directie over privacy;
- Opstellen en coördineren van een verbeterplan m.b.t. privacybescherming;
- Coördineren van de implementatie van maatregelen op het gebied van privacy by design;
- Bijhouden van het verwerkingsregister conform art. 32 AVG;
- Intermediair richting de Autoriteit Persoonsgegevens;
- Klachten afhandelen over het gebruik van persoonsgegevens met betrokkenen.

De Privacy Officer rapporteert aan de directie.

5.5 Eigenaarschap

Aan ieder informatiesysteem en gegevensverzameling wordt in het register van gegevensverwerkingen een eigenaar toegewezen. Deze eigenaar ziet toe op naleving van beveiligingsrichtlijnen en -procedures voor het betreffende systeem en/of gegevens.
De verschillende eigenaren maken samen met de Security Officer afspraken over de uitvoering van de (beveiligings-) taken en leggen deze desgewenst vast in dienstverleningsovereenkomsten (SLA's).

5.6 Goedkeuringsproces voor middelen voor de informatievoorziening

De directie stelt voldoende middelen ter beschikking om de planning van de informatiebeveiliging te kunnen uitvoeren. De geringe omvang van Hecla maakt dat er geen formele goedkeuringsprocedures benodigd zijn.

5.7 Geheimhoudingsovereenkomst

Eisen voor vertrouwelijkheid die door Hecla worden gesteld aan de beveiliging van informatie horen in een geheimhoudingsovereenkomst te worden vastgesteld. Bij personeelsleden met een dienstbetrekking is geheimhouding onderdeel van de arbeidsovereenkomst (het geheimhoudingsbeding). Bij overige personeelsleden, externen en leveranciers wordt dit vastgelegd als onderdeel van de dienstverleningsovereenkomst of in een separate overeenkomst.

5.8 Contact met overheidsinstanties

Hecla heeft in de procedure datalekken vastgelegd wanneer contact gezocht wordt met de Autoriteit Persoonsgegevens inzake een meldingsplichtig datalek.

5.9 Contact met speciale belangengroepen

Informatiebeveiliging is een belangrijk kennisdomein voor Hecla. Kennis wordt ingewonnen via:

- de Security Officer van de managed hosting providers;
- contacten en trainingen van product- en dienstenleveranciers;
- het Nationaal Cyber Security Centrum.

5.10 Onafhankelijke beoordeling van informatiebeveiliging

De informatiebeveiliging wordt jaarlijkse door een interne en externe auditor beoordeeld t.b.v. de ISO 27001 certificering.

5.11 Samenwerking met externe partijen

De samenwerking met externe partijen heeft gevolgen voor de informatiebeveiliging van Hecla. Voor de samenwerking met externe partijen van de ontwikkeling en hosting van diensten dient een risicoanalyse te worden uitgevoerd conform de risicoanalysemethode van Hecla (zie 1.0 Algemeen).

Deze risicoanalyse zal worden meegenomen in de risicoanalyse van de bedrijfsmiddelen van Hecla. Noodzakelijke beheersmaatregelen ter bescherming van bedrijfsmiddelen dienen te worden geïmplementeerd. In de overeenkomst en begeleidende documentatie (zoals SLA's, geheimhoudingsovereenkomsten) met externe partijen dient aandacht te worden besteed aan informatiebeveiliging en worden procedures nader uitgewerkt.

5.12 Monitoring, controle en rapportage over informatiebeveiliging

Monitoring betreft het continu bewaken van het niveau van informatiebeveiliging binnen Hecla. Daar waar dit niveau in gevaar komt door het optreden van bedreigingen treedt incidentmanagement in werking om het gewenste beveiligingsniveau te waarborgen, c.q. zo snel mogelijk te herstellen (zie procedure 10.4 Incidentenbeheer informatiebeveiliging).

Met betrekking tot informatiebeveiliging worden de volgende controlevormen onderscheiden:

- *Operationele controle* op de naleving van het informatiebeveiligingsbeleid en de hieruit voortvloeiende richtlijnen en maatregelen. Wordt uitgevoerd door de Security Officer, die de resultaten rapporteert aan de directie. Zie 10.1.4 Operationele planning informatiebeveiliging.
- *Controle op de voortgang* van de implementatie en borging van het informatiebeveiligings-beleid en de hieruit voortvloeiende richtlijnen en maatregelen. Wordt uitgevoerd door de Security Officer, die de resultaten rapporteert aan de directie.
- *Onafhankelijke controle* met betrekking tot informatiebeveiliging wordt uitgevoerd door een onafhankelijke auditor.

6 Specifiek informatiebeveiligingsbeleid

De doelstellingen en uitgangspunten die Hecla heeft geformuleerd op het gebeid van informatiebeveiliging, hebben vanuit de ISO 27001 implementatie geleid tot informatiebeveiligingsbeleid op diverse specifieke punten. Dit beleid heeft betrekking op medewerkers en externe partijen die informatie van Hecla verwerken en hebben als doel, de informatie te beveiligen tegen verlies, beschadiging of oneigenlijk gebruik.

6.1 Mobiele apparatuur en telewerken

Vertrouwelijke data van klanten bevindt zich in een productie omgeving. Via mobiele apparatuur kunnen gebruikers en beheerders via een beveiligde verbinding toegang krijgen tot de productie omgeving om hierin te werken (remote desktop). Er bevinden zich dus geen vertrouwelijke data op mobiele apparatuur (zero footprint). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is geldt: een mobiel apparaat (zoals een handheld computer, tablet, smartphone, PDA) biedt de mogelijkheid om de toegang te beschermen d.m.v. een wachtwoord en versleuteling van die gegevens.

'Bring your own device' is binnen Hecla niet toegestaan. Een device wat niet door Hecla is uitgeleverd mag geen gebruikmaken van het Hecla netwerk en de daarbij behorende diensten. Gast apparatuur mag enkel gebruik maken van het gasten Wifi netwerk en Experience Center Wifi netwerk.

Indien een Hecla medewerker op klantlocatie en/of thuislocatie werk verricht voor Hecla en/of de klanten van Hecla dient men gebruik te maken van het door Hecla voorziene apparaat (laptop/mobiele telefoon/tablet).

Er zijn voorzieningen om de actualiteit van anti-malware programmatuur op laptops te garanderen.

Bij melding van verlies of diefstal wordt de communicatiemogelijkheid met de centrale applicaties afgesloten.

6.2 Back-up en restore

Van alle data van Hecla, waaronder persoonsgegevens wordt dagelijks geautomatiseerd een back-up gemaakt. Dit geldt alleen voor data die op de (virtuele) servers wordt geplaatst. De afdeling ICT, verantwoordelijk voor het beheer van de informatie van Hecla, controleert dagelijks het verloop van de back-up aan de hand van de rapportages die de back-up software afgeeft voor de systemen waarvan een back-up is gemaakt.

De gegevens waarvan een back-up is gemaakt worden direct op storage op de andere fysieke bedrijfslocatie van Hecla opgeslagen.

De afdeling ICT beschikt over de tools om vanaf de gemaakte back-ups een gecontroleerde gehele of gedeeltelijke restore te kunnen uitvoeren, om gegevens die verloren zijn gegaan of beschadigd zijn geraakt, opnieuw te kunnen beschikbaar stellen.

6.3 Toegangsbeveiliging

Zie document 10.3.1 Toegangsbeleid.

6.4 Cryptografie

De belangrijkste reden voor Hecla om cryptografie te gebruiken is de vertrouwelijkheid, integriteit en authenticiteit van informatie te kunnen waarborgen. Technologie en de organisatorische aspecten zijn essentieel om dit mogelijk te maken. Doel van cryptografie is dus om een gecodeerd bericht te sturen dat alleen voor bepaalde personen leesbaar is.
Bij de inzet van cryptografische middelen wordt door Hecla een afweging van de risico's aangaande locaties, processen en behandelende partijen.
Hecla heeft de volgende maatregelen toegepast:

- De gegevens die via de websites van Hecla wordt uitgewisseld zijn met een SSL-certificaat beveiligd;
- De gegevens die via e-mail worden uitgewisseld zijn standaard voorzien van TLS-versleuteling;
- Op de mobiele devices van Hecla wordt vanaf Q3 2019 schijfencryptie ingesteld en toegepast.

6.5 Datalekken

Van een datalek is sprake als er toegang tot, vernietiging, wijziging of vrijkomen van persoonsgegevens van Hecla heeft plaatsgevonden, zonder dat dit de bedoeling is.

Voorbeelden van inbreuk kunnen zijn:

- kwijtraken van een USB -stick;
- diefstal van een laptop;
- inbraak door een hacker;
- persoonsgegevens per ongeluk gepubliceerd;
- hacking, malware of phishing;
- persoonsgegevens aan verkeerde persoon verstuurd;
- calamiteiten zoals brand.

Zowel interne als externe medewerkers en leveranciers van diensten verwerken persoonsgegevens voor Hecla. Indien één van hen een (mogelijk) datalek constateert waarbij het om gegevens van Hecla gaat, moet dit datalek direct (diezelfde dag nog) gemeld worden aan de Privacy Officer van Hecla, zodat deze tijdig het datalek kan inschatten en eventueel kan melden bij de Autoriteit Persoonsgegevens. Ook bij twijfel dient het mogelijke datalek te worden gemeld. De complete procedure is opgenomen in het document 10.4 Incidentenbeheer informatiebeveiliging, hoofdstuk 4.