BIJLAGE 10 – BELEID GEGEVENSBESCHERMING EN INFORMATIEVEILIGHEID

BIJLAGE BIJ HET ARBEIDSREGLEMENT

PREAMBULE

Nu meer dan ooit is informatie een van de belangrijkste pijlers van een organisatie. Informatie op zich, het beheer, de opslag en de verwerking ervan zijn echter onderhevig aan veiligheidsrisico's. Gemeente en OCMW Borgloon zijn zich bewust van deze risico's en nemen de nodige stappen om deze risico's te beheersen. De beheersing van deze risico's begint met het vaststellen van een gegevensbescherming- en informatieveiligheidsbeleid door het management. Dit document voorziet hierin. De beleidsregels die in dit document zijn opgenomen moeten vervolgens ook toegepast worden binnen de organisaties. Waar nodig zal dit onder andere leiden tot specifieker beleid rond specifieke thema's.
Dit beleidsdocument is opgemaakt voor het gemeente- en OCMW-bestuur Borgloon, verder in deze tekst beschreven als organisatie of bestuur.

BELANG VAN INFORMATIEVEILIGHEID EN GEGEVENSBESCHERMING

Het bestuur staat er voor garant dat het verzamelen en verwerken van de gegevens van burgers, medewerkers en derden gebeurt met de grootst mogelijke zorgvuldigheid, op een professionele manier, en met aandacht voor het beschermen van de persoonlijke levenssfeer van de betrokkenen.
Het bestuur streeft continu naar verbetering, met als doel een veilige informatieomgeving te creëren, en alle persoonsgegevens te beschermen conform de Europese Algemene Verordening voor Gegevensbescherming.

In het bijzonder wilt het bestuur de gegevens beschermen tegen

- **Verlies**: de gegevens zijn niet meer beschikbaar.
- **Lekken**: gegevens komen in de verkeerde handen terecht.
- **Fouten**: gegevens zijn niet correct (vb. verouderd of onvolledig).
- **Niet toegankelijk**: gegevens zijn niet beschikbaar. –
- **Onterecht inkijken**: ingekeken door personen die hiertoe niet gemachtigd zijn.
- **Ontbrekende verantwoording**: het niet kunnen nagaan wie de gegevens inkeek, wijzigde of verwijderde.
- **Verwerkingen** die niet in lijn liggen met regelgeving, richtlijnen en normen.

Het bestuur wil beroep doen op iedereen die betrokken is bij het verwerken van persoonsgegevens om samen vanuit een gemeenschappelijke visie de verwerking van de persoonsgegevens binnen het bestuur correct te laten verlopen.

Dit beleid dient als norm voor het verwerken van persoonsgegevens. Het is een leidraad voor alle verwerkingsprocessen en biedt een referentie voor audit en controle. Het biedt elke bewoner, medewerker en externe een inzage in het veiligheidsbeleid en de manier waarop we omgaan met gevoelige persoonsgegevens. Deze tekst draagt ook bij aan de bewustwording omtrent informatieveiligheid.

BEGRIPPENKADER

Voor de toepassing van dit reglement wordt verstaan onder:

Algemene Verordening Gegevensbescherming: de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, met haar wijzigingen en Europese uitvoeringswetgeving;

Wetgeving Gegevensbescherming: de Algemene Verordening Gegevensbescherming, andere Europese regelgeving waarin bepalingen met betrekking tot gegevensbescherming en privacy worden opgenomen, evenals de toepasselijke nationale wetgeving inzake gegevensbescherming en privacy in de lidstaten met haar wijzigingen en uitvoeringsbesluiten, met inbegrip van voor de sector toepasselijke goedgekeurde richtlijnen.

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (het personeelslid). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. Ook gepseudonimiseerde gegevens die door het gebruik van aanvullende gegevens aan een natuurlijke persoon kunnen worden gekoppeld, zijn dus persoonsgegevens. Anonieme gegevens, die op geen enkele wijze nog kunnen worden gelinkt aan een persoon, vallen niet onder de Verordening Gegevensbescherming.

Bijzondere persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen gebruiken, verstrekken door middel van

doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Bestand: elk gestructureerd geheel van personeelsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.

Betrokkene: de geïdentificeerde of identificeerbare natuurlijke persoon van wie gegevens worden verwerkt.

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Stad Borgloon houdt persoonsgegevens bij van de medewerkers in het kader van de bestuur – werknemer arbeidsrelatie. Deze persoonsgegevens worden verwerkt onder de verantwoordelijkheid van stad Borgloon, Speelhof 10 – 3840 Borgloon, KBO 0206.914.361.

Het e-mail adres van de verwerkingsverantwoordelijke van stad Borgloon: informatieveiligheid@borgloon.be

Informatieveiligheid: Informatieveiligheid om van het geheel van technische en organisatorische maatregelen die ervoor zorgen dat een door het veiligheidsbeleid vooropgesteld veiligheidsniveau wordt nagestreefd. Hierbij staan de integriteit, de beschikbaarheid en de vertrouwelijkheid van de gegevens centraal.

Gegevensbescherming: houdt de maatregelen in tot naleving van de regels met betrekking tot de verwerking van persoonsgegevens en het vrije verkeer van persoonsgegevens, zoals deze worden bepaald in de Verordening Gegevensbescherming en andere regelgeving over de verwerking van persoonsgegevens.

In voornoemde regelgeving worden regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens. De regelgeving vrijwaart het recht op bescherming van persoonsgegevens.

HOOFDSTUK I. TOEPASSINGSGEBIED

Het beleid gegevensbescherming en informatieveiligheid is van toepassing op de verwerking van persoonsgegevens waarbij het bestuur als verwerkingsverantwoordelijke (al dan niet samen met anderen) of verwerker wordt aangeduid.

Het beleid is van toepassing op alle persoonsgegevens die het bestuur verwerkt. Niet alleen de gegevens van de burgers, maar ook bijvoorbeeld van medewerkers, al dan niet in dienstverband, bezoekers, vrijwilligers, … Dus elke geïdentificeerde of identificeerbare persoon. Het gegevensbeschermingsbeleid is van toepassing op alle verwerkingsdoelen (administratief, financieel, kwaliteits-en risicocontroles, rapportering, research, etc..).

HOOFDSTUK II: DE ORGANISATIE VAN GEGEVENSBESCHERMING EN INFORMATIEVEILIGHEID

A. Het managementteam en ICT PD

Het managementteam fungeert als formeel beslissingsplatform voor informatieveiligheid. Het is bevoegd om beslissingen te nemen die betrekking hebben op volgende aspecten:

- De risicoanalyse en bijhorende methodiek
- De effectieve risicobeoordeling
- Het ontwikkelen van het informatieveiligheidsbeleid en de bijhorende richtlijnen
- De implementatie van beveiligingsmaatregelen (i.e. de inhoud van het veiligheidsplan)
- Het nakomen van alle wettelijke verplichtingen inzake gegevensbescherming

B. Data Protection Officer (DPO)

De DPO verleent bijstand, verstrekt informatie over en kijkt toe op de verplichtingen van het bestuur ten aanzien van de verordening. De DPO is bevoegd voor volgende aspecten:

- Bijstand en advies verlenen (wettelijke taak)
  - De principes van het verwerken van persoonsgegevens en in het bijzonder gevoelige persoonsgegevens.
  - De rechten van de betrokkene.
  - Gegevensbescherming bij ontwerp en standaardinstellingen, het register voor de verwerkingsactiviteiten.
  - De informatieveiligheid.
  - De elementen die horen bij het afhandelen en melden van inbreuken.
- Toekijken op de naleving van de wetgeving
  - De correcte toepassing van het beleid voor gegevensbescherming.
  - De correcte toepassing van alle Europese, Federale en Vlaamse regelgeving over het verwerken van persoonsgegevens.
  - Toekijken of iedereen de in dit beleidsdocument omschreven verantwoordelijkheid opneemt.
  - Toekijken op het bewustzijn inzake gegevensbescherming bij de interne/externe klanten.
  - Toekijken en kennisnemen van de inhoud van andere audits en controles die handelen (of elementen bevatten) van audits.
- Advies verstrekken over gegevensbeschermingseffectenbeoordelingen (GEB).
- Contactpunt zijn voor de Gegevensbeschermingsautoriteit en hiermee samenwerken.
- Coördineren van incidentmeldingen in verband met gegevensbescherming.

C. De medewerker

Iedereen (intern of extern) die persoonsgegevens verwerkt (bijvoorbeeld inkijkt, registreert, wijzigt, …), doet dit volgens de principes uit dit beleid. De medewerker verwerkt gegevens in overeenstemming met de discretieplicht, en conform volgende principes:

- Is verantwoordelijk voor de gegevens van de betrokkenen die hij/zij verwerkt.
- Voert de veiligheidsrichtlijnen uit tijdens zijn/haar verwerkingsopdracht.
- Verwerkt enkel die gegevens die horen bij de taak.
- Draagt zorg voor de gegevens.
- Meldt inbreuken.
- Respecteert het beroepsgeheim (artikel 458 van het Strafwetboek) en de discretieplicht.

D. Diensthoofd

Bijkomend aan de verantwoordelijkheid van de medewerker, ziet het diensthoofd toe op de goede uitvoering van de veiligheidsbepalingen:

- Volgt de veiligheidsrichtlijnen op en informeert de medewerkers hierover (bijvoorbeeld personaliseren van gekregen wachtwoorden, na gebruik afmelden, informatie op papier niet laten liggen, …).
- Zorgt voor een veiligheidscultuur op de dienst en onderhoudt deze (bijvoorbeeld door het bespreken van de beleidsrichtlijnen op het teamoverleg).

E. De ICT-leverancier

De ICT-medewerker(s) is verantwoordelijk voor:

- Implementatie van de technische maatregel.
- Implementatie van de veiligheidsinstellingen in lijn met dit beleid.
- Melden van veiligheidsproblemen die ontstaan voor, tijdens of na de implementatie van ICT middelen aan de DPO.
- Fungeren als expert. Vanuit deze rol neemt hij/zij deel aan de identificatie zowel als aan de remediëring van de informatieveiligheidsrisico's.
- Wijst op eventuele veiligheidsrisico's van geleverde toepassingen.
- Wijst op de op te nemen veiligheidstaken.
- Streeft een transparant veiligheidsbeleid na door te communiceren over het eigen actuele veiligheidsniveau.
- Geeft ondersteuning bij de afhandeling van veiligheidsincidenten.

HOOFDSTUK III: BELEIDSDOELSTELLINGEN VOOR GEGEVENSBESCHERMING

Algemene doelstellingen

Het bestuur in haar rol als verwerkingsverantwoordelijke:

1. Is **transparant** over de persoonsgegevens die het verwerkt en het verwerkingsdoel, zowel naar de betrokkene als naar de toezichthouders. De gevoerde communicatie is eerlijk, eenvoudig toegankelijk en begrijpelijk. Het transparantieprincipe is ook van toepassing wanneer persoonsgegevens worden uitgewisseld.

2. Verwerkt enkel de gegevens die **relevant** zijn voor het uitvoeren van haar taken. Elke taak waarbij persoonsgegevens worden verwerkt, is **rechtmatig**. Dit betekent onder meer dat de verwerking in overeenstemming is met de wettelijke en statutaire doelen van het bestuur. Dit wordt telkens geëvalueerd bij een nieuw verwerkingsdoel.
3. Verwerkt enkel de persoonsgegevens die **strikt noodzakelijk** zijn voor de uitvoering van de activiteiten zoals benoemd in de privacyverklaring. Zo worden identificatoren die horen bij de persoonsgegevens tot een minimum herleid.
4. Kijkt toe op de **integriteit** van de persoonsgegevens tijdens de volledige verwerkingscyclus.
5. **Bewaart** gegevens niet langer dan noodzakelijk. De noodzakelijkheid is afgetoetst tegenover wettelijke verplichtingen en de rechten en vrijheden van de betrokkene.
6. Voorkomt **inbreuken die voortvloeien uit het verwerken** van persoonsgegevens. Informatieveiligheid, gegevensbescherming door ontwerp en privacy-vriendelijke standaardinstellingen zijn hiervoor hulpmiddelen. Wanneer een inbreuk plaatsvindt, wordt hierover **gerapporteerd** in lijn met de regelgeving ter zake.
7. Is in staat om alle geldende **rechten van een betrokkene**, zoals het recht op inzage, afschrift en eventueel ook schrapping, uit te voeren. het bestuur waakt hierbij over de eventuele beperkingen die op deze rechten van toepassing zijn.
8. Verwerkt gegevens in lijn met de rechten en vrijheden die gelden in de Europese Economische Ruimte en controleert de toepassing hiervan wanneer de gegevens worden uitgewisseld daarbuiten. Het bestuur leeft bijgevolg alle **wettelijke en normerende kaders na** (i.e. zowel Vlaamse, Federale als Europese regels) bij het verwerken van persoonsgegevens en heeft daartoe haar verantwoordelijkheid over de persoonsgegevens en die van anderen duidelijk in kaart gebracht. het bestuur monitort daarenboven ook de in de sector geldende gedragscodes (indien van toepassing) en past deze toe.
9. Kan aantonen dat het alle beleidsdoelstellingen naleeft, conform de wettelijke bepalingen. Deze **verantwoordingsplicht** wordt bewaakt door interne toezicht en controle en is uitvoerbaar volgens de wettelijk geldende principes.

HOOFDSTUK IV: VERPLICHTINGEN VAN DE VERWERKINGSVERANTWOORDELIJKE

Los van de algemene verplichtingen zijn er ook een aantal specifieke verplichtingen die de GDPR oplegt:

1. Het bijhouden van een register van verwerkingsactiviteiten.
   Het bestuur beheert een register van alle activiteiten waarbij persoonsgegevens worden verwerkt.
2. Maatregelen ter beveiliging van de verwerking.
   Persoonsgegevens mogen slechts verwerkt worden indien er passende technische en organisatorische maatregelen zijn genomen voor het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de verwerkte persoonsgegevens.
3. Melden van inbreuken in verband met verwerking van persoonsgegevens.

Uit de AVG volgt een plicht voor het bestuur om een incidentmeldingssysteem voor de interne registratie van inbreuken te hebben die betrekking heeft op het verwerken van persoonsgegevens.

4. Aanstellen van een functionaris voor de gegevensbescherming (DPO).
   Iedere verwerkingsverantwoordelijke is verplicht om een Data Protection Officer (DPO) aan te stellen indien de kerntaak een grootschalige verwerking van persoonsgegevens is. Het bestuur is dus verplicht tot de aanstelling van een DPO.
5. Naleving van de rechten van de betrokkene.
   Het bestuur dient gedocumenteerde bedrijfsprocessen op te stellen die voorzien in het naleven van de rechten van de betrokkene (het recht op inzage, afschrift, gegevenswissing, rectificatie, beperking van de verwerking, kennisgeving, overdraagbaarheid).

HOOFDSTUK V: BELEIDSDOELSTELLINGEN VOOR INFORMATIEVEILIGHEID

Informatieveiligheid is een belangrijk onderdeel binnen gegevensbescherming, beiden zijn echter wel degelijk verschillend.

Gegevensbescherming omvat alle aspecten zoals benoemd in de GDPR/AVG over de wijze waarop persoonsgegevens mogen worden verwerkt. Het betreft in feite de principes zoals deze ook benoemd zijn in dit hoofdstuk. Een onderdeel hiervan is de beveiliging van de gegevens, maar gegevensbescherming is dus breder dan enkel het beveiligen van gegevens.

Informatieveiligheid betreft de beveiliging van alle soorten informatie binnen een organisatie, waaronder persoonsgegevens. Dit is waar informatieveiligheid relevant is voor gegevensbescherming, en waar de twee elkaar ontmoeten: informatieveiligheid omvat het beveiligen, naast alle andere informatie, van persoonsgegevens en gegevensbescherming omvat dan weer alle aspecten rond de omgang met persoonsgegevens, waaronder de beveiliging.

Als onderdeel van dit gegevensbeschermingsbeleid wordt zodoende ook aandacht besteed aan informatieveiligheid, waarbij de belangrijkste beleidsprincipes rond informatieveiligheid in dit hoofdstuk worden benoemd. De structuur is gebaseerd op de internationaal erkende norm met betrekking tot informatieveiligheid, de ISO2700 (specifiek: het controlekader van de ISO27002).

Specifieke voorwaarden waaraan het beleid informatieveiligheid moet voldoen:

Voorwaarde	Toelichting	Minimaal na te leven norm
1.Identiteitsbeheer	Stemt de digitale en de burgerlijke identiteit van de medewerker (natuurlijke persoon)	Een procedure voor identiteitsbeheer en de implementatie van de nodige maatregelen om deze af te dwingen, waaronder zowel technische als maatregelen zoals bewustwording bij de gebruikers. De

	van de Dienst overeen (of met andere woorden: is hij/zij de persoon die hij/zij beweert te zijn).	procedure heeft als doel de levensloop van de digitale identiteit te koppelen aan de bewegingen binnen de organisatie (instroom, doorstroom en uitstroom van medewerkers). Deze procedure wordt ondersteund door een risicoanalyse en bevat maatregelen om deze risico's te beperken.
2. Toegangsbeheer	Bewaakt dat iedere medewerker de beoogde bewerking met persoonsgegevens mag uitvoeren (consulteren, wijzigen, bijwerken).	Een procedure die het opstellen en onderhouden van een takenmatrix, alsook de naleving hiervan bij het toewijzen van de taken, garandeert. Maatregelen worden genomen om misbruik, gewild of ongewild, te voorkomen, waaronder toezicht.
3. Relatie met de betrokkene	Een aantoonbare 'overeenkomst', die het verwerken van de gegevens van de betrokkene rechtvaardigt. In deze overeenkomst is het tevens duidelijk op welke manier de betrokkene rechten kan uitoefenen inzake verwerking van persoonsgegevens en de bijhorende procedures.	Een procedure die toelicht welke stappen er nodig zijn om aan de voorwaarden te voldoen van het verkrijgen van een geldige relatie met de betrokkene en garanties biedt dat deze relatie correct wordt opgevolgd (bijvoorbeeld het beëindigen van de relatie moet correct worden opgevolgd). Deze garanties kunnen bestaan uit technische en organisatorische maatregelen, waaronder bewustwording.
4. Logging	Elke handeling van elke medewerker moet kunnen worden opgespoord en verantwoord.	Een procedure die instructies geeft over de wijze van logging en de systematische controle van de logging met het oog op kwaliteitsgaranties.

Naast garanties dat maatregelen en procedures zijn geïmplementeerd met betrekking tot identiteiten toegangsbeheer, onderhoud van de relatie met de betrokkene en logging, zullen ook garanties worden afgedwongen bij iedereen die bij de verwerking betrokken is, waaronder personeelsleden en leveranciers. Voor personeelsleden omvat dit aandacht voor de nodige afspraken en instructies, inclusief sancties bij overtredingen. Gezien de technische implementatie in quasi alle gevallen in handen is van een leverancier van software, dienen deze eveneens garanties te geven die in een contract met de leverancier zijn voorzien.

Voorwaarde	Toelichting	Minimaal na te leven norm
5. Omgaan met medewerkers en leveranciers	Afdwingen dat de nodige technische en organisatorische maatregelen in acht nemen bij het uitvoeren van verwerkingsactiviteiten.	Voor personeelsleden: bewustwordingssessies en afspraken. Voor leveranciers: een procedure voor het afsluiten en onderhouden van een contract, inclusief een beheer van alle operationele verplichtingen.

Bovenstaande vijf specifieke voorwaarden worden omkaderd met een algemeen beleid informatieveiligheid en een op een risicoanalyse gebaseerd veiligheidsplan. Dit alles onder toezicht van een functionaris voor de gegevensbescherming.

Voorwaarde	Toelichting	Na te leven norm
Algemene voorwaarde: Veiligheidsbeleid	Een beleidstekst waarin de uitgangspunten van het veiligheidsbeleid, inclusief de verantwoordelijkheden en taken worden toegelicht.	Een veiligheidsbeleid dat veiligheidsmaatregelen omkadert en verantwoordelijkheden aanduidt.
Algemene voorwaarde: Veiligheidsplan	Een op een risicoanalyse gebaseerd veiligheidsplan waarin te implementeren maatregelen om de risico's in te perken, in een plan van aanpak worden uitgezet.	Elke organisatie heeft risico's inzake informatieveiligheid in kaart gebracht.
Algemene voorwaarde: Toezicht door functionaris voor gegevens-bescherming	De functionaris voor de gegevensbescherming bewaakt de toepassing van de onderhavige richtsnoeren.	De verwerkingsactiviteiten staan onder toezicht van de functionaris voor de gegevensbescherming
Algemene voorwaarde: Voldoen aan nalevings-voorwaarden	De organisatie kan zich steeds verantwoorden voor de naleving van de veiligheids-voorwaarden en	Voorzien in een procedure voor inbreuken bij verwerkingsactiviteiten of in het kader van de naleving van veiligheidsvoorwaarden.

	neemt maatregelen wanneer er inbreuken of incidenten plaatsvinden	

Andere aandachtspunten voor informatieveiligheid.

Onderstaande punten zijn eveneens na te leven.

1. **Beheer bedrijfsmiddelen:**
   Het bestuur beheert een overzicht van alle in gebruik zijnde bedrijfsmiddelen en wie deze in gebruik heeft, het betreft voornamelijk laptops en smartphones.
2. **Cryptografie:**
   Het bestuur heeft haar website beveiligd met een https verbinding en maakt gebruik van encryptie waar nodig bij de opslag van digitale gegevens.
3. **Fysieke veiligheid & bescherming van de omgeving.**
   Volgende systemen en procedures garanderen de fysische bescherming van belangrijke gegevens:
   - Camerabewaking
   - Sleutel/alarm buiten kantooruren
   - Medewerkers worden geacht wanneer ze hun toestellen onbeheerd achterlaten hun schermbeveiliging te activeren.
   - Medewerkers worden geacht geen onnodige gegevens (op papier dan wel digitaal) op hun werkplek achter te laten.
4. **Operationele veiligheid:**
   - Back-ups, back-up schema
   - Logging in applicaties
   - Monitoring van servers en apps
   - Antivirus, firewall, spamfilter
5. **Communicatieveiligheid:**
   - Afgeschermd LAN netwerk
   - Beveiligde WAN connecties
   - Wifi netwerk voor gasten
6. **Beheer van informatieveiligheidsincidenten:**
   Het bestuur beschikt over een procedure voor veiligheidsincidenten.
7. **Informatieveiligheidsaspecten van bedrijfscontinuïteitsbeheer:**
   Het bestuur beschikt over een continuïteitsplan.
8. **Naleving:**
   Het bestuur heeft verantwoordelijkheden toebedeeld om er voor te zorgen dat alle wettelijke, contractuele, en regelgevende kaders bekend zijn en dat het bestuur hieraan voldoet.
   Het bestuur draagt er zorg voor dat enkel legale software gebruikt wordt en dat deze enkel wordt aangeschaft bij erkende verkopers. Waar nodig zijn voldoende licenties beschikbaar voor het aantal gebruikers van gegeven software.