Beleidslijn informatieveiligheid en privacy

Continuïteitsbeheer

(BLD BCM)

INHOUDSOPGAVE

1. INLEIDING 3
2. CONTINUÏTEITSBEHEER 3
BIJLAGE A: DOCUMENTBEHEER 4
BIJLAGE B: REFERENTIES 4
BIJLAGE C: RICHTLIJNEN ROND CONTINUÏTEIT VAN INFORMATIEVEILIGHEID EN PRIVACY 5
BIJLAGE D: LINK MET DE ISO-NORM 27002:2013 8

1. Inleiding

Dit document maakt integraal deel uit van de methodologie informatieveiligheid en privacy binnen de sociale zekerheid. Dit document is bestemd voor de verantwoordelijken, voor de verwerkers van informatie, voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van de sociale zekerheid (OISZ).
De voornaamste doelstellingen van continuïteitsbeheer zijn

- kritieke processen beschermen tegen de gevolgen van ernstige incidenten of rampen
- een coherente en gemeenschappelijke aanpak hanteren voor de verwezenlijking van het continuïteitsplan.
- ervoor zorgen dat alle noodzakelijke componenten aanwezig zijn zodat de organisatie gepast kan reageren op ernstige incidenten of rampen en een tijdig herstel kan bewerkstelligen

Continuïteitsbeheer is breder dan ICT: het uitvallen van medewerkers (ziekte, ontslag, dood) of het verdwijnen van een kritieke leverancier kan een reële bedreiging zijn. Bij de inrichting van continuïteitsbeheer dienen alle relevante aspecten meegenomen te worden die de continuïteit in gevaar kunnen brengen.

In dit document worden aspecten van informatieveiligheid en privacy behandeld op het vlak van informatieverwerking bij het beheer van continuïteit van een organisatie : een pragmatische aanpak om (kritieke) processen te beschermen tegen de gevolgen van omvangrijke storingen of rampen en om tijdig herstel te bewerkstelligen in lijn met de verwachtingen van de organisatie.

2. Continuïteitsbeheer

Elke organisatie onderschrijft de volgende beleidslijnen van informatieveiligheid en privacy voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de organisatie:

a. Voor alle kritieke processen en essentiële informatiesystemen moet er een continuïteitsplan zijn, waarin activiteiten, maatregelen en belangrijke gegevens van de processen van de organisatie worden beschreven, die tot doel hebben de onderbrekingstijd tot een aanvaardbaar niveau te beperken.

b. Informatieveiligheid en privacy dienen een integraal onderdeel te zijn van continuïteitsbeheer.

c. Elke organisatie heeft een eigen continuïteitsplan met minimaal aandacht aan:
    1) Identificatie en documentatie van essentiële processen en bijhorende informatiesystemen van de organisatie;
    2) Risico-beoordeling met invulling van kans, impact en huidige controlemaatregelen;
    3) Kennis en competenties van medewerkers om essentiële processen en bijhorende informatiesystemen van de organisatie draaiende te houden of weer op te starten;
    4) Wie mag wanneer en hoe wordt het continuïteitsplan geactiveerd bij een ernstig incident of ramp;
    5) Informatie (aanvaardbaarheid van verlies van informatie);
    6) Prioriteiten en volgorde van herstel;
    7) Communicatie tijdens en na een ernstig incident of ramp;
    8) Wie mag wanneer en hoe wordt het uitgevoerde continuïteitsplan formeel afgesloten na een ernstig incident of ramp.

d. Door het inrichten van een adequaat continuïteitsbeheer dient een organisatie te waarborgen dat de impact van een ernstig incident of ramp en het herstel daarvan tot een aanvaardbaar niveau wordt beperkt in lijn met de verwachtingen van de organisatie.

e. Het continuïteitsplan dient regelmatig getest en aangepast te worden. De resultaten van de testen dienen gecommuniceerd te worden naar de directie van de organisatie voor validatie en goedkeuring van verdere acties.

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2014		V2014	Eerste versie	20/09/2014	01/10/2014
2017		V2017	Integratie EU GDPR	07/03/2017	07/03/2017

Fouten en weglatingen

Wanneer bij het lezen van dit document fouten of problemen worden vastgesteld, dan wordt u als lezer verzocht om een korte beschrijving van de fout of het probleem en de locatie in het document samen uw contactinformatie door te geven aan de informatieveiligheidsconsulent (CISO) / functionaris van gegevensbescherming (DPO) van de organisatie.

Definities

Om consistentie te garanderen in gebruikte terminologie en begrippen doorheen alle beleidsdocumenten, worden alle definities met betrekking tot informatieveiligheid en privacy gecentraliseerd in één document genaamd “Definities informatieveiligheid en privacy”.

Bijlage B: Referenties

Hieronder staan documenten vermeld die hebben gediend als inspiratie voor dit document:

- ISO, “ISO/IEC 27001:2013 Information Security Management System Requirements”, september 2013, 23 blz.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, september 2013, 80 blz.
- ISO, “ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity”, juni 2016, 36 blz.
- ISO, “ISO/IEC 22301:2012 Societal security. Business continuity management systems. Requirements”, mei 2012, 24 blz.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.
- FOD Binnenlandse Zaken, “BUSINESS CONTINUITY MANAGEMENT, handleiding voor implementatie”, juni 2009, 132 blz.

Hieronder staan referenties naar websites die hebben gediend als inspiratie voor dit document:

- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- https://www.iso.org/standard/44374.html
- https://www.iso.org/standard/50038.html
- http://www.isaca.org/cobit
- http://crisiscentrum.be/nl/publication/business-continuity-management-een-handleiding-bij-de-implementatie
- http://www.ccb.belgium.be/nl/work
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Bijlage C: Richtlijnen rond continuïteit van informatieveiligheid en privacy

Het proces inzake continuïteitsbeheer

In het proces van continuïteitsbeheer (business continuity management of BCM) worden de bedreigingen voor een organisatie geïdentificeerd zodat deze haar missie kan blijven vervullen in geval van een ernstige gebeurtenis of een ramp. Continuïteitsbeheer resulteert in het opstellen, het actualiseren en, in geval van schade, het activeren van het continuïteitsplan totdat de normale toestand hersteld is.
De activiteiten omvatten:

1. Het continuïteits-programma: deze fase legt de organisatiestructuur en de doelstellingen van het project vast.
2. Het begrip van de organisatie: Door middel van een impact- en risico-beoordeling worden in deze fase de gevolgen van een procesonderbreking voor de organisatie geëvalueerd en kunnen de beschikbaarheidscriteria voor elk proces in de organisatie bepaald worden.
   Veiligheidsdoelstelling: in deze analyse wordt rekening gehouden met de informatieveiligheid
3. Strategie van het continuïteitsplan (Business Continuity Plan of BCP): Uitwerken van de continuïteitsstrategie volgens de te bereiken doelstellingen
   Veiligheidsdoelstelling: Definitie van de minimale veiligheidsnormen
4. Implementatie van het continuïteitsplan: Opstellen van het continuïteitsplan
   Veiligheidsdoelstelling: ervoor zorgen dat er rekening wordt gehouden met de veiligheidsvereisten
5. Testen van het continuïteitsplan: Door de plannen te testen kan geverifieerd worden dat de kritieke activiteiten hersteld kunnen worden binnen de vooropgestelde termijn
   Veiligheidsdoelstelling: Nagaan of de veiligheidsvereisten operationeel zijn
6. Onderhoud en herziening van het continuïteitsplan en opleiding van medewerkers in het kader van het continuïteitsplan:
   Veiligheidsdoelstelling : De continuïteitsplan-documenten bijwerken

Richtlijnen inzake het aspect informatieveiligheid en privacy in het continuïteitsplan

Strategie inzake de continuïteit van de informatieveiligheid en privacy

- De directie moet een kader bieden voor het vaststellen van de doelstellingen inzake de continuïteit; met inbegrip van de verbintenis om aan alle toepasselijke voorwaarden te voldoen, om inherente verantwoordelijkheden toe te kennen en om tevens te werken aan de permanente verbetering van het continuïteitsplan.
- Continuïteit is een interactief proces dat actief beheerd moet worden. Om te beginnen kan het continuïteitsplan beheerd worden door middel van een aanpak voor projectbeheer. Dit plan moet minstens één keer per jaar worden geactualiseerd.
- Voor alle activa die als kritiek worden omschreven door de organisatie, moeten de beschikbaarheidscriteria betreffende de hervatting van de activiteiten omschreven en gedocumenteerd worden. De minimale beschikbaarheidscriteria zijn de volgende: RTO–RPO.
- Het is ook noodzakelijk om bij de start van elk nieuw toepassingsproject of elk project betreffende een service reeds de informatieveiligheid- en privacy-vereisten te vermelden in de voorafgaande analyse, in het bijzonder de beschikbaarheidscriteria.
- De waardering en de behandeling van de informatieveiligheid- en privacy-risico's van de informatiesystemen dragen bij tot de uitwerking van deze plannen, onder meer door het kritieke karakter van de activiteiten en de informatiesystemen, de residuele risico's en de te integreren veiligheidsmaatregelen te omschrijven. De informatieveiligheidsconsulent (CISO) en de functionaris voor de gegevensbescherming (DPO) die integraal deel uitmaken van het risico beheerproces, moeten samenwerken met de in het continuïteitsplan aangestelde verantwoordelijke voor de uitwerking van het continuïteitsplan.
- Bij de risico-beoordeling moet de organisatie tevens elke kritieke activiteit identificeren en nagaan waarin zij afhankelijk is van leveranciers en andere derden en ervoor zorgen dat de aspecten informatieveiligheid en privacy opgenomen zijn in het continuïteitsplan.

Ontwikkeling van de continuïteit van de informatieveiligheid en privacy

- De organisatie verbindt zich ertoe om een permanent en formeel proces te implementeren voor het beheer van de continuïteit van de informatieveiligheid en privacy, alsook de geschikte structuur om zich voor te bereiden op een ongewenst voorval, het te beperken en erop te reageren.
- In dit kader is er een incidentenbeheer operationeel in de organisatie (waar er rekening wordt gehouden met informatieveiligheids- en privacy-incidenten).
- Op basis van een bestaand continuïteitsplan of een risico-beoordeling moet de organisatie het toelaatbare niveau bij verminderde dienstverlening bepalen als activiteiten worden hervat na een ernstig incident of ramp.
- Het vereiste minimale informatieveiligheid- en privacy-niveau bij verminderde dienstverlening wordt gedocumenteerd in het continuïteitsplan.
- Er moet voor gezorgd worden dat de informatieveiligheid- en privacy-vereisten operationeel zijn in de back-up- en herstelvoorzieningen.

Controle, herziening en evaluatie van de continuïteit van de informatieveiligheid en privacy

- Er wordt een jaarlijks testplan bepaald en goedgekeurd door de directie.
- De informatieveiligheidsconsulent (CISO) en de functionaris voor de gegevensbescherming (DPO) gaan na of er bij de voorgestelde tests rekening wordt gehouden met de continuïteit van informatieveiligheid en privacy.
- De organisatie voert regelmatig evaluaties uit van haar procedures en capaciteiten inzake continuïteit en zorgt ervoor dat het vastgestelde niveau nageleefd wordt bij verminderde dienstverlening.
- Aangezien het plan regelmatig herzien worden, moet dit in het begin van het jaar gepland worden, zodat de plannen tegen een vastgelegde datum geconsolideerd zijn.
- De organisatie moet erover waken dat het continuïteitsplan gepubliceerd en verdeeld worden onder de betrokkenen, zodat deze plannen beschikbaar zijn in geval van een ernstig incident of ramp waarbij hun uitvoering vereist is.
- Bij elke herziening van het continuïteitsplan voorziet de organisatie voor de betrokken actoren een sensibiliseringssessie omtrent de aanpassingen.
- De informatieveiligheidsconsulent en de functionaris voor de gegevensbescherming zien regelmatig het continuïteitsplan na. Ze analyseren de testresultaten om lacunes en incoherenties op te sporen. Indien nodig, stellen ze relevante verbeteringen voor.

Redundanties

Op basis van een risico-beoordeling heeft de organisatie de vereisten geïdentificeerd inzake de beschikbaarheid van informatiesystemen:

- Indien de beschikbaarheid van de informatiesystemen niet kan gegarandeerd worden met de bestaande infrastructuur, moet redundantie van de componenten of de architectuur overwogen worden.
- Wanneer het van toepassing is, moet de redundantie van de informatiesystemen regelmatig getest worden om ervoor te zorgen dat de omschakeling van de ene component naar de andere naar behoren functioneert.
- De implementatie van de redundantie kan nieuwe risico's met zich meebrengen op het vlak van de integriteit en de vertrouwelijkheid van de informatiesystemen; hiermee moet rekening worden gehouden tijdens het ontwerp van deze redundantie.

Beheersmaatregelen

1. Kader voor continuïteitsplan

De organisatie dient een kader voor een continuïteitsplan te ontwikkelen/adopteren. Dit om te waarborgen dat alle plannen consistent zijn, om informatieveiligheids- en privacy-vereisten op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud.

2. Informatieveiligheid en privacy opnemen in het proces van continuïteitsbeheer

De organisatie dient een proces voor continuïteit te ontwikkelen en bij te houden, zodat de naleving van vereisten voor informatieveiligheid en privacy wordt geborgd die nodig zijn voor de continuïteit van de werking van de organisatie.

3. Continuïteit en risicobeoordeling

Gebeurtenissen die tot onderbreking van processen kunnen leiden, moeten geïdentificeerd worden door het uitvoeren van een risico-beoordeling. Aan de hand van een risico analyse dienen de waarschijnlijkheid/kans en de gevolgen/impact van de onderbreking in kaart gebracht te worden in termen van tijd, schade en herstelperiode. Het is verstandig en efficiënt om informatieveiligheidsaspecten op te nemen in de normale risico analyse van het continuïteitsbeheer. Dit impliceert dat de continuïteitsvereisten rond informatieveiligheid en privacy expliciet worden geformuleerd in de procedures van het continuïteitsbeheer. De achterliggende gedachte is om tijd en moeite te besparen aangezien er geen 'extra' risico analyse voor informatieveiligheid en privacy moet uitgevoerd worden.

4. Continuïteitsplan ontwikkelen, valideren, implementeren en communiceren

Er moeten plannen ontwikkeld en geïmplementeerd worden om de activiteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vooraf afgesproken niveau en binnen in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritieke processen. Hierbij wordt expliciet rekening gehouden met informatieveiligheid en privacy aspecten.

De ontwikkelde continuïteitsplannen kunnen gebruikt worden in de bewustwording-, training- en testactiviteiten.

5. Testen, beoordelen en aanpassen van continuïteitsplan

Continuïteitsplan dient regelmatig getest te worden om te waarborgen dat het actueel en doeltreffend blijft. Aan de hand van de resultaten dient het continuïteitsplan aangepast en gecommuniceerd te worden naar de betrokken partijen.

Prioriteiten

Tijdens een ernstig incident of ramp kunnen niet alle processen doorgaan: daarvoor zijn over het algemeen te weinig middelen en medewerkers beschikbaar. Er dienen dus keuzes te worden gemaakt: hoe zet de organisatie de schaarse mensen en middelen in? Wat zijn de prioriteiten voor de organisatie?

Processen kunnen bijvoorbeeld ingedeeld worden in groepen (prioriteiten):

- processen die geen dag uitgesteld kunnen worden;
- processen die maximaal 1 dag uitgesteld kunnen worden;
- processen die maximaal 1 week uitgesteld kunnen worden;
- processen die maximaal 1 maand uitgesteld kunnen worden;
- processen die maximaal 3-6 maanden uitgesteld kunnen worden.

Voor organisaties is de product- en service-catalogus een handig hulpmiddel.

Bijlage D: Link met de ISO-norm 27002:2013

Hier wijzen we op de voornaamste clausule(s) van de ISO-norm 27002:2013 die verband houden met het onderwerp van het huidige document.

ISO-norm 27002:2013	
Veiligheidsbeleid	
Organisatie van de informatieveiligheid.	
Veilig personeel	
Beheer van bedrijfsmiddelen	
Toegangsbeveiliging	
Cryptografie	
Fysieke beveiliging en beveiliging van de omgeving	
Beveiliging processen	
Communicatieveiligheid	
Aankopen, onderhouden en ontwikkelen van informatiesystemen	
Leveranciersrelaties	
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	**Ja**
Naleving	

***** EINDE VAN DIT DOCUMENT *****