



Betreft: **Cyberterrorisme**
Revisie: 0

Document:
Uitgifte datum: PR-35
25-10-2024

Eigenaar : Bestuurder

1. Toepassingsgebied (scope)

Met hulp van een Business Impact Analyse is in kaart gebracht wat de belangrijkste kritische gebeurtenissen en bedreigingen voor de continuïteit van zorg zijn voor Stichting Het Robertshuis.

Dit heeft geleid tot de volgende crisisscenario's:

- Sluiting (delen) van de locatie
- Verplaatsen van cliënten bij evacuatie
- Groot aanbod van cliënten van een andere organisatie in nood
- Tekort aan personeel
- Uitval van nutsvoorzieningen, apparatuur en ICT-middelen
- Uitbraak infectieziekten
- Cyberterrorisme

Het onderhavige protocol beschrijft de maatregelen die genomen dienen te worden in het geval van cyberterrorisme. Indien na een calamiteit de situatie genormaliseerd is, is tevens weergegeven welke verantwoordelijkheden zijn belegd (Fase 'Groen'). Onderstaande escalatiefases maken inzichtelijk bij welke crisissituatie het crisisscenario in werking treedt.



2. Definities

Crisisteam	Team bestaande uit FOBO-functionarissen, brandveiligheid functionaris, facilitair medewerker en gedragswetenschapper, Bestuurder en een lid van de Raad van Toezicht.
GHOR	De Geneeskundige Hulpverleningsorganisatie in de Regio (GHOR) organiseert de geneeskundige hulpverlening bij zware ongevallen, rampen en crises. De GHOR is onderdeel van een veiligheidsregio.



Betreft:	Cyberterrorisme	Document:	PR-35
Revisie:	0	Uitgifte datum:	25-10-2024

3. Crisisscenario

Wie		Wat	Waarmee
Medewerker	1.	Signaleert cyberterrorisme en Informeert FOBO-functionaris.	
FOBO-functionaris	2.	Informeert Bestuurder.	
Bestuurder	3.	Schat escalatiefase in, in samenspraak met relevante locatie leidinggevende	
	4.	Inventariseert omvang van de calamiteit, eventueel verwachte tijdsduur en gevolgen voor de organisatie.	
	5.	Escaleert zo nodig naar het Crisis-team, indien omvang, verwachte tijdsduur en/of gevolgen daarom vraagt.	Integraal crisisplan
Crisisteam	6.	Inventariseert uit te voeren werkzaamheden en draagt zorg voor afstemming met ICT leverancier en de functionaris voor gegevensbescherming.	
	7.	Neem bij calamiteiten met acute of voorziene knelpunten voor de zorgcontinuïteit contact op met de GHOR, hulpdiensten en/of overheid.	Integraal crisisplan
	8.	Draagt continu zorg voor in- en externe communicatie cf. beleid.	Integraal crisisplan



Protocol

Pagina 3 van 3

Betreft: Revisie:	Cyberterrorisme 0	Document: Uitgifte datum:	PR-35 25-10-2024
----------------------	-----------------------------	------------------------------	---------------------

Wie		Wat	Waarmee
Bestuurder	9.	Draagt zorg voor continue afstemming met in- en externe relevante betrokkenen, inzake voortgang en verwachte oplossing.	
	10.	Draagt zorg voor inschatting situatie en draagt eindverantwoordelijkheid voor beslissing naar escalatiefase 'Groen'.	
Crisisteam	11.	Opstellen van een plan voor herstel.	Herstelplan
	12.	Draagt zorg voor in- en externe communicatie cf. Beleid, inzake de-escalatie crisis.	Integraal crisisplan
	13.	Draagt zorg voor nazorgactiviteiten richting cliënten, medewerkers en overige betrokkenen.	Integraal crisisplan
	14.	Draagt zorg voor evaluatie crisis.	

4. Registratie

Document	Verantwoordelijke	Bewaarplaats	Bewaartermijn
Integraal crisisplan	Bestuurder	Op locatie en digitaal	Zolang actueel