Term	Afkorting	Betekenis
Kantoorautomatisering	KA	Hiermee bedoelen we het geheel aan fysieke, digitale en organisatorische infrastructuurvoorzieningen die nodig zijn om het functioneren van het kantoor en de daar werkzame medewerkers te ondersteunen. Kantoorautomatisering omvat de werkplek (laptop en AVD), applicatielaag KA met office en bassiapplicaties zoals notepad en 7-zip en daarnaast is ook het lokale netwerk en printvoorziening op het zwartewoud een onderdeel
Azure Virtual Desktop	AVD	De gevirtualiseerde werkplek op het Microsoft Azure platform die benaderbaar is door medewerkers zonder GGD GHOR device.
Authenticatie		Proces van verifieren van de identiteit van een gebruiker, apparaat of systeem om toegang te verlenen tot gevoelige gegevens en systemen.
Back-up		Afzonderlijke middelen om een functie te garanderen voor het maken en bewaren van kopieën van gegevens om deze te kunnen herstellen in geval van verlies of beschadiging.
Beschikbaarheid		Het vermogen van een systeem of dienst om operationeel te blijven en toegankelijk te zijn wanneer nodig.
BIV-classificatie	BIV	Het classificeren van informatie op basis van beschikbaarheid, integriteit en vertrouwelijkheid, vaak op een vijfpuntsschaal.
Cloud (computing)		Het op aanvraag (via een netwerk) beschikbaar stellen van gedeelde, configureerbare IT-resources - zoals netwerken, servers, opslag, applicaties en diensten - die snel en met minimale beheerinspanningen kunnen worden uitgerold. Kenmerken van de Cloud zijn self-service (op aanvraag), schaalbaarheid, toegankelijkheid, resource pooling (verdelen van IT middelen over grote groepen gebruikers) en gemeten dienstverlening en facturering op basis van gebruik.
Clouddienst		Een IT-dienst die via Cloud computing wordt geleverd; SaaS, PaaS en IaaS zijn in dit verband verschillende typen (service modellen) van Cloud computing. Het betreft in dit kader expliciet alleen zogenaamde Public Clouddiensten.
Cloudprovider		De entiteit die via het internet Clouddiensten levert, zoals SaaS, PaaS of IaaS. In het OCF geadresseerd als Leverancier.
Datacenters		Faciliteiten die IT-apparatuur huisvesten en beheren, waaronder servers en opslag.
Dataherstel		Het proces waarbij gegevens - na verlies of beschadiging - worden hersteld.
Dataminimalisatie		Beginsel van het verzamelen, bewaren of anderszins verwerken van slechts de minimale hoeveelheid Persoonsgegevens die nodig is voor een specifiek doel.
Digitale gegevensopslag		Het bewaren van gegevens in digitale vorm, zoals op harde schijven, SSD's, of cloudopslag.
Disaster recovery		Het proces voor en de procedures rondom het herstellen van cruciale IT-systemen, infrastructuren en/of data na een verstoring of calamiteit om de bedrijfscontinuïteit te waarborgen.
Documenten		Schriftelijke of elektronische records die informatie bevatten.
Elektronisch communicatienetwerk		Netwerk dat elektronische communicatie mogelijk maakt, zoals internet en intranet.
European Union Agency for Cybersecurity (Enisa)	Enisa	EU-agentschap dat zich - door middel van het bieden van richtlijnen en tools - op het beschermen van burgers en bedrijven tegen cyberdreigingen richt.
European Telecommunications Standards Institute (ETSI)	ETSI	Onafhankelijke Europese non-profit standaardisatieorganisatie (ESO) ie zich richt op de ontwikkeling en het testen van wereldwijde technische standaarden voor ICT-systemen, -toepassingen en -diensten.
Event logging		Het proces van het registreren van gebeurtenissen in een systeem voor monitoring en analyse.
Functieprofielen		Beschrijvingen van de verantwoordelijkheden en vereisten van specifieke functies binnen een organisatie, hetgeen duidelijkheid schept over de specifieke rollen en verantwoordelijkheden van medewerkers die betrokken zijn bij het beheer, de ontwikkeling en de beveiliging van cloudomgevingen.
Functionele Regie Organisatie	FRO	Voor GGD GHOR Nederland gewenste organisatievorm, waarbij niet-kritische voorzieningen worden uitbesteed en waarbij GGD GHOR Nederland dit aanstuurt op basis van Functionele Regie.
Fysieke beveiligingscontroles		Maatregelen die fysieke toegang tot IT-apparatuur en gegevens beperken.
Gebruikers-ID's		Unieke identificatoren die aan gebruikers worden toegewezen om toegang tot systemen en diensten te beheren.
Gebruikerstoegangsverleningsprocedure		Procedures voor het toekennen en beheren van toegang tot systemen en gegevens voor gebruikers.

Gegevens		De gegevens die verwerkt worden via de Clouddienst die wordt geleverd conform de V-classificatie
Gegevensuitwisseling		Het proces van het delen van gegevens tussen systemen of organisaties.
Gegevensverlies		Het verlies van gegevens door bijvoorbeeld technische storingen, menselijke fouten, of cyberaanvallen.
Hybrid Cloud		Een hybrid cloud is een samenstelling van 2 of meer afzonderlijke cloudinfrastructuren (private, community of public). Deze blijven unieke entiteiten, maar zijn met elkaar verbonden door gestandaardiseerde of bedrijfseigen technologie die overdraagbaarheid van gegevens en toepassingen mogelijk maakt (bijv. cloud bursting voor het verdelen van de belasting tussen clouds).
Industriestandaard		Formeel vastgestelde, algemeen aanvaarde normen, specificaties of richtlijnen die binnen een bepaalde sector of markt worden toegepast om consistentie en kwaliteit te waarborgen.
Informatiebeveiligingsincidenten		Gebeurtenissen die de veiligheid van informatie bedreigen, zoals datalekken of cyberaanvallen.
Infrastructure as a Service (IaaS)	IaaS	Een service model van Cloud computing, waarbij de Cloudprovider de fysieke infrastructuur (die in de Cloud draait) zoals servers, opslag en netwerken host. Cloudprovider biedt gebruikers daarmee een infrastructuur die zij naar eigen behoefte kunnen configureren en beheren. Voorbeelden zijn Amazon Web Services, Microsoft Azure en Google Cloud Platform.
Integriteit		Het beschermen van informatie tegen ongeoorloofde wijziging, vernietiging of verlies en het waarborgen van de authenticiteit en volledigheid van gegevens, met als doel te voorkomen dat gegevens op ongeautoriseerde of onopgemerkte wijze worden gewijzigd.
Interoperabiliteit		Het vermogen van twee of meer dataruimten of communicatienetwerken, systemen, verbonden producten, toepassingen, dataverwerkingsdiensten of componenten om gegevens uit te wisselen en te gebruiken teneinde hun functies te vervullen.
Kwetsbaarheidsbeheer		Het proces van het identificeren, beoordelen, en mitigeren van kwetsbaarheden in systemen.
Landelijke Beheer Organisatie	LBO	Mogelijk beoogde nieuwe en/ of bestaande ZBO organisatie die gespecialiseerd is in het managed beheer van (ICT/IV) Producten en Diensten. GGD GHOR Nederland is een Verenigings- en/ of Projectenbureau, is geen ZBO en is als zodanig niet gespecialiseerd in managed beheer.
Mandaatregister		Een register waarin mandaten en bevoegdheden binnen een organisatie worden bijgehouden.
Marktpraktijk		Geheel aan handelswijzen, gedragingen, procedures en normen (best practices) die gangbaar zijn binnen een bepaalde sector of markt.
Multi-factor authenticatie		Een beveiligingsproces waarbij meer dan één verificatiemethoden wordt gebruikt om de identiteit van een gebruiker te bevestigen.
Netwerksegregatie		Het scheiden van netwerkcomponenten om de veiligheid en prestaties te verbeteren.
Noodcontactpersoon		Een persoon die verantwoordelijk is voor het coördineren van responsactiviteiten tijdens noodsituaties.
Patchbeheer		Het proces van het updaten en beveiligen van software door patches toe te passen.
Patiëntgegevens		Gegevens die betrekking hebben op de gezondheid en medische geschiedenis van patiënten.
Persoonlijke gezondheidsinformatie		Gegevens die betrekking hebben op de gezondheid van individuen en die vertrouwelijk moeten worden behandeld.
Persoonsgegevens		Gegevens als bedoeld in artikel 4 lid 1 AVG.
PII-principals		Principes voor het beheren en beschermen van persoonlijk identificeerbare informatie (PII).
Platform as a Service (PaaS)	PaaS	Een service model van Cloud computing, waarbij de Cloudprovider de onderliggende infrastructuur, inclusief netwerk, servers, opslag en besturingssystemen host. Cloudprovider biedt gebruikers daarmee een platform waarop zij hun eigen applicaties kunnen ontwikkelen, testen, uitvoeren en beheren. Voorbeelden zijn Google App Engine en Microsoft Azure App Service.
Private cloud(dienst)		Implementatiemodel met een cloudomgeving die is ingericht voor exclusief gebruik door één organisatie, bestaande uit meerdere interne gebruikers en/of bedrijfseenheden. De infrastructuur kan worden beheerd door de organisatie zelf of door een derde partij. Voornoemde infrastructuur kan zich op locatie (on-premise) of extern (off-premise) bevinden.
Publieke cloud(dienst)		Implementatiemodel en een cloudomgeving die openlijk beschikbaar is voor algemeen gebruik door meerdere gebruikers. De infrastructuur kan eigendom zijn van, beheerd en/of geëxploiteerd worden door een bedrijf, academische instelling, overheidsorganisatie of een combinatie hiervan. Voornoemde infrastructuur bevindt zich (on-premise) op locatie van de
Redundantie		Redundantie is een onderdeel van het aspect Beschikbaarheid, het ziet op het voorkomen van 'single points of failure' door te zorgen dat er altijd een reserveproces of systeem klaar staat om de uitval op te vangen.

Software as a Service (SaaS)	SaaS	Een service model van Cloud computing, waarbij de Cloudprovider op cloudinfrastructuur draaiende softwaretoepassingen host. Cloudprovider biedt gebruikers daarmee software die zij lokaal niet hoeven te installeren, de Cloudprovider beheert namelijk alles, inclusief de applicatie, data, runtime, operating systems, servers, opslag en netwerken. Voorbeelden zijn Google Workspace, Microsoft Office 365 en Salesforce.
Tenant-isolatie		Het scheiden van gegevens en resources van verschillende gebruikers binnen een gedeelde omgeving.
Testprotocol		Procedures en richtlijnen voor het testen van systemen en applicaties.
Toegangs(beheers)rechten		Processen en mechanismen die worden gebruikt om te bepalen wie toegang heeft tot welke bronnen en onder welke omstandigheden. Dit omvat het toewijzen, beheren en controleren van toegangsrechten (op basis van Functieprofielen), om ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot gevoelige informatie.
Toegangsrechten		Specifieke rechten of permissies die een gebruiker of systeem heeft om toegang te krijgen tot bepaalde bronnen of informatie, zoals lees-, schrijf- of uitvoeringsrechten. Deze rechten kunnen worden toegewezen op basis van Functieprofielen, die de verantwoordelijkheden, taken en vereiste vaardigheden voor een specifieke functie binnen de organisatie beschrijven.
Toeleveranciers		Onderaannemers en/of 'sub contractors', zoals maar niet beperkt tot verwerkers en (sub-)verwerkers in de zin van de AVG.
eIDAS		EU-Verordening, die een kader biedt voor elektronische identificatie en vertrouwensdiensten voor elektronische transacties binnen de Europese interne markt
Uitvalsduur		De tijdsduur waarin een systeem of dienst niet beschikbaar is.
Utility program		programma dat algemene, vaak benodigde diensten biedt voor computergebruikers en onderhoudspersoneel
Vertrouwelijkheid		Het waarborgen dat gegevens alleen toegankelijk zijn voor geautoriseerde personen en dat informatie niet beschikbaar of bekend wordt gemaakt aan onbevoegde personen, entiteiten of processen.
V-classificatie		Classificatie van vertrouwelijkheid van gegevens conform de indeling van GGD GHOR (zie schema hiernaas)
Verwerking		Verwerking als bedoeld in artikel 4 lid 2 AVG.
Woo-verzoeken	Woo	Wet open overheid. Een verzoek tot openbaarmaking van informatie aan een publiekrechtelijke instelling zoals beschreven in artikel 4.1 van de Woo
Gemeentelijke Gezondsheidsdienst	GGD	gemeentelijke gezondheidsdienst, gemeentelijke geneeskundige dienst, geneeskundige gezondheidsdienst of gemeenschappelijke gezondheidsdienst is de dienst waarover elke gemeente in nederland volgens de wet dient te beschikken om een aantal taken op het gebied van de publieke gezondheid uit te voeren. De GGD'en vormen samen met de GHOR-organisaties de leden van GGD GHOR Nederland.
Verwerkersovereenkomst	VWO	Een verwerkersovereenkomst is een overeenkomst tussen een verwerkingsverantwoordelijke en een verwerker. Deze overeenkomst is verplicht volgens de Algemene Verordening Gegevensbescherming bij het uitbesteden van de verwerking van persoonsgegevens
Provisioning		Provisioning is het proces van het voorbereiden en inrichten van IT-infrastructuur en het verlenen van toegang aan gebruikers en systemen.
GGD GHOR Nederland	GGN	GGD GHOR Nederland is de belangenbehartiger voor de publieke gezondheid en veiligheid in Nederland en de overkoepelende brancheorganisatie van de 25 GGDén en GHOR-bureaus.
Carve out		Een carve-out is een overname van een bedrijfsactiviteit uit een groter bedrijf of geheel naar een andere of nieuwe entiteit
Configuratie Management Database	CMDB	Database die wordt gebruikt voor het beheren, documenteren, koppelen en volgen van configuratie-items (CI's) gedurende de levenscyclus van bijvoorbeeld een product, computersysteem of software.
Chief Information Officer	CIO	MT-lid die verantwoordelijk is voor de IT-strategie en de algehele informatievoorziening.
Chief Information Security Officer	CISO	Sr. Leidinggevende die verantwooordelijk is voor de algehele informatiebeveiliging
Commercial Of The Shelf software	COTS	Standaard Software-applicaties die op basis van licenties kunnen worden afgenomen en direct worden gebruikt
Data Lake		Een datalake is een gecentraliseerde opslagplaats die grote hoeveelheden data, zowel gestructureerd als ongestructureerd, in hun oorspronkelijke, onbewerkte formaat opslaat. Dit maakt het mogelijk om verschillende soorten data te analyseren en te gebruiken voor diverse doeleinden, waaronder het leveren van datasets, datafeeds, datadashboards en rapportages.
Kantoor Netwerkomgeving		Hiermee bedoelen we het geheel van met elkaar verbonden computers, servers, randapparatuur en communicatiesystemen binnen een kantooromgeving zoals LAN, WiFI e.d. bij GGD GHOR NL

Kantoorinfrastructuur		Hiermee bedoelen we het geheel aan fysieke, digitale en organisatorische infrastructuurvoorzieningen die nodig zijn om het functioneren van het kantoor en de daar werkzame medewerkers te ondersteunen.
Kantoor Cloudhosting		Hiermee bedoelen we het geheel van aanbieden en gebruiken van kantoorsoftware, dataopslag en rekenkracht via externe servers in de cloud, zodat medewerkers altijd en overal veilig toegang hebben tot hun digitale werkplek en applicaties.
Virtuele werkplekken	AVD	Hiermee bedoelen we een digitale werkomgeving die via internet toegankelijk is en waarin medewerkers vanaf elke locatie en elk apparaat (Bring Your Own Device BYOD) veilig toegang hebben tot hun applicaties, bestanden en communicatiemiddelen alsof zij op kantoor werken.
Fysieke werkplekken		Hiermee bedoelen we hetzelfde als de medewerkers virtuele werkplek, met als verschil dat ook de hardware (laptop, tablet, randapparatuur) ter beschikking wordt gesteld. Voorts geldt de regel binnen GGD GHOR NL dat medewerkers óf een virtuele werkplek hebben, of een fysieke. Het wordt niet toegestaan van beide typen werkplek gebruik te maken.
Managed End User Services		Dit wordt ook wel Managed Workplace Services genoemd. Hiermee bedoelen we IT-diensten waarbij het beheer, de ondersteuning en de optimalisatie van de fysieke en virtuele digitale werkplekken van eindgebruikers uitbesteed worden aan een gespecialiseerd dienstverlener.
Managed Workplace Services		Dit wordt ook wel Managed End-user Services genoemd. Hiermee bedoelen we IT-diensten waarbij het beheer, de ondersteuning en de optimalisatie van de fysieke en virtuele digitale werkplekken van eindgebruikers uitbesteed worden aan een gespecialiseerd dienstverlener.
OSINT	OSINT	Open Source Intelligence = Het geheel van verzamelen, analyseren en gebruiken van publiek beschikbare informatie en databronnen om inzicht te krijgen in personen, organisaties, dreigingen of risicovolle situaties.
MXDR	MXDR	Managed eXtended Detection & Response - Een outsourcing-model waarbij een externe dienstverlener (Managed Security Service Provider - MSSP) de XDR-omgeving van een organisatie beheert. Dit omvat 24/7 monitoring, diepgaande dreigingsanalyse en actieve incidentrespons door gespecialiseerde security-engineers.
Zero Trust		Een strategisch cybersecurity-raamwerk gebaseerd op het principe "never trust, always verify". Het gaat ervan uit dat er geen impliciet vertrouwen wordt toegekend aan assets of gebruikers op basis van hun fysieke of netwerklocatie. Elke toegangsaanvraag moet expliciet worden geverifieerd via strikte identiteitscontrole en het principe van least privilege.
UEBA	UEBA	User and Endpoint Behaviour Analytics - Een proces dat grote hoeveelheden data analyseert om een baseline van normaal gedrag vast te stellen voor gebruikers en entiteiten (zoals apparaten en applicaties). Door middel van statistische analyses en algoritmen worden significante afwijkingen gedetecteerd die kunnen wijzen op insider threats of gecompromitteerde accounts.
SOAR	SOAR	Security Orchestration, Automation & Respons - Een softwarestack die organisaties in staat stelt om beveiligingsdata te verzamelen en taken te automatiseren via playbooks. SOAR integreert verschillende beveiligingstools om de workflow van het Security Operations Center (SOC) te stroomlijnen en de reactietijd bij incidenten (MTTR) te verkorten.
XDR	XDR	eXtended Detection and Respons - Een SaaS-gebaseerde beveiligingsbenadering die detectie- en responstechnologieën integreert over meerdere beveiligingslagen heen (endpoints, netwerk, cloud en e-mail). XDR correleert data uit deze verschillende bronnen om complexe dreigingen sneller te identificeren en de context van een aanval volledig in kaart te brengen.
EDR	EDR	Endpoint Detection & Respons - Een beveiligingsoplossing die continu toezicht houdt op endpoints (zoals workstations, servers en mobiele apparaten). Het verzamelt gegevens over systeemactiviteiten en gebruikt geavanceerde analyse om afwijkend gedrag te detecteren, incidenten te onderzoeken en geautomatiseerde responsacties uit te voeren.
NDR	NDR	Network Detection and Respons - Een technologie die gebruikmaakt van non-intrusive netwerkanalyse (vaak via machine learning) om kwaadaardige patronen in het netwerkverkeer te identificeren. NDR richt zich op het detecteren van post-compromise activiteiten, zoals lateral movement en data-exfiltratie, die traditionele firewalls kunnen passeren.