Begrippenlijst behorende bij de informatienota “Informatiebeveiliging ENSIA 2024”

Afkorting/ Begrip	Voluit	Omschrijving
BAG	Basisregistratie Adressen en Gebouwen	De BAG bevat gemeentelijke basisgegevens van alle adressen en gebouwen in een gemeente.
BCP	BedrijfsContinuïteitPlanning	BCP is het proces van het ontwikkelen van plannen om de kritieke bedrijfsactiviteiten te waarborgen tijdens en na een verstoring of crisis.
BGT	Basisregistratie Grootschalige Topografie	De BGT is een digitale kaart van Nederland waarop gebouwen, wegen, waterlopen, terreinen, spoorlijnen etc eenduidig zijn vastgelegd
BIO	Baseline Informatiebeveiliging Overheid	Met ingang van 2020 heeft de BIO alle eerdere sectorale normenkaders vervangen rondom informatiebeveiliging. Hierdoor is de BIO het gezamenlijke normenkader voor alle overheidslagen.
BIO2.0	Baseline Informatiebeveiliging Overheid versie 2	Met ingang van Q3/Q4 2025 zal de BIO2.0 in werking gaan. Deze geeft invulling aan de zorgplicht in de Cyberbeveiligingswet en is een sterke afgeleide van de wereldwijde beveiligingsnorm ISO27001/2.
BRO	Basisregistratie Ondergrond	De BRO bevat een breed scala aan informatie over de ondergrond.
BRP	Basisregistratie Persoonsgegevens	De BRP bevat persoonsgegevens van inwoners van Nederland (ingezetenen) en van personen die Nederland hebben verlaten.
CBW	Cyberbeveiligingswet	De Cyberbeveiligingswet (CBW) is een Nederlandse implementatie van de Europese NIS2-richtlijn en verplicht vitale en belangrijke organisaties om passende maatregelen te nemen voor cybersecurity en ernstige incidenten te melden aan de toezichthouder
CISO	Chief Information Security Officer	Binnen een organisatie is de CISO verantwoordelijk voor het informatiebeveiligingsbeleid. Dit betreft zowel het implementeren van beleid als het toezicht houden op de uitvoering ervan.
DigiD	Digitale Identiteit	DigiD is een systeem waarmee Nederlandse overheden op internet iemands identiteit kunnen verifiëren.
ENSIA	Eenduidige Normatiek Single Information Audit	De ENSIA is het sinds 2017 jaarlijks verplichte verantwoordingsproces op informatiebeveiliging bij gemeenten.
GAP-analyse		Een GAP-analyse is een methode waarmee je inzichtelijk maakt waar je nu staat (huidige situatie) en waar je naartoe wilt (gewenste situatie), om zo de verschillen (de ‘gaps’) te identificeren en gericht verbeteracties te formuleren.

Dit document is geclassificeerd als intern

Begrippenlijst behorende bij de informatienota “Informatiebeveiliging ENSIA 2024”

Afkorting/ Begrip	Voluit	Omschrijving
ISMS	Information Security Management System	Een ISMS (Information Security Management System) is een systematische aanpak waarmee een organisatie beleid, processen en maatregelen beheerst om informatiebeveiliging continu te verbeteren en risico’s te beheersen volgens bijvoorbeeld de ISO 27001-norm
ISO27001/2	International Organization for Standardization	De ISO 27001/27002 is een internationale norm voor informatiebeveiliging die organisaties helpt bij het opzetten (27001) en invullen (27002) van een beheerssysteem om vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen
IoT	Internet of Things	IoT verwijst naar een netwerk van fysieke apparaten die via internet met elkaar verbonden zijn en automatisch gegevens verzamelen, uitwisselen en soms zelfstandig acties uitvoeren
KRT	Kernregistratie Topografie	De KRT is een interne databron binnen onze organisatie waarin alle geografische objecten van de gemeente Lelystad zijn geregistreerd
NIS2	Network and Information Security directive	NIS2 is een Europese richtlijn die organisaties in vitale en belangrijke sectoren verplicht om strengere maatregelen te nemen op het gebied van cybersecurity en incidenten tijdig te melden aan de toezichthouder
PUN	Paspoort Uitvoerings-regeling Nederland	De Paspoort Uitvoeringsregeling Nederland bevat de operationele regels en procedures voor de aanvraag, productie, uitgifte en beheer van paspoorten en identiteitskaarten in Nederland
RDI	Rijksinspectie Digitale Infrastructuur	De Rijksdienst voor Digitale Infrastructuur is de uitvoeringsorganisatie van het Rijk die toezicht houdt op digitale veiligheid, waaronder als nationale toezichthouder voor de overheid onder de NIS2, en verantwoordelijk is voor de betrouwbaarheid van vitale digitale infrastructuur
Suwinet	Suwi-netwerk	Suwinet is een digitale infrastructuur die is ontwikkeld door en om ervoor te zorgen dat, de Suwipartijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak
	<einde overzicht>	

Dit document is geclassificeerd als intern