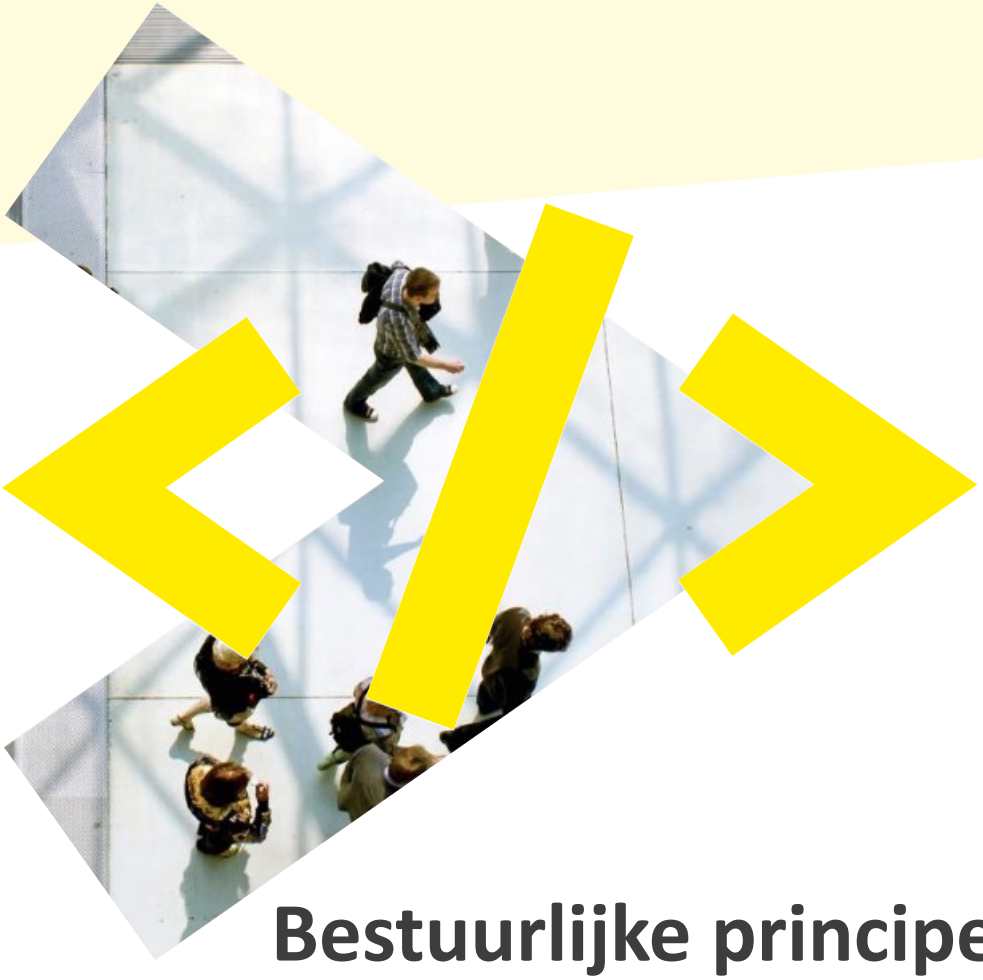
Behorende bij het Informatieclassificatieraamwerk van de Vlaamse overheid

Vlaamse overheid



Bestuurlijke principes voor Informatieveiligheid

Versie: maart 2023

Bron: CIP Nederland

Doelgroep: Leidend ambtenaren

DIGITAAL VLAANDEREN

Voor een **veilige** digitale overheid

Eigenaarschap is verantwoordelijkheid voelen en nemen als een goede huisvader/-moeder

DIGITAAL VLAANDEREN

Het thema Informatieveiligheid is de laatste jaren steeds belangrijker geworden door de toegenomen digitalisering van de maatschappij. We worden afhankelijker van informatietechnologie en de daarmee gepaarde kwetsbaarheden en dreigingen.

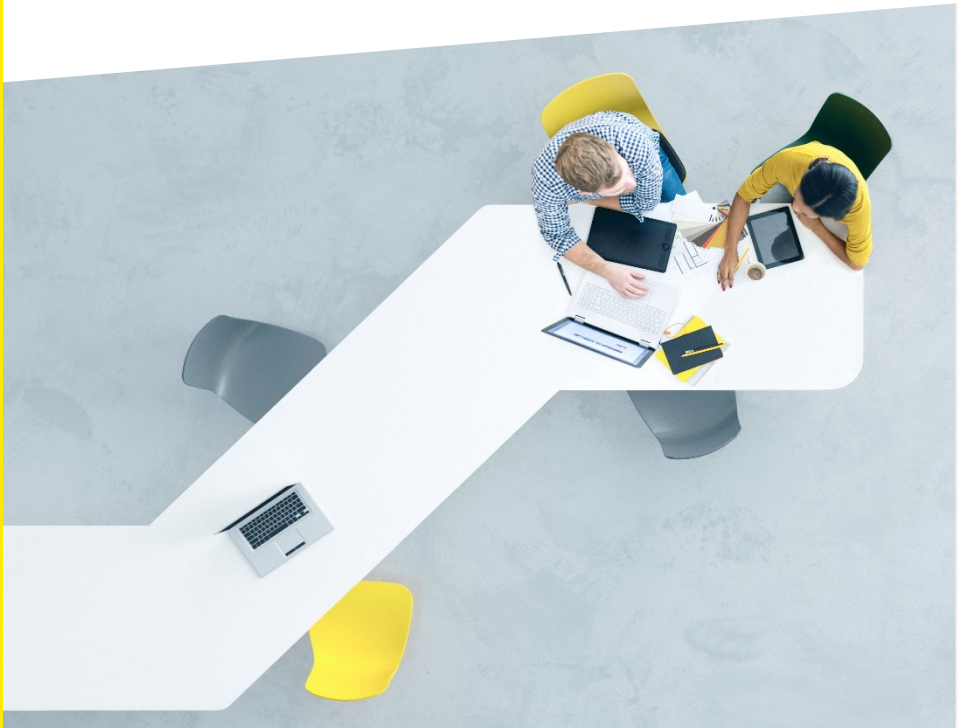
De overheid verzamelt en verwerkt meer en meer gevoelige data van burgers, bedrijven en organisaties om haar publieke opdracht te kunnen vervullen. Maar ook om de wensen van gebruikers met een meer gepersonaliseerde en geautomatiseerde dienstverlening te beantwoorden. De samenleving verwacht dat de overheid zorgvuldig met die informatie omgaat en ze adequaat beschermt.

Permanente aandacht voor Informatieveiligheid binnen de Vlaamse overheid is van kritisch belang voor het succes van een veilige digitale samenleving en moet breed gedragen en verankerd worden in de bestuurdersverantwoordelijkheid van leidend ambtenaren en directiecomités.

Het vakgebied van de Informatieveiligheid wordt overspoeld door vakjargon. Over het algemeen behoort dit taalgebruik niet tot de spontane parate kennis van een bestuurder.

Deze flyer bevat acht principes die helpen bij het invullen van eigenaarschap en de leidende rol die worden verwacht van een leidend ambtenaar.

De doelgroep van deze flyer zijn leidend ambtenaren en security officers of informatieveiligheidsconsulenten. Dit is een informatief instrument om te helpen bij het afstemmen van de verwachtingen rond eigenaarschap in interactie met de leidend ambtenaar.



Raadpleeg het Informatieclassificatie raamwerk voor meer informatie **via deze QR:**

Bron: CIP Nederland

DIGITAAL VLAANDEREN

De 8 bestuurlijke principes voor Informatieveiligheid

Bewustzijn	U zorgt ervoor dat er regelmatig bewustmaking campagnes worden uitgevoerd, gericht op alle medewerkers van uw organisatie. Dit om het bewustzijn rond veiligheidsrisico's te vergroten.
Veilige cultuur	U bevordert een open en veilige cultuur waarin medewerkers zich vrij voelen om risico's en incidenten te melden. Zodat er doeltreffend kan worden gereageerd en er een lerende organisatie ontstaat.
Eigenaarschap	U bevordert eigenaarschap van, en verantwoordelijkheid voor, Informatieveiligheid op alle niveaus binnen de organisatie van topkader en middenkader tot en met het lager kader en uitvoerende medewerkers.
Budget	U stelt voldoende budget en middelen beschikbaar voor de ontwikkeling, het onderhoud en de uitvoering van het Informatieveiligheidsbeleid.
Organisatie	U stelt een verantwoordelijke aan die een organisatie ondersteunende rol heeft bij de uitvoering van het informatieveiligheidsbeleid. Dit kan een Security Officer, veiligheidsconsultent of equivalent zijn.
Proces	U richt Informatieveiligheid in als een cyclisch, herhalend en terugkerend proces met duidelijke regels en hulpmiddelen voor risicoanalyses, de implementatie van beheersmaatregelen, de beoordeling en acceptatie van (rest)risico's en rapportering.
Keten-samenwerking	U zorgt ervoor dat er regelmatig afstemming is met samenwerkingspartners en leveranciers over Informatieveiligheid en beheersmaatregelen om risico's op een acceptabel niveau te brengen en te houden.
Controleren en evalueren	U voert regelmatig controle en evaluatie uit op directieniveau om inzicht te krijgen in de mate waarop het Informatieveiligheidsbeleid en informatierisicobeheer is verankerd in de organisatie. U garandeert hierbij regelmatige bijsturing.

Bron: CIP Nederland