1. Veiligheid

IRMA-E4	Veiligheid
Stelling	Informatie en dienstverlening zijn veilig en beschermd tegen misbruik, verlies en ongeautoriseerde toegang. Veiligheid van informatie is structureel geborgd in ontwerp, gebruik en beheer
Beschrijving	Informatie van de overheid moet in eerste instantie openbaar en toegankelijk zijn, anderzijds moeten er restricties worden opgelegd aan informatie met het oog op onder meer privacy. Ook mogen mensen die hiertoe geen recht hebben geen toegang hebben tot informatie, om te voorkomen dat er onjuist gebruik gemaakt kan worden van de informatie. Dit geldt met name voor de informatie van burgers.
Rationale	Met persoonsgegevens, medische gegevens, enz. moet dan ook zorgvuldig worden omgegaan. Deze informatie mag bijvoorbeeld niet langer bewaard worden dan noodzakelijk en moet tijdig vernietigd worden. Ook mogen enkel de mensen die hiertoe recht hebben toegang tot de informatie verkrijgen. Dit geldt niet alleen voor de informatie, maar ook voor de metadata en registraties. Er mag niet via een omweg alsnog herleidbaar zijn wat, wanneer een persoon gedaan heeft (dit geldt eveneens voor registraties en backups). Ook informatie gebruiken voor andere doeleinden dan waarvoor de informatie is aangeleverd of opgemaakt moet worden voorkomen, tenzij er expliciet toestemming is gegeven hiervoor.
Implicaties	Er moet bij elk proces helder zijn wie toegang mag hebben tot de informatie. Bij veel processen gelden er restricties omdat er wordt gewerkt met (gevoelige) privé informatie. Hier moeten autorisaties goed zijn geregeld. Er zijn meerdere gradaties van autorisaties wanneer er restricties zijn aan informatie; autorisaties op het niveau van een ketenproces, autorisaties op het niveau van een werkproces en autorisaties op het niveau van één of meerdere personen binnen een werkproces. Denk bijvoorbeeld aan het beroepsgeheim van een arts, waarbij de informatie van een patiënt slechts ingezien mag worden door de behandelend arts. Naast autorisaties betreft vernietiging een belangrijk aspect met betrekking tot veiligheid. Er kan geen oneigenlijk gebruik gemaakt worden van (gevoelige) informatie wanneer deze tijdig en correct vernietigd is.
Voorwaarden	Autorisaties, Openbaarheid, Vernietiging
Wettelijke onderbouwing	**Archiefbesluit *(Artikel 13, Lid 2)*:** “De zorgdrager beveiligt zijn archiefruimten en archiefbewaarplaatsen op toereikende wijze tegen brand, inbraak en wateroverlast”
	Archiefwet *(Artikel 17, Lid 2)*: “De beheerder is bevoegd een verzoek tot raadpleging of gebruik van archiefbescheiden af te wijzen, indien naar zijn oordeel de toestand van de archiefbescheiden zich daartegen verzet of deze aan de verzoeker niet veilig kunnen worden toevertrouwd“
	Archiefwet *(Artikel 25a, Lid 4)*: “Indien een toezichthouder […] een ruimte betreedt waarin […] archiefbescheiden worden bewaard […] neemt hij de voorschriften ten aanzien van de beveiliging van geheimen in acht”

Samengevat:

Veiligheid binnen IRMA betekent dat informatie en dienstverlening zijn beschermd tegen misbruik, verlies en ongeautoriseerde toegang. Dit wordt structureel geborgd in ontwerp, gebruik en beheer via passende autorisaties, zorgvuldige omgang met (gevoelige) informatie en tijdige vernietiging, zodat privacy wordt beschermd en informatie alleen wordt gebruikt door bevoegden en voor het juiste doel.

From:
https://irma.denhaag.nl/ - **IRMA**

Permanent link:
https://irma.denhaag.nl/veiligheid

Last update: **2026/04/17 09:44**