

CERTIFICERINGSSHEMA 2018

INFORMATIEBEVEILIGING EN PRIVACY ROSA

Versiebeschrijving en definities

DATUM	22 maart 2018
VERSIE	2018
AUTEUR	Edustandaard werkgroep IBP

De licentie op het certificeringsschema is CC BY 4.0 (Attribution 4.0 International, <https://creativecommons.org/licenses/by/4.0/>). Dit betekent in eenvoudige termen dat je vrij bent om het werk te delen en te bewerken, mits je bronvermelding toepast. Let wel op dat het certificeringsschema specifiek is ontworpen voor de educatieve keten.

VERSIEBESCHRIJVING

Het certificeringsschema bestaat uit meerdere documenten. Omdat informatiebeveiliging en privacy continu in ontwikkeling zijn moeten deze ook regelmatig worden bijgewerkt. Daarom is gekozen voor een bepaalde aanpak voor versiebeheer.

Alle documenten worden gedurende het jaar meermaals bijgewerkt. Eenmaal per jaar wordt een versie vastgesteld van het certificeringsschema. Deze krijgt als versieaanduiding het jaartal. Deze versiebeschrijving geeft aan welke versie van de onderliggende documenten daarbij hoort.

Deze versie van het certificeringsschema is vastgesteld in de Standaardisatieraad op 22 maart 2018 en bestaat uit de volgende versies:

Document	Type	Vastgestelde versie	Meest recente versie
Algemene beschrijving	Tekstdocument	2.05	-
Proces	Tekstdocument	2.05	-
Classificatie	Spreadsheet	2.0	2.01
Toetsingskader	Spreadsheet	1.2	-
Toezicht	Tekstdocument	2.05	-

GELDIGHEID

Tijdens de toetsing moet gebruik gemaakt worden van de meest recente versie die op dat moment is goedgekeurd. Wanneer bijvoorbeeld certificeringsschema 2018 in maart 2018 is goedgekeurd, dient vanaf die datum versie 2018 gebruikt te worden totdat versie 2019 is goedgekeurd.

Omdat alle documenten na goedkeuring ook meermaals worden bijgewerkt wordt aangeraden om de meest recente versie van de documenten te gebruiken. Iedere organisatie is echter vrij om alleen de versies te gebruiken die in de versiebeschrijving staan.

DEFINITIES

De volgende definities worden gehanteerd in deze versie van het certificeringsschema:

Term	Definitie	Bron
Beschikbaarheid	<p>De mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening waarborgen.</p> <p>Deelaspecten hiervan zijn:</p> <ul style="list-style-type: none"> - Continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is. - Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructures gewaarborgd is. - Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden. 	BIR/NOREA
Integriteit	<p>De mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.</p> <p>Deelaspecten hiervan zijn:</p> <ul style="list-style-type: none"> - Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd. - Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is. - Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd. 	BIR/NOREA
Vertrouwelijkheid	<p>De mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.</p> <p>Deelaspecten hiervan zijn:</p> <ul style="list-style-type: none"> - Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is. - Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is. - Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn. 	BIR/NOREA

	<ul style="list-style-type: none">- Periodieke controle op de bestaande bevoegdheden.- Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.	

Definitie toevoegen of aanpassen

Wanneer een definitie ontbreekt of niet klopt kan een verzoek worden ingediend bij de werkgroep IBP door contact op te nemen met Bureau Edustandaard via info@edustandaard.nl.

REFERENTIES

De volgende externe bronnen worden gebruikt in het certificeringsschema:

Organisatie	Omschrijving	Link
OWASP	De OWASP logging cheat sheet beschrijft best practices rondom logging maatregelen	https://www.owasp.org/index.php/Logging_Cheat_Sheet
NCSC	ICT-beveiligingsrichtlijnen voor mobiele apps	https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-mobiele-apps.html
NCSC	ICT-beveiligingsrichtlijnen voor Webapplicaties	https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html
NIST	Digital Identity Guidelines	https://pages.nist.gov/800-63-3/
ENISA	ENISA's opinion paper on encryption	https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption/view