**Certificeringsschema IBP ROSA**

**(Classificatiekader mbo)**

****

**IBPDOC19**

Verantwoording

**Bron:**

**ROSA**

*Augustus 2016*

**ROSA**

ROSA is de Referentie Onderwijs Sector Architectuur, de referentiearchitectuur voor het onderwijsdomein die zich richt op informatieketens en (onderwijs) sector overstijgende aspecten van informatievoorziening. De ROSA heeft als doel de informatievoorziening binnen het onderwijsdomein te optimaliseren. Hiervoor is samenwerking tussen organisaties essentieel. Scholen, de overheid en derden werken in toenemende mate samen in ketens, een goede informatie-uitwisseling is hierbij essentieel.

**Bewerkt door:**

Kennisnet / saMBO-ICT

**Auteurs**

Leo Bakker (Kennisnet)

Ludo Cuijpers (Kennisnet)

Axel Eissens (Kennisnet)

Versie 1.01, juni 2018

**Sommige rechten voorbehouden**

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgever van Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.

**Creative commons**

Naamsvermelding 3.0 Nederland

(CC BY 3.0)

**De gebruiker mag:**

* Het werk kopiëren, verspreiden en doorgeven
* Remixen – afgeleide werken maken

**Onder de volgende voorwaarde:**

* Naamsvermelding – De gebruiker dient bij het werk de naam van Kennisnet te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

**Inhoudsopgave**

[1. Classificatiekader voor breed gebruik 5](#_Toc493838880)

[**1.1** **Verantwoording** 5](#_Toc493838881)

[**1.2** **Toelichting BIV classificatie** 5](#_Toc493838882)

[**1.3** **Classificatie-aspecten: BIV** 6](#_Toc493838883)

[**1.4** **Doelstelling classificatieproces: classificatie en maatregelen** 6](#_Toc493838884)

[**1.5** **Uitgangspunten** 6](#_Toc493838885)

[**1.6** **Concrete aanpak** 7](#_Toc493838886)

[**1.7** **Gehanteerde classificatie <MBO INSTELLING>** 8](#_Toc493838887)

[**1.8** **Classificatie van data binnen de <MBO INSTELLING>** 9](#_Toc493838888)

[**1.9** **Toelichting op de tabel.** 9](#_Toc493838889)

[**1.10** **Technische ondersteuning** 10](#_Toc493838890)

[2. Classificatiekader voor ICT medewerkers 11](#_Toc493838891)

[**2.1** **Toelichting toetsingskader** 11](#_Toc493838892)

[**2.2** **Relatie tussen het certificeringsschema en andere normenkaders** 14](#_Toc493838893)

[**2.3** **Aanvullende opmerking** 14](#_Toc493838894)

[Bijlage 1: ROSA classificatiekader 15](#_Toc493838895)

[1. Beschikbaarheid midden 15](#_Toc493838896)

[**1.1** **NOREA definitie** 15](#_Toc493838897)

[**1.2** **Beheersmaatregelen (controls)** 15](#_Toc493838898)

[**1.3** **Technische en procesmatige realisatie** 15](#_Toc493838899)

[**1.3.1** **Overbelasting** 15](#_Toc493838900)

[**1.3.2** **Business continuity** 15](#_Toc493838901)

[**1.3.3** **Backup/ restore/ recovery** 15](#_Toc493838902)

[**1.3.4** **Single points of failure** 16](#_Toc493838903)

[**1.3.5** **Software** 16](#_Toc493838904)

[**1.3.6** **Logging / monitoring / testen** 16](#_Toc493838905)

[**1.3.7** **Actuele dreigingen (DDoS, ransomware)** 16](#_Toc493838906)

[2. Beschikbaarheid hoog 17](#_Toc493838907)

[**2.1** **NOREA definitie** 17](#_Toc493838908)

[**2.2** **Beheersmaatregelen (controls)** 17](#_Toc493838909)

[**2.3** **Technische en procesmatige realisatie** 17](#_Toc493838910)

[**2.3.1** **Overbelasting** 17](#_Toc493838911)

[**2.3.2** **Business continuity** 17](#_Toc493838912)

[**2.3.3** **Backup/ restore/ recovery** 17](#_Toc493838913)

[**2.3.4** **Single points of failure** 17](#_Toc493838914)

[**2.3.5** **Software** 18](#_Toc493838915)

[**2.3.6** **Logging / monitoring / testen** 18](#_Toc493838916)

[**2.3.7** **Actuele dreigingen (DDoS, ransomware)** 18](#_Toc493838917)

[3. Integriteit laag 19](#_Toc493838918)

[**3.1** **NOREA definitie** 19](#_Toc493838919)

[**3.2** **Beheersmaatregelen (controls)** 19](#_Toc493838920)

[**3.3** **Technische en procesmatige realisatie** 19](#_Toc493838921)

[**3.3.1** **Herleidbaarheid** 19](#_Toc493838922)

[**3.3.2** **Functiescheiding** 19](#_Toc493838923)

[**3.3.3** **Application controls** 19](#_Toc493838924)

[**3.3.4** **Manual controls** 19](#_Toc493838925)

[**3.3.5** **Onweerlegbaarheid** 19](#_Toc493838926)

[**3.3.6** **Actuele dreigingen (DDoS, ransomware)** 19](#_Toc493838927)

[4. Integriteit midden 20](#_Toc493838928)

[**4.1** **NOREA definitie** 20](#_Toc493838929)

[**4.2** **Beheersmaatregelen (controls)** 20](#_Toc493838930)

[**4.3** **Technische en procesmatige realisatie** 20](#_Toc493838931)

[**4.3.1** **Herleidbaarheid** 20](#_Toc493838932)

[**4.3.2** **Functiescheiding** 20](#_Toc493838933)

[**4.3.3** **Application controls** 20](#_Toc493838934)

[**4.3.4** **Manual controls** 20](#_Toc493838935)

[**4.3.5** **Onweerlegbaarheid** 20](#_Toc493838936)

[**4.3.6** **Actuele dreigingen (DDoS, ransomware)** 21](#_Toc493838937)

[5. Integriteit hoog 22](#_Toc493838938)

[**5.1** **NOREA definitie** 22](#_Toc493838939)

[**5.2** **Beheersmaatregelen (controls)** 22](#_Toc493838940)

[**5.3** **Technische en procesmatige realisatie** 22](#_Toc493838941)

[**5.3.1** **Herleidbaarheid** 22](#_Toc493838942)

[**5.3.2** **Functiescheiding** 22](#_Toc493838943)

[**5.3.3** **Application controls** 22](#_Toc493838944)

[**5.3.4** **Manual controls** 22](#_Toc493838945)

[**5.3.5** **Onweerlegbaarheid** 22](#_Toc493838946)

[**5.3.6** **Actuele dreigingen (DDoS, ransomware)** 23](#_Toc493838947)

[6. Vertrouwelijkheid laag 24](#_Toc493838948)

[**6.1** **NOREA definitie** 24](#_Toc493838949)

[**6.2** **Beheersmaatregelen (controls)** 24](#_Toc493838950)

[**6.3** **Technische en procesmatige realisatie** 24](#_Toc493838951)

[**6.3.1** **Levenscyclus gegevens** 24](#_Toc493838952)

[**6.3.2** **Fysieke toegang** 24](#_Toc493838953)

[**6.3.3** **Logische toegang** 24](#_Toc493838954)

[**6.3.4** **Opslag en transport** 25](#_Toc493838955)

[**6.3.5** **Logging / auditing** 25](#_Toc493838956)

[**6.3.6** **Actuele dreigingen (DDoS, ransomware)** 25](#_Toc493838957)

[7. Vertrouwelijkheid midden 26](#_Toc493838958)

[**7.1** **NOREA definitie** 26](#_Toc493838959)

[**7.2** **Beheersmaatregelen (controls)** 26](#_Toc493838960)

[**7.3** **Technische en procesmatige realisatie** 26](#_Toc493838961)

[**7.3.1** **Levenscyclus gegevens** 26](#_Toc493838962)

[**7.3.2** **Fysieke toegang** 26](#_Toc493838963)

[**7.3.3** **Logische toegang** 26](#_Toc493838964)

[**7.3.4** **Opslag en transport** 26](#_Toc493838965)

[**7.3.5** **Logging / auditing** 27](#_Toc493838966)

[**7.3.6** **Actuele dreigingen (DDoS, ransomware)** 27](#_Toc493838967)

[8. Vertrouwelijkheid hoog 28](#_Toc493838968)

[**8.1** **NOREA definitie** 28](#_Toc493838969)

[**8.2** **Beheersmaatregelen (controls)** 28](#_Toc493838970)

[**8.3** **Technische en procesmatige realisatie** 28](#_Toc493838971)

[**8.3.1** **Levenscyclus gegevens** 28](#_Toc493838972)

[**8.3.2** **Fysieke toegang** 28](#_Toc493838973)

[**8.3.3** **Logische toegang** 28](#_Toc493838974)

[**8.3.4** **Opslag en transport** 29](#_Toc493838975)

[**8.3.5** **Logging / auditing** 29](#_Toc493838976)

[**8.3.6** **Actuele dreigingen (DDoS, ransomware)** 29](#_Toc493838977)

[**Bijlage: Framework informatiebeveiliging en privacy in het mbo** 30](#_Toc493838978)

# Classificatiekader voor breed gebruik[[1]](#footnote-1)

## Verantwoording

Binnen het onderwijs vervult ict een belangrijke rol. Op verschillende manieren wordt gebruik gemaakt van ict-toepassingen voor onderzoek, onderwijs of onderwijsondersteunende producten en diensten. De aard en inhoud van deze ict-toepassingen kunnen onderling sterk verschillen, maar zij hebben als gemeenschappelijk kenmerk dat de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevensbewerking cruciaal is. Ook de toegenomen aandacht en strengere wetgeving rondom privacy dwingt alle partijen in de onderwijsketen expliciet aandacht te besteden aan informatiebeveiliging en privacy (IBP).

Daarom hebben ketenpartijen in het onderwijsdomein gezamenlijk het ‘certificeringsschema informatiebeveiliging en privacy ROSA’ opgesteld. Deze standaard is onderdeel van de Referentie Onderwijs Sector Architectuur (ROSA) en wordt binnen Edustandaard beheerd door de werkgroep Informatiebeveiliging & Privacy, afgekort IBP. Deze werkgroep bestaat uit IBP-specialisten uit de onderwijsketen en vertegenwoordigt zowel onderwijs als leveranciers. Via deze werkgroep kunnen alle partijen in de onderwijsketen invloed uitoefenen op de inhoud van de standaard.

De <MBO INSTELLING> hanteert deze standaard. Indien, om praktische redenen, wordt afgeweken van deze landelijke standaard dan wordt dat nadrukkelijk aangegeven.

Dit classificatiekader is geschreven in het kader van de nieuwe Europese Privacywetgeving Privacy wetgeving ‘Algemene Verordening Gegevensbescherming’, afgekort (AVG),die op 25 mei 2016 gestart is en op 25 mei 2018 door de <MBO INSTELLING> moet zijn geïmplementeerd. Dit kader is ook goed bruikbaar voor de classificatie van systemen en processen.

## Toelichting BIV classificatie

De Open Universiteit streeft naar een goede balans tussen het optimaal gebruik van ict-middelen enerzijds en het borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van data[[2]](#footnote-2) anderzijds. Deze doelstellingen kunnen enkel bereikt worden met een gedegen uitgevoerde classificatie – en beleid – op functioneel, technisch en organisatorisch vlak.

Classificatie helpt bij:

* een veilige onderzoek- leer- en werkomgeving;
* een goed imago;
* in control zijn;
* naleving van wetgeving, zoals Algemene Verordening Gegevensbescherming (AVG).

Classificatie van data helpt bij:

* het selecteren van maatregelen die genomen moeten worden om data adequaat te beschermen, de integriteit te waarborgen en de beschikbaarheid te optimaliseren;
* het vergroten van de alertheid van de organisatie met betrekking tot de waarde van data en beveiligingsrisico’s.

Data, ook op papier, worden in de praktijk verwerkt binnen één of meerdere onderzoek-, onderwijs- en bedrijfsprocessen en op één of meer systemen/applicaties. Deze context wordt dan ook bij de classificatie betrokken.

## Classificatie-aspecten: BIV[[3]](#footnote-3)

Het beschermingsniveau van data wordt getoetst aan de kwaliteitscriteria Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).

**Beschikbaarheid:** de mate waarin de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening gewaarborgd wordt.

Deelaspecten hiervan zijn:

* 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 infrastructuren gewaarborgd is;
* Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

**Integriteit:** de mate waarin de juistheid, volledigheid en tijdigheid van de IT-dienstverlening gewaarborgd wordt.

Deelaspecten hiervan zijn:

* 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 (actualitieit): de mate waarin de correcte werking van de IT-processen is gewaarborgd.

**Vertrouwelijkheid:** 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.

Deelaspecten hiervan zijn:

* 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;
* Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de juiste autorisaties hebben.

## Doelstelling classificatieproces: classificatie en maatregelen

Classificatie geeft een inschatting van de gevoeligheid en het belang van de data om tot een juiste mate van beveiliging te komen. Niet alle data zijn even vertrouwelijk of moeten bij een incident even snel weer beschikbaar te zijn. Het is niet erg efficiënt of gebruiksvriendelijk om niet vertrouwelijke data op dezelfde manier te beschermen als vertrouwelijke data.

## Uitgangspunten

* Alle data (persoonsgegevens) categorieën hebben een eigenaar.
* De (gemandateerd) eigenaar bepaalt de classificatie (het vereiste beschermingsniveau) en welke restrisico’s aanvaardbaar zijn.[[4]](#footnote-4)
* De Functionaris Gegevensbescherming, afgekort FG controleert of classificatie in overeenstemming is met de geldende wet en regelgeving. De eigenaar is en blijft eindverantwoordelijk voor de classificatie.
* De IBP manager, in afstemming met eigenaren, applicatiebeheerders en ICT, bepaalt wat bij het beschermingsniveau passende beveiligingsmaatregelen zijn.
* Er wordt gestreefd naar een verantwoord, maar zo passend mogelijk classificatieniveau; overbodig hoge classificatie leidt tot onnodige drempels en kosten. Te lage classificatie leidt tot teveel potentiele risico’s.
* De IBP manager beheert het register van alle classificatierapporten en initieert de periodieke review door de eigenaar.

## Concrete aanpak

De <MBO INSTELLING> heeft voor de volgende aanpak gekozen om te komen tot de classificatie van data:

* Allereerst is de governance vastgesteld. Leidend in de classificatie is, bijvoorbeeld, de eigenaar van een categorie persoonsgegevens (deelverzameling van de data). Een directeur wordt aangewezen door de Verwerkersverantwoordelijke (Voorzitter CvB) als gemandateerde Verwerkersverantwoordelijke voor de categorie “Medewerkers in loondienst”.
* Samen met de IBP manager en ICT verantwoordelijken bepaalt hij namens de “business” de classificatie van de Categorieën van de persoonsgegevens.

Bijvoorbeeld:

|  |  |
| --- | --- |
| **B** | **Categorie:****Medewerkers****in loondienst** |
| **D** | **Categorieën van persoonsgegevens** | **BIV****classificatie** |
|
| 1 | **Contactgegevens (Beperkte set = naam, e-mail en organisatorische eenheid, code X b)** | M-H-M |
| 2 | **Personeelsnummer** | M-H-M |
| 3 | **Nationaliteit en geboorteplaats** | M-H-M |
| 4 | **Medische gegevens** (op eigen verzoek) | M-H-M |
| 5 | **Godsdienst** (op eigen verzoek) | M-H-M |
| 6 | **Ervaringen** (werkervaringen en opleidingen) | M-H-M |
| 7 | **R&O gesprekken** (Resultaat en ontwikkeling) | M-H-**H** |
| 8 | **Financiën** (inclusief de financiële cyclus) | M-H-M |
| 9 | **Beeldmateriaal** | M-H-**H** |
| 10 | **Overige gegevens** | M-H-M |
| 11 | **BSN** | M-H-**H** |

* Eventueel wordt gebruik gemaakt Certificeringsschema classificatie (beschikbaar op de R-drive-projecten-AVG). Op basis van ingevulde antwoorden wordt dan een classificatie voorgesteld.
* De classificatie wordt getoetst door de FG in zijn rol van toezichthouder.

## Gehanteerde classificatie <MBO INSTELLING>[[5]](#footnote-5)

**B**eschikbaarheid

De mate waarin de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening gewaarborgd wordt.

**Midden:** de hersteltijd is maximaal 24 uur voor servers, applicaties en data en 48 uur voor het netwerk.

**Hoog:** de hersteltijd is maximaal 8 uur voor servers, applicaties en data en 24 uur voor het netwerk[[6]](#footnote-6).

**I**ntegriteit

De mate waarin de volledigheid, juistheid en actualiteit van de IT-dienstverlening gewaarborgd wordt. **Laag:** Volledigheid, alle gevraagde data zijn ingevuld.

 Bijvoorbeeld de postcode (4 cijfers en 2 letters), de geboortedatum (12 januari 1991).

**Midden:** Juistheid, een medewerker van de <MBO INSTELLING> controleert of de gegevens juist zijn.

 Bijvoorbeeld klopt de postcode (controle middels **B**asis **R**egistratie **P**ersonen), klopt de naam (controle d.m.v. ID).

**Hoog:** Actualiteit, een medewerkers van de <MBO INSTELLING>, bijvoorbeeld een medewerker van de salarisadministratie, toetst of de medewerker nog steeds in dienst is binnen de <MBO INSTELLING>.

**V**ertrouwelijkheid

De mate waarin uitsluitend geautoriseerde personen gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.
Deelaspecten hiervan zijn:

* Identificatie: wie bent u?
* Authenticiteit: toon aan dat u het bent (wachtwoord of pasje).
* Autorisatie: welke bevoegdheden heeft u?
* Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.
* Periodieke controle op de bestaande bevoegdheden.

**Laag:** toegang tot diensten en faciliteiten op basis van aanstellingsovereenkomst (netwerk, e-mail, etc.).

**Midden:** toegang op basis van rol of functie (bijvoorbeeld: medewerkers mogen cijfers invoeren van studenten op basis van de autorisatiematrix).

**Hoog:** toegang alleen op basis van persoonlijke rechten (bijvoorbeeld: een medewerker, leidinggevende en andere aangewezen personen hebben toegang tot een bepaald personeelsdossier). Ook andere data (dus geen persoonsgegevens) kunnen als hoog worden geclassificeerd, denk aan wetenschappelijk onderzoek, aanbestedingen, etc.

## Classificatie van data binnen de <MBO INSTELLING>

De volgende dataclassificatie wordt binnen de <MBO INSTELLING> gehanteerd:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nr.** | **Categorie** | **B** | **I** | **V** | **Uitzonderingen** |
| **1** | **Medewerkers in loondienst** | M | H | M |  |
|  | M | H | **H** | R&O gesprekken |
|  | M | H | **H** | Beeldmateriaal |
|  | M | H | **H** | BSN |
| **2** | **Extern personeel** (incl. data bij aanbestedingen) **als gevolg van opdrachten** (commercieel) | M | M | M |  |
| **3** | **Extern personeel als gevolg van samenwerking** (niet commercieel) | M | H | M |  |
| **4** | **Personen die meewerken aan Wetenschappelijk onderzoek en enquêtes** | M | H | H |  |
| **5** | **Belangstellenden** | H | L | M |  |
| **6** | **Studenten** | H | H | M |  |
|  | H | H | **H** | Medische gegevens studenten |
| **7** | **Alumni** | M | M | M |  |
| **8** | **Ouders, voogden en bewindvoerders** | M | H | M |  |

## Toelichting op de tabel.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nr.** | **Categorie** | **B** | **I** | **V** | **Uitzonderingen** |
| 1 | **Medewerkers in loondienst** | M | H | M |  |

Voor de categorie medewerkers in loondienst is gekozen voor de **Beschikbaarheid** midden (M). Met andere woorden als er een verstoring van de informatievoorziening optreedt dan garandeert de <MBO INSTELLING> een hersteltijd van maximaal 24 uur voor servers, applicaties en data en 48 uur voor het netwerk.

Als gekozen zou worden voor hoog (H) dan zou dat extra kosten meebrengen.

De **Integriteit** van de persoonsgegevens van de Medewerkers in loondienst is hoog (H). De gegevens zijn volledig, juist en actueel. Doordat de accountant meekijkt (goedkeuring op de jaarrekening) is het ondenkbaar dat er medewerkers in loondienst bij de <MBO INSTELLING> rondlopen die ten onrechte salaris ontvangen en waarbij verkeerde gegevens worden gedeeld met de belastingdienst en het ABP.

**Bijvoorbeeld:**

|  |  |  |
| --- | --- | --- |
| **Integriteit** | **Beheersmaatregel (control)** | **Toelichting** |
| **Integriteit** **laag** | **Application controls en business rules**Hierdoor wordt de medewerker gedwongen om volgens een vast format data in te voeren in een digitaal invulformulier.**De data zijn volledig.** | Stel er moeten 10 data (naam, postcode, geboortedatum, etc.) worden ingevoerd dan dwingt de applicatie om alle gegevens op een bepaalde manier in te typen. Bijvoorbeeld postcode moet bestaan uit 4 cijfers en 2 letters. De geboortedatum kan alleen worden aangeklikt worden op dag (keuze 1 t/m 31), maand (januari t/m december) en jaar (1930 t/m 2017).De gegevens zijn dus volledig, maar hoeven niet juist te zijn. Immers de medewerker kan de verkeerde geboortedatum hebben aangeklikt. |
| **Integriteit midden** | **Manual control**Menselijke of machinale (koppeling met controle bestanden, zoals GBA) controle.**De data zijn volledig en juist.** | Een medewerker van de <MBO INSTELLING> (personeelsadministratie) controleert of de data kloppen aan de hand van overlegde bewijzen (paspoort, ID, diploma, etc.) |
| **Integriteit hoog** | **Meervoudige manual controls**Meerdere medewerkers en applicaties controleren de data.**De data zijn volledig, juist en actueel.** | Maandelijks wordt het salaris overgemaakt naar de medewerker. Meerdere medewerkers van de <MBO INSTELLING> controleren de actualiteit van de data. Zo wordt vastgesteld of de medewerkers nog steeds werkt binnen de <MBO INSTELLING> en niet ziek is geweest, etc. |

De **Vertrouwelijkheid** van de meeste persoonsgegevens (data) van medewerkers in loondienst wordt geclassificeerd op midden (M). Concreet betekent dit dat medewerkers van de salarisadministratie en consulenten op basis van hun rol gegevens mogen invoeren die leiden tot de uitbetaling van het salaris. Een medewerker van de <MBO INSTELLING> weet dus niet wie zijn/haar gegevens, om te komen tot een salarisuitbetaling, heeft ingevoerd. Hij/zij weet wel welk functie dit mag doen.

Dit is anders als het gaat om de RenO gesprekken. Hier geldt een **Vertrouwelijkheid** hoog (H). De medewerker deelt vertrouwelijke persoonsgegevens met zijn leidinggevende en moet er dan ook van uit kunnen gaan dat niet 20 collega’s het verslag kunnen lezen. Technische en organisatorische maatregelen moeten dit dan ook onmogelijk maken. Denk daarbij aan een extra wachtwoord of aan versleutelde documenten.

## Technische ondersteuning

De BIV classificatie wordt bepaald door de gemandateerde beheerder van de data (bijvoorbeeld een directeur). Om deze classificatie mogelijk te maken moet er achter de schermen nog een en ander technisch geregeld worden. De volgende hoofdstukken gaan daar dieper op in en veronderstellen dan ook een redelijk technisch ICT kennis.

# Classificatiekader voor ICT medewerkers

## Toelichting toetsingskader

Het toetsingskader bestaat de kwaliteitscriteria Beschikbaarheid, Integriteit en Vertrouwelijkheid. Voor elk van deze aspecten moet de <MBO INSTELLING> maatregelen[[7]](#footnote-7) treffen.

De maatregelen zijn uitgewerkt op 3 niveaus (beschikbaarheid op 2 niveaus): Laag, Midden en Hoog. Dit classificatiekader beschrijft concrete maatregelen voor een ict-toepassing per kwaliteitscriterium. Daarbij geldt:

* De maatregelen beperken zich nadrukkelijk tot het technisch domein.
* De maatregelen moeten op basis van het comply-or-explain principe worden beoordeeld.
* Maatregelen op het gebied van organisatie en proces zijn momenteel buiten scope van het classificatiekader gelaten, het is echter wel mogelijk dat maatregelen op het gebied van organisatie en proces, maatregelen op technisch niveau overbodig maken.

Ter illustratie een overzicht van mogelijke maatregelen per kwaliteitscriterium (deze worden gedetailleerd in de bijlage verder uitgewerkt:

**B**eschikbaarheid maatregelen

|  |  |  |  |
| --- | --- | --- | --- |
|   | **Bedreigingen** | **Midden**  | **Hoog** |
| **1** | **Overbelasting** | Regulering en maatregelen | Zie midden |
| **2** | **Business continuity** | Er is een 'Warm Standby' aanwezig. | Er is een 'Hot Standby' aanwezig. |
| **3** | **Backup/ restore/ recovery** | Backup verplicht, minimaal dagelijks.Recovery test= 2x per jaar. | Backup verplicht, minimaal dagelijks.Recovery test= 4x per jaar. |
|  |  | **Hersteltijd:**Netwerk:Servers:Applicaties:Data: | 48 uur24 uur24 uur (RTO)[[8]](#footnote-8)24 uur (RPO) | **Hersteltijd:**Netwerk:Servers:Applicaties:Data: | 24 uur8 uur8 uur (RTO)8 uur (RPO) |
| **4** | **Single points of failure** | Single points of failures zijn niet toegestaan in ketens | Zie midden |
| **5** | **Software / hardware** | Patchen en updates van firmware en software zijn ingeregeld en worden periodiek uitgevoerd. | Zie midden |
| **6** | **Logging / monitoring / testen** | Onbeschikbaarheid en afname van performance wordt gemeten en geregistreerd / gelogd. | Onbeschikbaarheid en afname van performance wordt gemeten en geregistreerd / gelogd.Er is aantoonbaar actieve monitoring, testing en rapportage van performance. |
| **7** | **Actuele dreigingen (DDoS, ransomware).** | Risico die optreden door bijvoorbeeld antivirus, anti-malware, intrusion detection worden spoedig gedetecteerd. | Actieve bescherming tegen aanvallen (hardening van servers, et cetera) |

**I**ntegriteit maatregelen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Bedreigingen** | **Laag** | **Midden** | **Hoog** |
| **1** | **Herleidbaarheid** | Mogelijkheid tot correctie. | Herleidbaar *wie, wanneer, welke* gegevens/configuraties gewijzigd heeft. | Zie midden. |
| **2** | **Functiescheiding** | Functiescheiding niet noodzakelijk.  | Goedkeuring door een tweede persoon is noodzakelijk.  | Functiescheiding noodzakelijkGoedkeuring door meerdere personen is noodzakelijk. |
| **3** | **Application controls** | Controle of alle noodzakelijke gegevens zijn ingevuld. | Verschillende groepen van informatie of diensten, gebruikers en informatiesystemen moeten gescheiden worden op het netwerk. | Zie midden |
| **4** | **Manual control** | Regelmatige rapportage over aantal fouten (onvolledige gegevens). | Bevestiging/verificatie van de gebruiker (bijvoorbeeld handtekening of actieve handeling).Handmatige controle/verificatie (bijvoorbeeld bij paspoort). | Bevestiging/verificatie van een derde (van de ketenpartij zelf of externe partij). |
| **5** | **Onweerlegbaarheid** | **Logging is optioneel.**Gelogd wordt:* handelingen van beheerders.
 | **Logging is verplicht.** Gelogd wordt:* handelingen van beheerders;
* beveiligingsovertredingen.
 | **Logging is verplicht.**Gelogd wordt:* handelingen van beheerders;
* beveiligingsovertredingen;
* verstoringen van het productieproces;
* handelingen van gebruikers.
 |
| **6** | **Actuele dreigingen (DDoS, ransomware)** | Bij ransomware is rollback mogelijk naar een gecontroleerde situatie korter dan **48** uur geleden. | Bij ransomware is rollback mogelijk naar een gecontroleerde situatie korter dan **24** uur geleden. | Bij ransomware is rollback mogelijk naar een gecontroleerde situatie korter dan **8** uur geleden. |

**Vertrouwelijkheid maatregelen**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Bedreigingen** | **Laag** | **Midden** | **Hoog** |
| **1** | **Levenscyclus gegevens** | Er wordt invulling gegeven aan wettelijke bewaartermijnen.De data moet gewist worden van de af te voeren apparatuur. | De data moet gewist en overschreven worden (met random data) voordat de apparatuur afgevoerd mag worden. | Op apparatuur die wordt hergebruikt of de organisatie verlaat wordt data onherstelbaar vernietigd.Informatie in deze categorie wordt altijd gelabeld. |
| **2** | **Fysieke toegang** | Fysieke toegangscontrole middels toegangspas of sleutel. Informatie mag op iedere locatie gebruikt / bewerkt worden, exclusief door medewerkers van de organisatie. | Fysieke toegangscontrole middels toegangspas met extra privileges.Informatie blijft binnen locaties van de organisatie of technische partners.Informatie is toegankelijk voor een beperkte groep mensen binnen de organisatie. | Fysieke toegangscontrole middels toegangspas is aangevuld met pincode, biometrische verificatie of soortgelijke oplossingen.Informatie blijft binnen locaties van de organisatie, of technische partners met een certificering op het gebied van informatiebeveiliging welke regelmatig wordt gecontroleerd. |
| **3** | **Logische toegang** | Toegangscontrole tot infrastructuur componenten.Alleen geautoriseerde personen hebben toegang | Authenticatie/autorisatie afhankelijk van locatie gebruiker:* Binnen eigen locaties: Gebruikersnaam en wachtwoord.
* Vanaf buiten eigen locaties: Gebruikersnaam en wachtwoord en tweede factor.
 | Authenticatie/autorisatie afhankelijk van locatie gebruiker:* Binnen eigen locaties: Gebruikersnaam en wachtwoord.
* Vanaf buiten eigen locaties: Gebruikersnaam en wachtwoord en tweede factor.
 |
| **4** | **Opslag en transport** | Beperkte encryptie van opslag en transport. | Altijd encryptie van opslag en transport. | Altijd encryptie van opslag en transport.PKI infrastructuur met externe en vertrouwde CA. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **5** | **Logging / auditing** | Logging is enkel toegankelijk voor bevoegde personen.Integriteit van logbestanden is gewaarborgd tegen ongeautoriseerde wijzigingen. | **Overeenkomstig ‘Laag’ met als aanvulling+**Handelingen van beheerders moeten worden gelogd en traceerbaar zijn naar individuele personen. | **Overeenkomstig ‘Midden’ met als aanvulling+**Logging moet regelmatig worden gecontroleerd op rechtmatigheid van toegang en gebruik.Audits vinden periodiek (minimaal jaarlijks) plaats.  |
| **6** | **Actuele dreigingen (DDoS, ransomware)** | Bewustzijn van medewerkers over actuele dreigingen en het werken met data. | Je bent in staat om spoedig te detecteren of een risico optreedt door bijvoorbeeld antivirus, anti-malware, intrusion detection. | Actieve bescherming tegen aanvallen (hardening van servers, et cetera). |

## Relatie tussen het certificeringsschema en andere normenkaders

De standaarden ISO 27001 en ISO 27002 zijn internationaal algemeen geaccepteerde standaarden voor een betrouwbare informatieverwerking; ze zijn in 2017 overgenomen als Europese norm. ISO 27001 is een standaard die beschrijft hoe een organisatie procesmatig met het beveiligen van data kan omgaan, met als doel om de vertrouwelijkheid, beschikbaarheid en integriteit van data zeker te stellen. Een organisatie die ISO 27001 gecertificeerd is heeft aangetoond de omgang met informatiebeveiliging goed te hebben ingericht. Er zijn adequate processen, procedures, werkinstructies om voor de organisatie informatiebeveiligingsrisico’s te identificeren en daar afdoende maatregelen op te nemen. Een organisatie bepaalt daarbij zelf wat de scope is van de certificering, is de hele organisatie gecertificeerd of bijvoorbeeld alleen de beheerafdeling. Ook bepaalt een organisatie zelf wat de belangrijkste risico’s zijn en of daar maatregelen op worden genomen of dat (een deel van) het risico wordt geaccepteerd.

ISO 27002 kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en effectieve methoden voor het bereiken van deze veiligheid.

## Aanvullende opmerking

De <MBO INSTELLING> maakt geen gebruik van de Beschikbaarheidsclassificatie laag (L). Deze is dan ook niet uitgewerkt.

## Bronnen

Bovenstaande classificatieschema is volledig gebaseerd op het standaard model (certificeringsschema) van Edustandaard, ook wel het ROSA classificatieschema genoemd. Meer informatie hierover is te vinden op:

<https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/>

**Bijlage: Framework informatiebeveiliging en privacy in het mbo**



1. **Certificeringsschema,** Informatiebeveiliging en Privacy ROSA, 29 mei 2017 [↑](#footnote-ref-1)
2. Data: waaronder persoonsgegevens [↑](#footnote-ref-2)
3. Bron NOREA [↑](#footnote-ref-3)
4. Afwijkend van SCIPR [↑](#footnote-ref-4)
5. Kwaliteitscriteria NOREA zijn beperkt aangepast om leesbaarheid te vergroten. [↑](#footnote-ref-5)
6. In het week end afwijkend. [↑](#footnote-ref-6)
7. **Deze technische maatregelen zijn uitgewerkt in nauw overleg met de “technische” collega’s van de <MBO INSTELLING>. De volgende hoofdstukken zijn dus alleen prettig leesbaar voor collega’s met een technische achtergrond.** [↑](#footnote-ref-7)
8. RTO en RPO zie pagina 13 en 14 voor de toelichting. [↑](#footnote-ref-8)