****

**Strategie**

Security Nederland

**Versiebeheer**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versie** | **Status** | **Datum** | **Auteur** | **Omschrijving** |
| 0.1 | Concept | 5-9-2023 | Ludo Cuijpers  Leo Jaarsma  Henk Links  Sebastiaan van Trigt | Basisdocument |
|  |  |  |  |  |

**Vastgesteld door Security Nederland:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Naam** | **Functie** |
| 1.0 |  |  | College van Bestuur |

**Sommige rechten voorbehouden**

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



Creative commons

MBO Raad 4.0 Nederland

(CC BY 4.0) **Copyright**

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 MBO Raad te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

[1. Inleiding 3](#_Toc144807477)

[**1.1.** **Informatiebeveiliging en Privacy** 3](#_Toc144807478)

[**1.2.** **Missie** 3](#_Toc144807479)

[**1.3.** **Visie in relatie tot Informatiebeveiliging en Privacy** 3](#_Toc144807480)

[2. Strategie 4](#_Toc144807481)

[**2.1.** **Strategische uitgangspunten** 4](#_Toc144807482)

[**2.2.** **Governance** 4](#_Toc144807483)

[**2.3.** **IBP-processen** 5](#_Toc144807484)

[**2.4.** **Technische weerbaarheid** 5](#_Toc144807485)

[**2.5.** **Slot en vervolg** 5](#_Toc144807486)

# Inleiding

Informatiebeveiliging en Privacy is geen opzichzelfstaand onderwerp. Het draagt bij aan een veilige leer- en werkomgeving en sluit daarmee aan op een groot aantal strategische uitgangspunten genoemd <naam strategisch plan onderwijsinstelling>.

Onze organisatie werkt veel met waardevolle en vertrouwelijke informatie en met de voortdurende ontwikkelingen op digitaal gebied is Informatiebeveiliging en Privacy een breed en complex onderwerp geworden. Het werken vanuit een visie en strategische uitgangspunten voor Informatiebeveiliging en Privacy is daarom noodzakelijk om aantoonbaar te groeien naar een professionele en veilige manier van omgaan met de beschikbaar gestelde informatie.

Dit document geeft binnen de context van de door Security Nederland benoemde strategische richting een basis om concreet en planmatig aan de slag te gaan met Informatiebeveiliging en Privacy.

* 1. **Informatiebeveiliging en Privacy**

Informatiebeveiliging en Privacy staat voor beveiliging van waardevolle informatie (Security) en bescherming van persoonsgegevens (Privacy). Security Nederland draagt hierin een grote verantwoordelijkheid.

Beschikbaarheid, Integriteit en Vertrouwelijkheid van de informatie zijn kernbegrippen.

Informatiebeveiliging en Privacy is essentieel voor:

1. De continuïteit van het onderwijsproces;
2. Kwalitatief hoogwaardig onderwijs;
3. Een veilige leer- en werkomgeving.

Informatiebeveiliging en Privacy is geen doel op zich maar draagt bij aan de volgende strategische uitgangspunten van Security Nederland:

1. Toekomstbestendig onderwijs;
2. Professionele (onderwijs)organisatie;
3. Intrinsieke leer- en verbetercultuur;
4. Een sterke organisatie.
   1. **Missie**

Security Nederland levert een bijdrage <benoem missie zoals, bijvoorbeeld, vermeld op de website van Security Nederland>.

* 1. **Visie in relatie tot Informatiebeveiliging en Privacy**

Security Nederland wil een veilige en professionele leer- en werkomgeving aanbieden en daarbij is het noodzakelijk dat de door Security Nederland verzamelde, verwerkte en gepubliceerde informatie te allen tijde beschikbaar, correct en beschermd is. Dit vraagt om een strategisch samenhangende aanpak van Informatiebeveiliging en Privacy, die aantoonbaar aan de eisen voldoet, om blijvend een veilige en toekomstbestendige leer- en werkomgeving beschikbaar te stellen.

1. **Strategie**

*BIJVOORBEELD:*

*Naar aanleiding van enkele steekwoorden uit het Instellingsplan 2023-2026. (Nooit af, Individualisering, Leven Lang ontwikkelen, Blended en hybride leren en De kwaliteitslat steeds hoger) wil de Security Nederland groeien naar een professionele organisatie, waar op een veilige manier onderwijs verzorgd en ondersteund kan worden.*

*In aansluiting hierop wil Security Nederland met een strategische aanpak op het gebied van Informatiebeveiliging en Privacy groeien naar een professioneel volwassen organisatie, waar op een veilige manier met informatie wordt omgegaan.*

*Deze strategie is richtinggevend en sluit aan bij de bovengenoemde uitgangspunten van Security Nederland, genoemd in het Instellingsplan 2023-2026.*

* 1. **Strategische uitgangspunten**

Met betrekking tot Informatiebeveiliging en Privacy onderscheiden we 3 aandachtsgebieden:

1. Governance
2. Processen
3. Technische Weerbaarheid

Hiermee hebben we het volgende op het oog:

* Iedere medewerker is verantwoordelijk voor de veiligheid van de informatie die door de organisatie beschikbaar wordt gesteld.
* Alle leidinggevenden binnen Security Nederland zien erop toe dat hun medewerkers voldoende geschoold zijn en het Informatiebeveiliging en Privacy beleid naleven.
* Het College van Bestuur is eindverantwoordelijk en moet verantwoording kunnen afleggen aan, bijvoorbeeld, de Raad van Toezicht.
* Proceseigenaren zijn benoemd en zijn bewust van hun verantwoordelijkheid bij de uitvoer van processen waar Informatiebeveiliging en Privacy een belangrijke rol speelt.
* IT is verantwoordelijk voor de technische weerbaarheid.
  1. **Governance**

De Governance gaat over het “wat en wie en met welk doel” en is gericht op de volgende thema’s:

1. Strategie: We sluiten aan bij de organisatiestrategie.
2. Beleid: We werken binnen vastgestelde kaders.
3. Architectuur: We werken vanuit een gekozen model.
4. Eigenaarschap: We benoemen rollen en verantwoordelijkheden en delen die toe.
5. Risk Management: We prioriteren op basis van een risicoanalyse.
6. Roadmap: We leggen de te nemen acties vast in de tijd en maken daar budget voor vrij.
7. Toetsing: We laten ons toetsen.

Alle te ondernemen acties in de processen en technische weerbaarheid zijn geborgd in de Governance:

**We weten wie wat doet met welk doel en in lijn met de strategische doelstellingen van de organisatie.**

Het belangrijkste doel van alle maatregelen is het mitigeren van de risico’s die we lopen op het gebied van Informatiebeveiliging en Privacy, waarmee we een veilige leer- en werk omgeving kunnen borgen.

Certificering (goedkeuring) wordt echter een steeds belangrijker onderdeel van de Governance. Een Certificering kan alleen gegeven worden door een professionele externe auditor. Vanwege recente grote veiligheidsincidenten binnen het onderwijsveld neigt het Ministerie van Onderwijs steeds meer naar een verplichte externe audit waarbij externe verantwoording steeds belangrijker wordt.

* 1. **IBP-processen**

Bij de volgende processen speelt Informatiebeveiliging en Privacy een grote rol:

1. Human Resources: betreft borging expertise en training.
2. ITIL: betreft Incident, Problem, Change, en Configuration Management en Fysieke Beveiliging.
3. Datamanagement: betreft opslag, beheer, verwijderen (bewaartermijnen) en bescherming van gegevens.
4. Identity & Access Management (IAM): betreft toegangsregels en - rechten tot informatie.
5. Security Baselines: minimale afspraken over hoe veilig te werken
6. Business Continuity: betreft opvangen van incidenten (waaronder crisismanagement).
7. Cloud Leveranciers: goede afspraken en controle daarop bij externe leveranciers.

Aan ieder proces is een proceseigenaar toegewezen en de processen zijn beschreven.

* 1. **Technische weerbaarheid**

Bij technische weerbaarheid zijn de volgende thema’s te onderscheiden:

1. Multi Factor Authenticatie/Thuiswerken: betreft veilig van buitenaf inloggen.
2. SOC SIEM: betreft 24 x 7 detectie van het netwerk (en respons).
3. Pentesten: betreft periodiek gericht testen op kwetsbaarheden in het netwerk.
4. Patchbeheer: betreft structureel bijwerken van de software (beveiligingsupdates).
5. Infrastructuur: betreft beschikbaarheid van het netwerk en systemen.
6. Security Policy: betreft inrichting technische beveiliging van het netwerk en systemen.
7. Computer Operations: betreft automatische IT-processen (bijvoorbeeld back-up).

De bovenstaande thema’s zullen uitgevoerd of onder regie uitbesteed worden door de IT-afdeling. Zij zullen hierover in begrijpelijke taal rapporteren aan het College van Bestuur. Bij deze rapportage hoort ook een financieel overzicht, zodat duidelijk is welke veiligheidsmaatregelen horen bij de gemaakt kosten/investeringen.

De thema’s Multi Factor Authenticatie/Thuiswerken, SOC SIEM en Security Policy vallen onder het zogenaamde Zero Trust principe.

* 1. **Slot en vervolg**

Deze visie op en strategische uitgangspunten van Informatiebeveiliging en Privacy zijn leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging en bescherming van de persoonsgegevens.

In het Informatiebeveiliging en privacy beleid zijn deze uitgangspunten uitgewerkt en gekaderd, zodat Security Nederland planmatig kan groeien in volwassenheid en stappen zet in de richting waar ze als organisatie voor gaat.