IBP-beleid

Strategie en visie Informatiebeveiliging en Privacy

Datum: juni 2024
Directeur-bestuurder: Peter Schutte
Vastgesteld op: 01-07-2024

Onderwijsgroep Buitengewoon

Strategie en visie Informatiebeveiliging en Privacy Onderwijsgroep Buitengewoon

1. 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 die genoemd zijn in ons Strategisch meerjarenbeleidsplan 2023 - 2026 “Samen Buitengewoon Sterk”.

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 Onderwijsgroep Buitengewoon benoemde strategische richting een basis om concreet en planmatig aan de slag te gaan met Informatiebeveiliging en Privacy.

1.1 Informatiebeveiliging en Privacy

Informatiebeveiliging en Privacy staat voor beveiliging van waardevolle informatie (Security) en bescherming van persoonsgegevens (Privacy). Onderwijsgroep Buitengewoon 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.

1.2 Missie / visie in relatie tot Informatiebeveiliging en Privacy

Onderwijsgroep Buitengewoon wil een veilige en professionele leer- en werkomgeving aanbieden en daarbij is het noodzakelijk dat de door Onderwijsgroep Buitengewoon 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. We hebben een groot netwerk op het gebied van onderwijs en onderwijsgerelateerde zorg. We zijn er namelijk van overtuigd dat we beter in staat zijn om onze ambities en doelen te realiseren, en dus meer voor onze leerlingen kunnen bereiken, door structureel samen te werken met

ketenpartners en stakeholders. Hierbij wordt informatiebeveiliging en privacy regelmatig besproken en worden hier conform wet- en regelgeving afspraken over gemaakt met onze samenwerkingspartners.

2. Strategie

2.1 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 Onderwijsgroep Buitengewoon zien erop toe dat hun medewerkers voldoende geschoold zijn en het Informatiebeveiliging en Privacy beleid naleven.
- De Aandacht Functionaris Digitalisering is nauw betrokken bij onderwijskundige ontwikkelingen en let hierbij mede op het waarborgen van informatiebeveiliging en privacy.
- De (Bovenschoolse) ICT-Coördinatoren en applicatiebeheerder zijn verantwoordelijk voor de technische weerbaarheid.
- De Functionaris Gegevensbescherming De FG heeft de volgende taken: Toezicht houden op bestaande en nieuwe (DPIA) verwerkingen van persoonsgegevens; Controleren van het verwerkings- en incidentenregister en logbestanden; Geven van (ongevraagd) advies en doen van aanbevelingen over privacy in het algemeen, vaak op basis van actuele ontwikkelingen; Overleg met (de contactpersoon van) de Autoriteit Persoonsgegevens; Jaarlijkse afstemming met de Security Officer/Bestuurder en het opstellen van een verslag van zijn werkzaamheden; Het (laten) afhandelen van klachten inzake privacy; het begeleiden en afhandelen van datalekken incl. meldingen bij de AP na overleg met verwerkingsverantwoordelijke;
- De Directeur-bestuurder is eindverantwoordelijk en legt verantwoording af aan de Raad van Toezicht.
- De Raad van Toezicht houdt toezicht op het beleid ten aanzien van Informatiebeveiliging en Privacy.

2.2. 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. Technische en Security Roadmap en Groeipad IBP: 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.

2.3. IBP-processen

Bij de volgende processen speelt Informatiebeveiliging en Privacy een grote rol:
1. Personeelsbeleid: betreffende borging, expertise en training.
2. ITIL (Information Technology Infrastructure Library): Changemanagement, Incidentmanagement, Problemmanagement, Patchmanagement, Threat- en Vulnerabilitymanagement en Configuratiemanagement.
3. Datamanagement: betreft opslag, beheer, verwijderen (bewaartermijnen) en bescherming van gegevens.
4. Identity & Access Management (IAM), toegangsbeleid: betreft regels en - rechten tot informatie. (autorisatiematrix)
5. 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. (contracten en verwerkers overeenkomsten)

2.4. Technische weerbaarheid

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

1. Veilig inloggen via Multi Factor Authenticatie
2. Periodiek gericht testen op kwetsbaarheden (bijvoorbeeld via Pentesten).
3. Bijwerken van de software (beveiligingsupdates).
4. Technische beveiliging van het netwerk en systemen. (Firewalls)
5. Automatische IT-processen (bijvoorbeeld back-up).

De bovenstaande thema's zullen uitgevoerd of onder regie uitbesteed worden door de Bovenschoolse ICT-Coördinator in samenspraak met de applicatiebeheerder en ICT-Coördinatoren en de netwerkbeheerder. De Bovenschoolse ICT-Coördinator rapporteert aan de directeur-bestuurder. Bij deze rapportage hoort ook een financieel overzicht, zodat duidelijk is welke kosten en investeringen horen bij welke veiligheidsmaatregelen.

2.5 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 Onderwijsgroep Buitengewoon planmatig kan groeien in volwassenheid en stappen zet in de richting waar ze als organisatie voor gaat.