Informatiebeveiligingsplan

Dockinga College
J.J. Boumanschool
Inspecteur Boelensschool Schiermonnikoog

DOCKINGA college
BETROKKENHEID
VERTROUWEN
RESPECT

J J Boumanschool
Chr. School voor Praktijkonderwijs

Inspecteur Boelensschool
onderwijs op maat

Voorwoord

Het Dockinga College, de J.J. Boumanschool en de Inspecteur Boelensschool Schiermonnikoog vallen elk onder een verschillend bevoegd gezag. Op het niveau van bestuur en intern toezicht is er sprake van een zogeheten personele unie: de directeur-bestuurder van het Dockinga College is tevens bestuurder van de J.J. Boumanschool en van de Inspecteur Boelensschool Schiermonnikoog (hierna te noemen: de besturen).
Om praktische redenen is er voor gekozen te gaan werken met een integraal informatiebeveiligingsplan voor de (afzonderlijke locaties van de) drie scholen.

Inleiding en wettelijk kader

Op grond van artikel 13 van de Wet bescherming persoonsgegevens zijn de besturen verplicht om passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
Deze maatregelen moeten een passend beveiligingsniveau garanderen gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.
Hierbij wordt rekening gehouden met de stand van de techniek en de kosten van de uitvoering. De maatregelen moeten er mede voor zorgen dat onnodige verzameling en verdere verwerking van persoonsgegevens wordt voorkomen.

In het voorliggende informatiebeveiligingsplan worden de maatregelen beschreven welke de besturen toepassen om te voldoen aan de wettelijke verplichtingen, mede ter uitvoering van artikel 10 van het privacyreglement van de besturen.

1 Uitgangspunten en beleidskader

1.1 Verantwoordelijkheid

Binnen de besturen worden zowel op schoolniveau als op bovenschools niveau functionarissen aangewezen die verantwoordelijk zijn voor het uitvoeren en up-to-date houden van de technische en organisatorische maatregelen die nodig zijn om persoonsgegevens te beveiligen.

1.2 Beschikbaarheid

Uitgangspunt is dat persoonsgegevens op werkdagen continu beschikbaar zijn voor de functionarissen die geautoriseerd zijn om ermee te werken.
Per locatie wordt een draaiboek opgesteld met een beschrijving van de taken, de verantwoordelijkheden en de noodzakelijke acties om bij calamiteiten de toegankelijkheid tot en de beschikbaarheid van persoonsgegevens als regel binnen 48 uur te kunnen herstellen.
Voor zover gegevens niet online toegankelijk zijn, wordt -afhankelijk van de aard en de omvang van de calamiteit- in voorkomende gevallen uitgeweken naar een ander schoolgebouw.

1.3 Incidenten

1.3.1 Incidenten op het gebied van informatiebeveiliging en privacy worden terstond gemeld en geregistreerd.

1.3.2 De medewerkers melden incidenten bij de schooldirectie en de schooldirecties melden deze bij de besturen.

1.3.3 De besturen draagt zorg voor een centrale registratie van incidenten.

1.3.4 Afhankelijk van de aard van de incidenten dragen de besturen zorg voor melding bij politie of justitie en/of bij de Autoriteit Persoonsgegevens (melding datalekken).

1.4 Bewerking

1.4.1 Als er sprake is van bewerking van persoonsgegevens in de zin van artikel 14 van de Wet bescherming persoonsgegevens dragen de besturen zorg voor een bewerkingsovereenkomst. Door middel van de bewerkingsovereenkomst wordt gewaarborgd dat de bewerker voldoet aan de wettelijke eisen, alsmede aan de beleidsuitgangspunten van de besturen.

1.4.2 Periodiek wordt door de besturen getoetst of de bewerker voldoet aan de beveiligingseisen in de overeenkomst.

1.5 Risicobewustzijn en communicatie

Om medewerkers bewust te maken en te houden, worden zij door de schooldirectie jaarlijks geïnstrueerd over mogelijks beveiligingsrisico's en de maatregelen die in dat kader door de besturen zijn genomen.

1.5.1 Instructie over beveiligingsrisico's en beveiligingsmaatregelen vormt een vast onderdeel van het introductieprogramma van nieuwe medewerkers.

1.5.2 Medewerkers worden door de schooldirectie direct aangesproken op ongewenst gedrag.

1.5.3 Ongewenst gedrag en incidenten worden besproken in de teamvergaderingen met de bedoeling daarvan collectief te leren.

1.5.4 Informatiebeveiliging en privacy maken onderdeel uit van de gesprekkencyclus met de medewerkers.

1.5.5 Periodiek worden in alle locaties door de schooldirecties en/of de bovenschoolse ICT-coördinator op een zichtbare wijze steekproefsgewijze controles uitgevoerd.

1.6 Verantwoording

1.6.1 Om te kunnen beoordelen op welke wijze wordt voldaan aan de wettelijke bepalingen en in hoeverre het informatiebeveiligingsplan wordt nageleefd, wordt door de schooldirecteuren jaarlijks gerapporteerd aan het bestuur.

1.6.2 De besturen rapporteren jaarlijks aan het intern toezichthoudend orgaan.

1.6.3 Bij ernstige incidenten wordt het intern toezichthoudend orgaan direct op de hoogte gebracht, dit ter beoordeling van de besturen.

2 Toegangsbeveiliging gebouwen

2.1 Risicoanalyse

Eens in de drie jaar laten de besturen de beveiligingssituatie van de gebouwen beoordelen door een onafhankelijke partij. De besturen stelt vast in hoeverre de uitvoering van eventuele aanbevelingen van de onafhankelijke deskundige passend is binnen de kaders van artikel 13 van de Wet bescherming persoonsgegevens.

2.2 Beveiligingsniveau

Alle persoonsgegevens, zowel de digitale gegevens als de hard-copy gegevens, worden zodanig bewaard dat er sprake is van een toegangsbeveiliging op 3 niveaus:

2.2.1 De schoolgebouwen en het bestuurskantoor zijn beveiligd door middel van algemene toegangsbeveiliging (inbraakalarm);

2.2.2 Persoonsgegevens worden bewaard in afsluitbare werkruimten;

2.2.3 Persoonsgegevens worden binnen de afsluitbare werkruimten bewaard in afsluitbare kasten of kluizen.

2.2.4 Om de toegang tot en de beveiliging van de gegevens te kunnen beheren en waarborgen, dragen de besturen per locatie zorg voor de registratie van de houders van sleutels/toegangspasjes/tags/toegangscodes, alsmede een regeling voor het gebruik en de bewaarplaats daarvan.

3 Toegangsbeveiliging systemen

3.1 Autorisaties

De schooldirecteuren zijn bevoegd om autorisaties toe te kennen voor de inzage en het gebruik van de op school in gebruik zijnde systemen.

3.1.1 De schooldirecteuren zijn verantwoordelijk voor de registratie van die autorisaties.

3.1.2 Tenminste jaarlijks wordt elke registratie gecontroleerd op actualiteit en geldigheid.

3.2 Wachtwoorden

Alle in gebruik zijnde systemen zijn alleen toegankelijk door middel van een gebruikersnaam en wachtwoord.
Deze wachtwoorden voldoen minimaal aan onderstaande eisen:

3.2.1 Elk wachtwoord bestaat uit tenminste 6 posities.

3.2.2 Elke wachtwoord bevat tenminste 1 cijfer, 1 letter en 1 leesteken.

3.2.3 Een wachtwoord is maximaal 90 dagen geldig.

3.2.4 Een wachtwoord moet op tenminste 4 posities verschillen ten opzichte van de voorgaande 3 wachtwoorden.

3.2.5 Na het invoeren van 3 foute wachtwoorden wordt de toegang tot het systeem geblokkeerd waardoor de (onbevoegde) gebruiker niet meer zonder hulp van het applicatie- of systeembeheer zelfstandig kan inloggen.

Zie voor de diverse applicaties het afzonderlijke document met wachtwoordbeleid.

3.3 Back-ups

3.3.1 Van alle niet-webbased systemen wordt wekelijks een back-up gemaakt. Deze back-ups worden zodanig bewaard dat reconstructie van persoonsgegevens mogelijk is. Hierin wordt voorzien door middel van het bewaren van een back-up op externe server(s) in een ander gebouw.

3.3.2 Van alle webbased systemen wordt als regel direct door de softwareleverancier een back-up gemaakt.

3.3.3 Het is niet toegestaan om back-ups op van persoonsgegevens op het huisadres, persoonlijke computer, usb stick of andere informatiedragers te bewaren.

3.3.4 Indien er een back-up van persoonsgegevens op een externe harde schijf worden bewaard dient deze bewaard te worden als omschreven in artikel 2.2 Beveiligingsniveau.

3.3.5 Indien persoonsgegevens op een door de school verstrekte laptop worden bewaard dient deze laptop te zijn beveiligd met een wachtwoord dat minimaal voldoet aan de eisen gesteld in artikel 3.2.

Dit reglement treedt in werking op 1 januari 2018.
Hiermee vervallen de reglementen welke op een eerdere datum zijn vastgesteld.