BIJLAGE 2: Technische en organisatorische beveiligingsmaatregelen voor "Op School"

1. Inleiding:

De Bewerker is overeenkomstig de Wbp en artikel 7 Bewerkersovereenkomst verplicht technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens. Hier volgt een omschrijving van de maatregelen zoals bedoeld in artikel 7.2 van de Bewerkersovereenkomst

In deze bijlage staan alle maatregelen die Bewerker heeft genomen voor de bewaking van de vertrouwelijkheid, integriteit en beschikbaarheid. Onderstaand verklaring van de termen.

- *Vertrouwelijkheid*: het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.
- *Integriteit*: het waarborgen van de correctheid en volledigheid van de informatie alsook de verwerking daarvan.
- *Beschikbaarheid*: het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot de informatie.

2. Begrippenlijst.

In dit document worden de volgende begrippen gebruikt:

Beveiligingsincident (datalek)
Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie in gevaar is of kan komen.

Back-up
Een back up is een reservekopie van de gegevens die zich binnen een applicatie bevinden.

HTTPS
HTTPS is de afkorting van Hyper Tekst Transfer Protocol Secure. Dit is een uitbreiding van het http protocol waarmee de verbinding met behulp van SSL encryptie wordt versleuteld. Http is een communicatie protocol waarmee een cliënt systeem met een server systeem communiceert om gegevens uit te wisselen.

SaaS
SaaS is een afkorting van Software as a Service. SaaS betekent dat de software die nodig is voor dataverwerking reeds is geïnstalleerd en gehost aangeboden wordt. De dienst is direct beschikbaar via het web.

SFTP
SFTP is de afkorting voor SSH File Transfer Protocol. Dit is een uitbreiding van het FTP protocol waarmee de verbinding via een SSH verbinding wordt getunneld. FTP is een communicatie protocol waarmee een cliënt systeem met een server systeem communiceert om bestanden uit te wisselen.

SSL
SSL is de afkorting van Secure Sockets Layer, het meest gebruikte beveiligingsprotocol.

3. Maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Verwerking van Persoonsgegevens.

De applicatie “Op School” is een SAAS oplossing. Het beheer en onderhoud worden uitsluitend door daartoe geautoriseerde personen uitgevoerd.

3.1 Toegang

Gebruikerstoegang is enkel mogelijk door in te loggen op de online applicatie. De verbinding maakt gebruik van TLS 1.2 en gecodeerd en geverifieerd met AES_128_GCM en gebruikt ECDHE_RSA als mechanisme voor sleuteluitwisseling. Het algoritme voor de handtekening is sha256RSA. De openbare sleutel is RSA (2048 Bits).

De volgende mensen hebben toegang tot de software en de daarin opgeslagen persoonsgegevens met de handelingen die zij uitvoeren:

- De eigenaren van de Onderwijspraktijk Harry Janssens als beheerder van “Op School”. Zij hebben toegang tot alle administratieve gegevens maar niet tot de leerling gegevens. Die zijn toegankelijk nadat de school daar schriftelijk toestemming voor heeft gegeven. De Onderwijspraktijk Harry Janssens vervult tevens de helpdeskfunctie, pr-activiteiten en facturering.
- Harry Janssens in zijn rol als onderwijsadviseur. Hij adviseert bij inhoudelijke vragen en analyseert gegevens in opdracht van de Onderwijsinstelling.
- Medewerkers Netgemak voor het ontwikkelen van software, updaten en testen en de admin-functie. Tevens zijn zij de technische helpdesk voor de Onderwijspraktijk. Ook zijn zij verantwoordelijk voor de koppeling met Parnassys.
- Beheerders namens de Onderwijsinstelling. Zij zijn gebruikers met eigen rechten maar kunnen die rechten ook delegeren naar andere gebruikers. Zij kunnen gebruikers, groepen en leerlingen aanmaken en verwijderen en gegevens aan elkaar koppelen.
- Gebruikers van de applicatie hebben toegang tot het dashboard. Hier worden alle gegevens waarvoor zij geautoriseerd zijn voor hen ontsloten. Gebruikers zijn altijd gekoppeld aan de Onderwijsinstelling en kunnen geen toegang krijgen tot het dashboard van andere Onderwijsinstellingen.
- De “Op School” beheerders hebben de machtigingen om te bepalen welke gegevens via het dashboard worden ontsloten. Het is voor “Op School” beheerder mogelijk om aangewezen gebruikers te markeren als beheerders namens de klant.

4. Omschrijving van de maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, verwerking, toegang of openbaarmaking.

4.1 Eisen aan het inloggen

Wachtwoorden:

- Wachtwoorden worden gecodeerd opgeslagen in de database. Mocht een hacker ooit binnen komen dan kan hij geen wachtwoorden achterhalen van gebruikers.
  Beheerders en gebruikers kunnen daar vervolgens een persoonlijk wachtwoord van maken.
- Een nieuw wachtwoord opvragen kan door het ingeven van een e-mailadres in de hiertoe bestemde functie. Deze is te benaderen via het inlogscherm. Indien het ingevoerde e-mailadres in de applicatie bekend is, zal naar dit e-mailadres een mail worden gestuurd met een link. Via deze link kan een (nieuw) wachtwoord worden ingegeven.
- Een nieuw wachtwoord moet bestaan uit totaal minimaal 8 tekens waarvan:
  - minimaal 1 hoofdletter is
  - minimaal 1 kleine letter is
  - minimaal 1 cijfer is
  - minimaal 1 vreemd teken is ($%&*@# enz)
  - het wachtwoord mag geen spaties bevatten.
  - het wachtwoord mag niet het zelfde zijn als de Gebruikersnaam.

- Een beheerder heeft een bij voorkeur een organisatie gebonden e-mailadres. De beheerder is verantwoordelijk voor de e-mailadressen die worden ingevoerd. Bij voorkeur zijn de e-mailadressen van andere gebruikers ook organisatie gebonden en wordt geen gebruik gemaakt van hotmail en gmail of enig ander privé mailadres.
- Er wordt een dringend beroep gedaan aan alle gebruikers hun inloggegevens niet af te geven aan andere gebruiker. Iedere gebruiker moet apart worden ingevoerd en “Op School” en kan vervolgens eigen inloggegevens opvragen.
- Er wordt een dringend beroep op de gebruikers gedaan om voor het uitwisselen of bespreken van leerling gegevens alleen gebruik te maken van de e-mailfunctie die in “Op School” is opgenomen en niet via andere e-mail kanalen.

4.2 Eisen aan de verbinding

- Voor “Op School” wordt gebruik gemaakt van een beveiligde verbinding (htpps)
- De Onderwijsinstelling is verantwoordelijk voor een adequate bescherming middels antivirusprogramma’s en firewall

4.3 Eisen aan opslag en back up

- Binnen de “Op School” applicatie worden alle data opgeslagen in een database. De gegevens in de database zijn vergrendeld.
- Aangeleverde bestanden worden 30 dagen bewaard.
- De servers zijn op de volgende manier beveiligd door middel van:
  - antivirusprogramma’s;
  - software update’s;
  - automatische back up’s;
  - aparte afgesloten ruimte;
  - alleen binnen Nederland;
  - toegang alleen door geautoriseerd personeel.
- **Back-ups** maken het mogelijk om gegevens tot drie maanden lang terug in de tijd te herstellen. Elke drie uur wordt een back-up gemaakt van de databases. Database back-ups zijn tot drie maanden opvraagbaar. Dit gaat als volgt: de 3-uurse back-ups worden 4 dagen lang bewaard. Na deze vier dagen worden van al de 3-uurse back-ups er 1 per dag bewaard gedurende 10 dagen. Na deze 10 dagen worden 11 weken lang wekelijkse back-ups bewaard. Back-ups worden gemaakt van een secundaire replicatie server.
- **Replicatie**: Live replicatie houdt in dat data bijna realtime worden weggeschreven van primaire fysieke database servers naar een secundaire server. Wanneer iets mis is met de primaire database server neemt de secundaire database server de taken transparant over om continuïteit van de applicatie te garanderen.

4.4 Eisen aan de (beveiliging) van de applicatie of software

- Alleen geautoriseerde personen kunnen met “Op School” werken.
- De software is zo opgebouwd dat per onderdeel gebruikers geautoriseerd kunnen worden.
- Voor de leerlingen vragenlijst wordt per leerling toegang verleend. Na het invullen ervan sluit de applicatie en moet de volgende leerling weer een wachtwoord invoeren. Zo kunnen de leerlingen niet bij de gegevens van andere leerlingen. Het is leerkrachten verboden hun inloggegevens aan de leerlingen te geven.
- Per licentie wordt een beheerder benoemd die anderen toegang kan geven tot de delen van het programma waar mee gewerkt wordt.
- De beheerder neemt die verantwoordelijkheid over van de Bewerker. Die kan wel worden ingeschakeld wanneer er problemen m.b.t. het beheer zijn.
- Door de Subbewerker wordt de werking van “Op School” gemonitord.
- Er wordt 1x per jaar een pen-test uitgevoerd op www.op-school.nl. De scan wordt uitgevoerd met een actuele software versie van Netsparker-Community Edition. Huidige versie Netsparker: 4.1.2.0.

- De Broncode is eigendom van Netgemak en is uitsluitend toegankelijk voor de ontwikkelaars, applicatie- en systeembeheerders. De Broncode is in Nederland opgeslagen. In de broncode worden geen gegevens opgeslagen, data worden uitsluitend in de database opgeslagen.
- Incryptie zit in de versleuteling van de gegevens en dat is gewaarborgd door het gebruik van SSL certificaten (Https).
- Wachtwoorden worden gecodeerd opgeslagen.
- Alleen binnen een schooljaar kunnen de gegevens worden bewerkt. M.i.v. het nieuwe schooljaar worden de gegevens gearchiveerd. Die kunnen wel worden benaderd maar niet meer worden bewerkt.
- Wanneer er een wijziging is van leerling gegevens waardoor die leerling uitstroomt, dan kan Subbewerker die informatie weer bij elkaar brengen

4.5 Dataservers en hostomgeving

Het “Op School” systeem maakt gebruik van een geavanceerde hostingomgeving om de betrouwbaarheid te maximaliseren. Het systeem wordt redundant gehost, hiermee wordt het volgende bewerkstelligd:

- Load balancing: gebruikers worden transparant vanuit de server met de laagste bezetting geserveerd;
- Fail over: als een server uitvalt kan de continuïteit van het systeem worden gegarandeerd omdat de werking door een andere server wordt overgenomen.

Ook voor de database server is gekozen voor een redundant systeem. Data worden bijna realtime op meerdere fysieke database servers opgeslagen. Deze constructie garandeert dat:

- als een database server uitvalt er geen gegevens verloren gaan, zelfs niet de gegevens die nog niet in de back-up procedure veilig zijn gesteld;
- back-ups worden gemaakt van de secunsaire server zodat men hierdoor geen performance hindernis ondervindt;
- data altijd op twee locaties is opgeslagen; als met de primaire database server problemen ontstaan zal de secundaire database de taken transparant worden overgenomen.

5. Omschrijving van de maatregelen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling.

5.1 Vertrek medewerker

Wanneer een medewerker vertrekt worden de “Op School” wachtwoorden waartoe de medewerkers beschikking had gewijzigd.

5.2 Vernietigen hardware

Gegevensdragers van afgeschreven hardware worden door middel van datavernietiging software onbruikbaar gemaakt. De volgende algoritmen kunnen worden gebruikt om de gegevens onherstelbaar te maken:

nnsa - U.S. NNSA Policy Letter NAP-14.1-C
dod - U.S. DoD 5220.22-M
usarmy - U.S. Army AR380-19
bsi - German Center of Security in Information Technologies
gutmann - 35-pass algorithm from Peter Gutmann's 1996 paper
schneier - algorithm described in Bruce Schneier's Applied Cryptography (1996)
pfitzner7 - Roy Pfitzner's 7-random-pass method
pfitzner33 - Roy Pfitzner's 33-random-pass method

6. Rapportage

6.1 Mochten er technische en organisatorische maatregelen getroffen zijn die afwijken van de in dit document opgenomen beschrijvingen of die getroffen zijn naar aanleiding van een beveiligingsincident, dan zal de directie en contactpersoon van “Op School” van de Onderwijsinstelling daarvan schriftelijk op de hoogte worden gebracht.

6.2 Voor de werkwijze rond datalekken of mededelingen n.a.v. beveiligingsincidenten, verwijzen wij naar artikel 8 van de bewerkersovereenkomst. Met de Onderwijsinstelling worden afspraken gemaakt over de afhandeling ervan.

Die afspraken omvatten:

- de wijze waarop monitoring en identificatie van incidenten plaatsvindt;
- de wijze waarop informatie wordt gedeeld;
- op welke manier (via e-mail, telefoon);
- aan wie gericht (contactpersonen en contactgegevens);
- met wie kan (bij vervolgacties) contact worden opgenomen;
- informatie die in ieder geval over een incident gedeeld moet worden;
- de kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
- de oorzaak van het beveiligingsincident;
- de maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
- benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
- de omvang van de groep betrokkenen;
- het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties);
- eventuele afspraken of, en zo ja hoe, Bewerker een melding aan de Autoriteit Persoonsgegevens kan verrichten.

Versie
November 2016