Protocol beveiligingsincidenten en datalekken SCO Delft e.o.

A. Doel van het protocol:

Dit protocol bevat regels en afspraken over de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken binnen SCO Delft e.o.

B. Uitgangspunten:

Dit protocol is van toepassing op de gehele organisatie van SCO Delft e.o., zoals vermeld in het Informatie Beveiliging Privacy beleid (IBP) en al haar medewerkers.

C. Belangrijke begrippen:

Beveiligingsincident	is een gebeurtenis die er voor zorgt of voor zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
Informatievoorziening	het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
Datalek	een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
Betrokkene	de persoon van wie de persoonsgegevens zijn gelekt.
Ontdekker	degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
Meldpunt	centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
Melder	degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
Technicus	degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

D. Wet- en regelgeving datalekken:

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Dit geldt bijvoorbeeld in de leerling administratie of digitale leermiddelen. SCO Delft e.o. heeft met de leveranciers, uitgevers en distributeurs die persoonsgegevens ontvangen van de scholen, aanvullende afspraken gemaakt over het melden van datalekken.

E. Datalek:

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten dat er persoonsgegevens verloren zijn gegaan. Als voorbeeld kan worden gegeven een hack waarbij een database met persoonsgegevens is gesloten, maar ook het verliezen van een usb-stick met daarop de adresgegevens van leerlingen is een datalek.

Als er een datalek is, moet binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

SCO Delft e.o. zal bij de beoordeling of er sprake is van een meldingsplichtig datalek rekening houden met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, zal SCO Delft e.o. melding doen.

F. Meldplicht:

Het bestuur van SCO Delft e.o. is verantwoordelijk voor de persoonsgegevens en heeft daarmee de meldplicht.
In sommige gevallen kan een bewerker namens de verantwoordelijke melding doen, maar dit is altijd onder verantwoordelijkheid van het bestuur van SCO Delft e.o.

G. Afspraken met leveranciers:

SCO Delft e.o. heeft, als verantwoordelijke voor de persoonsgegevens afspraken gemaakt met leveranciers die persoonsgegevens ontvangen over:

1. Het elkaar informeren over datalekken;
2. Wie doet de melding bij de Autoriteit Persoonsgegevens van een datalek;
3. Welke informatie gegevens moet de bewerker (leverancier) geven bij een datalek;
4. Welke informatie is nodig voor het doen van een melding;
5. Het elkaar informeren over de melding en de afhandeling daarvan;
6. De tijd waarbinnen de bewerker de gegevens moet aanleveren;
7. Wie de communicatie met de gebruikers doet indien nodig.

H. Melding beveiligingsincident of datalek:

1. Indien u een beveiligingsincident opmerkt, kunt u dit melden bij het Meldpunt via: meldpuntdatalekken@scodelft.nl. U kunt hiervoor het ‘meldingsformulier beveiligingsincident of datalek’ gebruiken.
   U dient zoveel mogelijk informatie te verzamelen en dit bij het Meldpunt kenbaar te maken. Het Meldpunt bepaalt of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zal het Meldpunt aanvullende vragen uitzetten bij u. Het Meldpunt zal de volgende informatie vastleggen:
   - Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
   - Datum/periode van het beveiligingsincident
   - Aard van het beveiligingsincident
   - Wanneer van toepassing (bij een datalek):
     - Omschrijving van de groep betrokkenen
     - Aantal betrokkenen
     - Type persoonsgegevens in kwestie
     - Worden de gegevens binnen een keten gedeeld
2. Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoed, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit Persoonsgegevens en/of betrokkenen vereist is.

De volgende informatie wordt vastgelegd door de Melder:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Of het datalek wordt gemeld aan de Autoriteit Persoonsgegevens?
- Of het datalek aan betrokkenen wordt gemeld?
- Hoe de meldingen worden gedaan en wat de inhoud van de melding is.

3. Indien SCO Delft e.o. concludeert dat er melding moet worden gedaan bij de Autoriteit Persoonsgegevens, dan zal de Melder dit binnen 72 uur na constatering doen bij het meldpunt datalekken. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen.
4. SCO Delft e.o. zal alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, archiveren. Het Meldpunt stuurt een samenvatting van de genomen maatregelen aan de Ontdekker.
5. Indien het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene, dan zal SCO Delft e.o. het datalek ook aan de betrokkenen zelf melden.

I. Meldingen van datalekken door derden:

Datalekken, veroorzaakt door derden die aan SCO Delft e.o. worden gemeld, worden door het Meldpunt vastgelegd. Indien het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van leerlingen, ouders en/of medewerkers van SCO Delft e.o. zal dit datalek ook aan betrokkenen worden gemeld.
Het Meldpunt archiveert alle informatie die met dit datalek te maken heeft.

J. Monitoring beveiligingsincidenten en datalekken:

Het Meldpunt en het bestuur van SCO Delft e.o. maken, tezamen met de Functionaris Gegevensbescherming, minimaal één keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken. In deze analyse worden zowel de meldingen die gemeld zijn vanuit SCO Delft e.o. als ook de meldingen van datalekken door derden meegenomen. Daarbij wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.