Politik for hændelseshåndtering på Odder Gymnasium

Formål

Formålet med retningslinjerne er at sikre at hændelser vedrørende informationssikkerheden bliver håndteret betryggende, samt at kritiske brud bliver rapporteret til skolens ledelse og øvrige relevante parter.

Metode

Der skal af skolens ledelse udpeges en medarbejder, der har det overordnede ansvar for, at der bliver fulgt op på hændelser, der kan kompromittere informationssikkerheden.

Skolen skelner mellem tre grundlæggende typer af sikkerhedsrelaterede hændelser:

- **Afvigelser** – svigt i efterlevelsen af sikkerhedspolitikker og retningslinjer.

- **Driftshændelser** – svigt i skolens systemer eller tab af information som følge af fejl eller uheld, som kan skade integriteten af data.

- **Sikkerhedshændelser** – brud på informationers fortrolighed eller tilgængelighed, herunder læk af persondata, uautoriseret adgang til, eller bevidst ændring eller destruktion af information, samt uautoriseret fysisk adgang, tyveri, hærværk som kan lede til kompromittering eller tab af datas integritet.
  Sikkerhedshændelser kan omhandle medarbejdere, samarbejdspartnere og leverandørers utilsigtede handlinger. Uheld og fejl kan have samme konsekvenser, som ondsindede angreb udefra.

Alle medarbejdere har i deres daglige arbejde pligt til at indrapportere identificerede hændelser og hurtigst muligt reagere, for at stoppe eller begrænse hændelsens omfang. Ansvaret for at følge op og evaluere på kritiske hændelser påhviler den udnævnte ansvarlige.
Afhængig af omfanget af hændelsen, skal berørte parter og myndigheder adviseres inden for en hver tid gældende lovgivnings tidsramme.
Ved hændelser, som har medført brud på persondatasikkerheden, skal tilsynsmyndigheden underrettes senest 72 timer efter at skolen har fået kendskab til bruddet.

Forløb

Alle identificerede hændelser skal igennem nedenstående 4 skridt for at sikre korrekt og rettidige behandling:

Identifikation: Når en hændelse identificeres skal der indsamles informationer om, hvilke data der er påvirket og hvis muligt noteres tidspunkter hvor bruddet er indtruffet.

Registrering: Alle indsamlede informationer omkring hændelsen skal dokumenters. På baggrund af den indsamlede dokumentation skal bruddets omfang vurderes herunder om der er brud på persondatasikkerheden. I denne proces skal det vurderes i hvilken form data var opbevaret. Var der tale om kritiske data, direkte identificerbar data, var data krypteret, var der benyttet pseudonymer mv. Konklusionen fra dette punkt er afgørende for det videre hændelses- og rapporteringsforløb.
Hvis det ikke konkluderes at der er tale om persondata eller anden kritisk data, som kan kategoriseres som en kritisk hændelse, skal sagen ikke eskaleres og der gås direkte til rapportering og evaluering af forløbet.

Eskaler: Hvis der er tale om tab af persondata, skal ansvarlige for hændelsesrapporteringen kontakte relevante tilsynsmyndigheder inden for 72 timer efter at hændelsen er identificeret. Herefter skal relevante instanser, myndigheder, samarbejdspartnere og berørte personer kontaktes med information omkring lækket af persondata.

Rapportering: Efter hændelsesforløbet er endt, skal der konkluderes på forløbet. Der skal identificeres svagheder i forløbet og baggrunden for at hændelsen opstod. Denne evalueringsproces er essentiel for at undgå lignende hændelser i fremtiden, da der her skal udpeges svagheder i interne processer og arbejdsgange, som kan have medvirket til hændelsen. På baggrund af denne proces bør man overveje om interne processer og arbejdsgange skal ændres. Al information om hvordan hændelsen opstod, kan bruges til at opnå forståelse for, hvorfor bruddet opstod og skolen på den måde kan undgå lignende hændelser fremadrettet.
Efter et hændelsesforløbet skal beviserne sikres, så disse kan bruges i en eventuelt retslig efterforskning.

Test

Processen omkring hændelseshåndtering bør testes løbende og minimum årligt. Der simuleres således hændelser, som påvirker informationssikkerheden, således at alle medarbejdere er bekendte med processerne omkring hændelseshåndtering.

Ansvar

Nedenstående skema skal udfyldes således at ansvaret er tydeligt fordelt blandt relevante personer på skolen:

	Skolens ansvarlige
Overordnet ansvarlig for hændelseshåndtering	Rasmus Pöckel
Planlægge og opdatere kontaktlister	Rasmus Pöckel
Kontakt til relevante myndigheder og leverandører	Rasmus Pöckel
Planlægge test	Rasmus Pöckel
Opdatering af hændelsesplanen	Rasmus Pöckel

Kontaktliste

Navn	**Ansvarsområde**	**Telefon**	**E-mail**	**Kommentar**
Rasmus Pöckel	Ansvarlig for den generelle hændelseshåndtering	86544500/ 51633227	rp@odder-gym.dk	
Jesper Rohde Pedersen	Ansvarlig for administration og arkivsystem	86544500/ 20148102	jp@odder-gym.dk	

Versionshistorik

Dato	***Ændret af***	**Godkendt af**	**Godkendt af**
13.5.2018	Rasmus Pöckel	Rektor Lars Bluhme	Bestyrelsesformand Bent Engelbrecht