Risikovurdering – Læringsplattform (skole)

Eksempler på hendelser er basert på Senter for IKT i utdanningens veiledere for "Sikker håndtering av personopplysninger". Dette er kun eksempler og den enkelte skoleeier må selv gjøre sine vurderinger av konsekvens, sannsynlighet, og hva som er akseptabel risiko.

Nr	Hendelse	Sikkerhetsbehov *	Faktor Konsekvens	Faktor Sannsynlighet	Risikofaktor	Akseptabel risiko	Tiltak beskrevet **
1.1	Elev får tak i og misbruker en annen elevs passord	K,I	3	3	9	6	1.1.1 1.1.2
1.2	Elev får tak i lærerens passord	K,I	4	2	8	6	1.1.1 1.1.2 1.1.3
1.3	Foreldre/foresatte får tilgang til elevens brukerkonto	K	3	3	9	6	1.1.2 1.1.4
1.4	Feil start- eller sluttdato	T	2	3	6	6	
1.5	Feil ved oppdatering / endring av programvaren	K,T	3	3	9	6	1.1.5 1.1.6 1.1.7
1.6	Sensitive eller sterkt personlige opplysninger registreres av lærer	K	4	3	12	6	1.1.1 1.1.3 1.1.8 1.1.9 1.1.10 1.1.11

*Sikkerhetsbehov: K: Konfidensialitet, T: Tilgjengelighet, I: Integritet

**Tiltak kan være både organisatoriske og tekniske.

Beskrivelse av hendelser:

1.1 Elev får tak i og misbruker en annen elevs passord:

Hvis elevene er uforsiktige med hvordan de håndterer passordene til læringsplattformen, kan andre elever få tak i disse. Dermed kan uvedkommende få tilgang til alle personopplysningene som er lagret i den aktuelle elevens brukerkonto. Uvedkommende kan også benytte den urettmessige tilgangen til å endre personopplysninger, for eksempel ved å slette eller redigere elevarbeid. Tilgangen kan også brukes til å sende elektroniske meldinger i elevens navn, eller til å avlegge prøver på vegne av den aktuelle eleven – identitetstyveri. Brudd på konfidensialitet og integritet.

1.2 Elever får tak i lærerens passord:

Hvis lærerne er uforsiktige med hvordan de håndterer passordene til læringsplattformen, kan elever få tak i disse. Elevene kan bruke tilgangen til å endre personopplysninger om mange elever som er lagret i lærerens brukerkonto. Det kan også tenkes at eleven får tilgang til sensitive personopplysninger om elever med vedtak om spesialundervisning. Elevene kan dessuten sende elektroniske meldinger eller poste beskjeder i lærerens navn (identitetstyveri). Brudd på konfidensialitet og integritet.

1.3 Foreldre/foresatte får tilgang til elevens brukerkonto:
Selv om foreldreansvaret innebærer at foreldre/foresatte skal være godt informert om elevens skolegang, har eleven rett til personvern. Uavkortet foreldre- eller foresatteinnsyn i personopplysninger på elevens brukerkonto kan derfor være å regne som brudd på opplysningenes konfidensialitet, det vil si at uvedkommende får tilgang til opplysningene. Dersom eleven har registrert opplysninger om andre elever i sin brukerkonto (for eksempel meldinger eller e-postkorrespondanse), kan dette føre til at foreldre/foresatte får tilgang til disse opplysningene. Brudd på konfidensialitet.

1.4 Feil start- eller sluttdato:
I læringsplattformen har administrator mulighet til å sette start- og sluttdato for brukerkontoene til ansatte, elever og foreldre/foresatte. Dersom administrator registrerer feil start- eller sluttdato på én eller flere brukere, kan personopplysninger ikke være å få tak i for brukere som har rettmessig behov for dem. Brudd på tilgjengelighet.

1.5 Feil ved oppdatering / endring av programvaren:
Læringsplattformen vil fra tid til annen være gjenstand for en del oppdateringer av programvaren fra leverandørens side. Det kan for eksempel skje når sikkerhetsmessige sårbarheter i programvaren oppdages. Dersom skolen eller skoleeier ikke er flinke til å følge opp meldinger om sikkerhetsoppdateringer fra leverandøren, kan dette føre til at kjente sårbarheter i programvaren ikke blir utbedret/rettet. Det kan føre til at uvedkommende utnytter sårbarhetene til å skaffe seg urettmessig tilgang til personopplysninger eller til at systemet ikke er tilgjengelig når det er behov for det. Brudd på konfidensialitet og tilgjengelighet.

1.6 Sensitive eller sterkt personlige opplysninger registreres av lærer:
I læringsplattformen har lærer mulighet til å lagre, laste opp og sende ut dokumenter. Dersom lærer lagrer for eksempel referat fra møter med andre lærere hvor det er diskutert enkeltelever, er det mulig at disse dokumentene kan inneholde sensitive opplysninger (for eksempel en diagnose). Slike dokumenter kan komme uvedkommende i hende dersom en lærer ved en feil sender dokumentet ut til feil mottaker eller at det sendes i ukryptert e-post. Dersom det er lagt opp til å bruke fritekstfelt i læringsplattformen, er dette også et sted hvor det kan legges sensitive opplysninger. Hvis uvedkommende får tilgang til lærers brukerkonto, kan dette føre til endring i opplysningene. Brudd på konfidensialitet og integritet.

<u>Beskrivelse av tiltak:</u>
1.1.1 Gjennomføre opplæring i bruk av læringsplattform med jevne mellomrom (organisatorisk tiltak).
1.1.2 Gjennomføre opplæring i sikker håndtering av passord (organisatorisk tiltak).
1.1.3 Innføre sterk autentisering (to-faktor) i forbindelse med lærerens innlogging i læringsplattform (teknisk tiltak).
1.1.4 Innføre egne brukerkonti for foreldre/foresatte med begrenset lesetilgang (teknisk tiltak).
1.1.5 Oppdateringer gjøres regelmessig (organisatoriske tiltak).
1.1.6 Oppdateringer gjøres i lukket testmiljø før det gjøres på alle brukere (teknisk tiltak).
1.1.7 Gjennomgå sikkerhetslogger for å sikre mot uautorisert tilgang (organisatorisk tiltak).
1.1.8 Fritekstfelt begrenses og erstattes med nedtrekksliste der det er mulig (teknisk tiltak).

1.1.9 Innføre klare rutiner for hvilke personopplysninger og dokumenter som kan lagres og sendes i læringsplattformen (organisatorisk tiltak).
1.1.10 Teknisk begrense muligheten for hvilke dokumenter som kan lagres av lærer (teknisk tiltak).
1.1.11 Ta i bruk et sakshåndteringssystem beskyttet med to uavhengige sikkerhetstiltak (teknisk tiltak).

Risikovurdering – Kommunikasjonsplattform (barnehage)

Nr	Hendelse	Sikkerhetsbehov *	Faktor Konsekvens	Faktor Sannsynlighet	Risikofaktor	Akseptabel risiko	Tiltak beskrevet **
1.1	Uvedkommende får tilgang til kommunikasjonsplattformen	K,I	3	3	9	6	1.1.1 1.1.2 1.1.12 1.1.13
1.2	Uvedkommende får tilgang til administratordelen	K,I	4	2	8	6	1.1.1 1.1.2 1.1.3 1.1.12 1.1.13
1.3	Hentelister er mulig å endre av alle brukere	I	4	2	8	6	1.1.1 1.1.2 1.1.3 1.1.9
1.4	Feil start- eller sluttdato	T	2	3	6	6	
1.5	Feil ved oppdatering / endring av programvaren	K,T	3	3	9	6	1.1.5 1.1.6 1.1.7
1.6	Sensitive eller sterkt personlige opplysninger registreres av ansatte	K	4	3	12	6	1.1.1 1.1.3 1.1.8 1.1.9 1.1.10 1.1.11
1.7	Det blir lagt ut bilder av barna uten at det er innhentet samtykke fra foreldrene	K	3	4	12	6	1.1.4
1.8	Ansatte får tilgang til administratordelen	K,I	3	3	9	6	1.1.12 1.1.13
1.9	Sensitive personopplysninger (for eksempel matallergi) registreres og kan endres av alle	K,I,T	4	3	12	6	1.1.3 1.1.14 1.1.15 1.1.16

*Sikkerhetsbehov: K: Konfidensialitet, T: Tilgjengelighet, I: Integritet

**Tiltak kan være både organisatoriske og tekniske.

Beskrivelse av hendelser:

1.1 Uvedkommende får tilgang til kommunikasjonsplattformen:

Det kan være flere årsaker til at uvedkommende får tilgang til kommunikasjonsplattformen:

a) Foreldre eller ansatte benytter felles passord ved pålogging.

b) Foreldre og ansatte får tildelt brukernavn som er enkelt å gjette seg til for eksempel mobiltelefonnummer.

c) Det stilles ikke krav fra kommunikasjonsplattformen om sterkt passord, hvilket kan føre til at foreldre lager passord som er enkelt å huske for eksempel barnets navn.
Dette kan føre til at uvedkommende får tilgang til personopplysninger om barna og har muligheten for å endre opplysninger.
Brudd på konfidensialitet og integritet.

1.2 Uvedkommende får tilgang til administratordelen på kommunikasjonsplattformen:
Hvis administrator (for eksempel styrer i barnehagen) er uforsiktig med hvordan de håndterer passordene til kommunikasjonsplattform, kan uvedkommende få tak i disse. Uvedkommende kan få tilgang til sensitive personopplysninger om barna, som helseopplysninger, opplysninger om atferd, og opplysninger som kan indikere allergi og religionstilhørighet. Uvedkommende kan sende elektroniske meldinger eller poste beskjeder i styrers navn (identitetstyveri). Uvedkommende kan endre på opplysninger om barna. Brudd på konfidensialitet og integritet.

1.3 Hentelister er mulig å endre av alle brukere
Hentelister i barnehagen inneholder informasjon om hvem som har lov til å hente et barn fra barnehagen. Dersom uvedkommende får tilgang til en annens brukerkonto, kan uvedkommende sette sitt eget navn på hentelisten og deretter hente ut andres barn fra barnehagen. Brudd på integritet.

1.4 Feil start- eller sluttdato:
I kommunikasjonsplattformen har administrator mulighet til å sette start- og sluttdato for brukerkontoene til ansatte, elever og foreldre/foresatte. Dersom administrator registrerer feil start- eller sluttdato på én eller flere brukere, kan personopplysninger ikke være å få tak i for brukere som har rettmessig behov for dem. Brudd på tilgjengelighet.

1.5 Feil ved oppdatering / endring av programvaren:
Kommunikasjonsplattformen vil fra tid til annen være gjenstand for en del oppdateringer av programvaren fra leverandørens side. Det kan for eksempel skje når sikkerhetsmessige sårbarheter i programvaren oppdages. Dersom barnehagen eller barnehageeier ikke er flinke til å følge opp meldinger om sikkerhetsoppdateringer fra leverandøren, kan dette føre til at kjente sårbarheter i programvaren ikke blir utbedret/rettet. Det kan føre til at uvedkommende utnytter sårbarhetene til å skaffe seg urettmessig tilgang til personopplysninger eller til at systemet ikke er tilgjengelig når det er behov for det. Brudd på konfidensialitet og tilgjengelighet.

1.6 Sensitive eller sterkt personlige opplysninger registreres av ansatte:
I kommunikasjonsplattformen har ansatte mulighet til å lagre, laste opp og sende ut dokumenter. Dersom en ansatt lagrer for eksempel referat fra møter med andre ansatte hvor det er diskutert enkeltbarn, er det mulig at disse dokumentene kan inneholde sensitive opplysninger (for eksempel en diagnose). Slike dokumenter kan komme uvedkommende i hende dersom en ansatt ved en feil sender dokumentet ut til feil mottaker eller at det sendes i ukryptert e-post. Dersom det er lagt opp til å bruke fritekstfelt i kommunikasjonsplattformen, er dette også et sted hvor det kan legges sensitive opplysninger. Hvis uvedkommende får tilgang til ansattes brukerkonto, kan dette føre til endring i opplysningene. Brudd på konfidensialitet og integritet.

1.7 Det blir lagt ut bilder av barna uten at det er innhentet samtykke fra foreldrene:
Ansatte filmer eller tar bilder av barna uten at det er innhentet samtykke fra foreldrene. Bildene blir så lagt ut på kommunikasjonsplattformen. Brudd på konfidensialitet.

1.8 Ansatte får tilgang til administratordelen:
Ansatte som ikke skulle hatt tilgang til administratordelen får tilgang til denne fordi det benyttes en felles PC som automatisk logger inn på kommunikasjonsplattformen. Ansatte får mulighet til å lese og endre opplysninger de ikke skulle hatt tilgang til fordi administrator har glemt å logge ut. Brudd på konfidensialitet og integritet.

1.9 Sensitive personopplysninger (for eksempel matallergi) registreres og kan endres av alle:
Hvis et barn er allergisk mot noe (for eksempel nøtter), blir dette registrert på barnet. Dersom informasjon om allergi og annen sykdom ikke er tilgjengelig for alle ansatte som har ansvar for dette barnet, kan det oppstå situasjoner som i verste fall er livstruende. Uvedkommende kan få tilgang til informasjonen som bevisst ønsker å skade barnet. Ansatte eller uvedkommende kan komme til å endre informasjonen ved uhell eller som en bevisst handling (for eksempel at allergi endres fra nøtter til egg). Brudd på konfidensialitet, integritet og tilgjengelighet.

<u>Beskrivelse av tiltak:</u>
1.1.1 Gjennomføre opplæring i bruk av kommunikasjonsplattform med jevne mellomrom (organisatorisk tiltak).
1.1.2 Gjennomføre opplæring i sikker håndtering av passord (organisatorisk tiltak).
1.1.3 Innføre sterk autentisering (to-faktor) i forbindelse med ansattes innlogging i kommunikasjonsplattform (teknisk tiltak).
1.1.4 Ha rutiner for kontroll av samtykke fra foreldrene ved fotografering eller filming av barna, og når bilder skal legges ut på plattformen (organisatorisk tiltak).
1.1.5 Oppdateringer gjøres regelmessig (organisatoriske tiltak).
1.1.6 Oppdateringer gjøres i lukket testmiljø før det gjøres på alle brukere (teknisk tiltak).
1.1.7 Gjennomgå sikkerhetslogger for å sikre mot uautorisert tilgang (organisatorisk tiltak).
1.1.8 Fritekstfelt begrenses og erstattes med nedtrekksliste der det er mulig (teknisk tiltak).
1.1.9 Innføre klare rutiner for hvilke personopplysninger og dokumenter som kan lagres og sendes i kommunikasjonsplattformen (organisatorisk tiltak).
1.1.10 Teknisk begrense muligheten for hvilke dokumenter som kan lagres av ansatte (teknisk tiltak).
1.1.11 Ta i bruk et sakshåndteringssystem beskyttet med to uavhengige sikkerhetstiltak (teknisk tiltak).
1.1.12 Tilgang til kommunikasjonsplattformen bør tidsbegrenses, og brukerne bør kobles fra automatisk hvis tilkoblingen har vært inaktiv i en viss tid.
1.1.13 Sørg for at ansatte ikke logges automatisk inn på kommunikasjonsplattformen hvis det benyttes felles PC i barnehagen, og sørg for at brukere automatisk logges av etter tid (teknisk tiltak).
1.1.14 Endring av sensitive opplysninger, som for eksempel matallergi eller sykdom, kan bare gjøres av administrator (teknisk tiltak).
1.1.15 Ved endring av sensitive opplysninger, som for eksempel matallergi eller sykdom, skal en advarsel komme opp, slik at man må bekrefte endringen en ekstra gang (teknisk tiltak).
1.1.16 Helseopplysninger som er viktig for ansatte som har ansvar for et barn, skal være synlig dem, men ikke mulig å endre for andre enn administrator (teknisk tiltak).