

Beredskapsplan Datasikkerhet

Saker vedrørende hacking, GDPR og datasikkerhet

Handling	Varsling	Kommunikasjon	Loggføring underveis
Hva må vi gjøre?	Hvem må vi kontakte?	Hva skal vi si?	Hva må vi dokumentere?
Hacking og sikkerhetsbrudd ☐ Umiddelbar respons: Isolere berørte systemer, fjerne trusselen, og hindre ytterligere skade. ☐ Undersøkelse av hendelsen: Grundig analyse av hvordan bruddet skjedde og hva som ble kompromittert. Er det fortsatt pågående trusler? Overholdelse av GDPR og personvern ☐ Meldingsplikt ved brudd: Ifølge GDPR må vi ved sikkerhetsbrudd hvor personopplysninger blir kompromittert vurdere om bruddet medfører risiko for personvernet til de berørte individene. Hvis ja, skal bruddet rapporteres til relevante datatilsynsmyndigheter innen 72 timer. ☐ Varsling til berørte personer: Om hacking eller sikkerhetsbrudd medfører høy risiko for de berørte individene (f.eks. tap av personopplysninger som kan føre til identitetstyveri), må vi informere disse så raskt som overhodet mulig.	Daglig leder Fagsjef IT Generalsekretær NIF-Digital Integrasjonspartnere	Media: Er det grunn til å tro at media vet? Eventuelt hva? Generalsekretær er vår hovedtalsperson. Anerkjenn alvoret i situasjonen. Bruk enkelt, konkret språk som ikke kan misforstås. Hovedbudskapet først, argumentene etterpå. Snakk sant. Dette er en pågående sak/ vi har tatt ulike grep for å beskytte oss, vi bruker nå tiden på å komme til bunns i hva som har skjedd. Ikke svar på direkten om du er uforberedt. Spør hva de er ute etter. Avtal at vi ringer tilbake. Oppdater ved ny informasjon. Usikker? Ikke spekul. Si du må sjekke. Husk at media kan kjenne saken dårlig eller være feilinformert. Det er sjelden selve krisen som feller, men måten den håndteres på.	☐ Alle hendelser skal dokumenteres av Fagsjef IT. Viktig både for interne formål og for å kunne rapportere til relevante myndigheter. ☐ Ved sikkerhetsbrudd rundt personvern bør vi evaluere og revidere våre prosedyrer for å sikre oss mot fremtidige brudd.