# IT-Beredskabsplan

## Formål

Denne Beredskabsplan for FGU XX har til formål, at bidrage til en stabil og sikker drift, samt minimering og i bedste fald forhindre tab af data i tilfælde at udefrakommende angreb, sabotage eller forsyningssvigt, ved at give alle medarbejdere hos FGU xx mulighed for at handle hurtigt og præcist i tilfælde af et angreb.

Ingen medarbejder hos FGU XX må i en krisesituation være forhindret i at handle korrekt på grund af manglende viden eller information om, den korrekte procedure.

**Procedure i tilfælde af** **Hackerangreb, Phishingangreb, Sikkerhedsbrud, Systemnedbrud eller anden form for sabotageaktivitet.**

**Hvem skal kontakte hvem?**

Umiddelbart efter du erkender at et angreb, et sikkerhedsbrud, et systemnedbrud eller en sabotageaktivitet har ramt dit driftsmiljø, skal du omgående kontakte nærmeste leder eller den IT-ansvarlige og informere om, hvad du har erkendt.

Kontaktdata: på IT-ansvarlige samt ledergruppen (Mail og telefon)

**Hvem skal udføre hvilke opgaver?**

Umiddelbart efter at være adviseret om problemet skal den IT-ansvarlige eller den pågældende leder kontakte Support-desk hos Statens IT eller anden driftsleverandør hvis ikke man bruger SIT på (kontakt til supporten: 72310001) og informere om den indtrufne hændelse:

* Hvad har man oplevet
* Hvornår er hændelsen første gang konstateret
* Hvem er FGU XX kontaktperson for yderligere informationer.

**Opfølgning på beredskabet**

Umiddelbart efter anmeldelse af hændelsen til supporten, påbegyndes dokumentation af sagen i en logfil (evt. gerne samme logfil som benyttes til GDPR sikkerhedsbrud).

Dokumentationen skal i givet fald komme fra udbyderen af den angrebne service. Hvis der f.eks. er tale om et angreb mod det studieadministrative system (IST, FGU Planer), eller hvis det er tale om at hjemmesiden er angrebet, hvorfor det i så fald er den pågældende udbyder f.eks. One.Com.

Dokumentationen skal indeholdende en beskrivelse af hændelsesforløbet, hvilke foranstaltninger har man truffet til afværgning for at stoppe angrebet. Hvilke foranstaltninger er der truffet for at undgå tilsvarende fremtidige angreb.

**Konsekvensvurdering**

Den dataansvarliges IT-ansvarlige og FGU XX’s ledelse skal efterfølgende udføre konsekvensvurdering og evt underretning til berørte personer om evt personlige konsekvenser

Konsekvensvurdering skal omfatte:

* Har der været tale om tab af data?
* Har der været tale om tab af integritet?
* Har der været tale om tab af tilgængelighed til data og i givet fald, hvor længe?
* Har der været tale om sabotage af bygningsinfrastruktur eller anden ikke IT-relateret påvirkning.
* Hvilken konsekvens vurderes hændelsen at have haft for FGU XX?
* Hvilken konsekvens vurderes hændelsen at have haft for de registrerede?
	+ Har konsekvensen en karakter, der gør det nødvendigt at informere de registrerede herom?
* Har konsekvensen en karakter der nødvendiggør anmeldelse til Datatilsynet?
	+ Tag kontakt til FGU Danmark fælles DPO for en evt afklaring.
* Har konsekvensen en karakter der nødvendiggør iværksætning af yderligere fysiske sikkerhedsforanstaltninger?
* På baggrund af de trufne foranstaltninger, hvor sandsynligt vurderes det, at denne type hændelse kan genopstå?