**Bilag A**
Eksempler på tekniske og organisatoriske informationssikkerhedshændelser

| **Teknisk informationssikkerhedshændelse** | **Organisatorisk informationssikkerhedshændelse** |
|---|---|
| ▪ Cyberangreb (destruktiv hacking, informationsforfalskning, website defacing, denial of service angreb, botnet angreb, spam angreb)<br>▪ Strømafbrydelse<br>▪ Brandskade<br>▪ Vandskade<br>▪ Elektromagnetisk beskadigelse (lynnedslag, solstorm, statisk elektricitet)<br>▪ Skade ved naturhændelse (storm, orkan, tordenstorm, skypumpe)<br>▪ Skade ved katastrofal ulykke (eksplosion i tilstødende bygninger eller faciliteter)<br>▪ Skade ved forsætlig destruktion (brandstiftelse, hærværk, terrorbombning, sabotage begået af hævngerrige eller korrupte ansatte)<br>▪ Tyveri af aktiver (indbrud, røveri, simpelt tyveri, tricktyveri, tyveri begået af ansatte)<br>▪ Leverandørkollaps (konkurs, nedlæggelse)<br>▪ Drifts- eller vedligeholdelsesfejl (serviceleverandørfejl, hostingleverandørfejl, fejl begået af drifts-, support- eller vedligeholdelsesstab)<br>▪ Kapacitetsfejl (kapacitetsmangel for datalagre eller –behandling)<br>▪ Softwarefejl (softwarenedbrud, bugs, databasekorruption, back-up retableres ikke, uautoriseret eller ikke-testet kode)<br>▪ Hardware-fejl (kommunikationslinjenedbrud, udstyrsnedbrud eller -defekt, slid, korrosion, henfald af lagringsmedier<br>▪ Fejl i fysisk miljøstyring (kølingsfejl, luftfiltreringsfejl, opvarmningsfejl, vandforsyningssvigt, frost, hedebølge/tørke<br>▪ El-forsyningsfejl (strømsvigt, el-forsyningslinjebrud, isslag, strømfluktuation, sag, surge, spike, brownout, forsyningsudstyrssvigt, UPS-fejl, generatorfejl, elforsyningsoverbelastning)<br>▪ Leverancesvigt (afvigelse fra aftalt serviceniveau) | ▪ Tab af USB nøgle, ekstern harddisk, SD-kort eller anden form for fysisk lagringsenhed<br>▪ Tab af laptop, bærbar PC, tablets, mobiltelefon<br>▪ Mail, der sendes til forkert modtager (både interne og eksterne modtagere)<br>▪ Medarbejdere får eller tager sig uautoriseret adgang til personoplysninger<br>▪ Personoplysninger, der slettes (uden at der er hjemmel til det)<br>▪ Aktivering af ukendt link i en mail, download af et ukendt program eller åbning af en fil fra et inficeret USB-stik, der installerer malware på computeren<br>▪ Phishing via e-mail eller websider<br>▪ Aktivering af ukendt link eller åbne en vedhæftet fil i en mail, der ser ud til at komme fra en troværdig afsender (Spear-phishing)<br>▪ Ansat har forladt sin PC, uden at den blev ”låst”<br>▪ Dokumenter printes uden anvendelse af FollowMe<br>▪ Dokumenter, der ikke destrueres korrekt<br>▪ Utilsigtet offentliggørelse af information på internettet<br>▪ Forsætligt misbrug (forfalskning, svindel, uautoriseret brug, misbrug af rettigheder, brud på ophavsrettigheder)<br>▪ Bevidst afsløring af beskyttet information (politisk motiveret informationslækning, økonomisk motiveret informationslækning)<br>▪ Informationslæk (fejlkonfiguration af adgangsrettigheder og sikkerhedssystemer, fejlagtig offentliggørelse af data, inkludering af skjulte data i datafiler)<br>▪ Brugerfejl (uforsætlig brugerhandlinger, fejlbehandlinger af medier, mangel på uddannelse, for vidtgående brugerrettigheder og –privilegier |