**Vejledning til anvendelse   
af Wired Relations’ skabeloner**A black background with black lines

Description automatically generated

Wired Relations’ skabeloner\* kan anvendes direkte i jeres arbejde med databeskyttelse og informationssikkerhed – men kan selvfølgelig også anvendes som inspiration til jeres eget materiale. I kan ændre efter behov, så det bliver præcis, som I ønsker det.

**OBS!** Der kan være afsnit, som ikke er relevante for alle virksomheder. Hvis dette er tilfældet, vil det tydeligt fremgå af teksten.

Der vil være steder i teksten, hvor der er lagt op til, at I indsætter virksomhedens navn eller andet. Dette vil i så fald være markeret jf. følgende: [*indsæt virksomhedens navn*].

|  | Tekstboksene i dokumentet indeholder opmærksomhedspunkter og gode råd. Vær opmærksom på, at tekstboksene bør fjernes fra den endelige udgave af den konkrete politik eller procedure. |  |
| --- | --- | --- |

I bunden af hver skabelon vil der fremgå en tabel, som giver et overblik over dokumentets version, seneste opdatering, samt hvem der har ansvaret for dokumentet.

|  | Her er nogle ekstra tips til brug af Wired Relations' skabeloner: |  |
| --- | --- | --- |
|  | * I kan tilføje eller fjerne sektioner, ændre ordlyd og tilføje virksomhedens eget logo og branding. |  |
|  | * Hold skabelonerne opdaterede. Krav til databeskyttelse og informationssikkerhed ændrer sig konstant, så det er vigtigt at sikre, at skabelonerne altid er opdaterede. |  |

**Procedure for håndtering af sikkerhedshændelser**

**1. Formål**

Formålet med denne procedure er at skabe klare retningslinjer for håndteringen af sikkerhedshændelser.

**2. Målgruppe**

Denne procedure er særligt målrettet *[Indsæt relevant kontaktpunkt / team, der vurderer og håndterer sikkerhedshændelser]*, der er ansvarlige for at vurdere og håndtere sikkerhedshændelser i *[Indsæt virksomhedens navn].*

|  | Det er vigtigt at få etableret et fast kontaktpunkt i virksomheden, der tager sig af vurdering og håndtering af sikkerhedshændelser. Dette kan bl.a. være beskrevet i en overordnet politik for håndtering af sikkerhedshændelser.  Medarbejderne i virksomheden skal vide, hvordan de skal reagere og hvem de skal kontakte, hvis de opdager en sikkerhedshændelse (eller blot har mistanke herom).  Derudover er det afgørende, at medarbejderne løbende modtager uddannelse eller træning i dette emne. |  |
| --- | --- | --- |

**3. Proces for håndtering af sikkerhedshændelser**

Når [*Indsæt relevant kontaktpunkt / team, der vurderer og håndterer sikkerhedshændelser]* får besked om, at der er identificeret en sikkerhedshændelse, er der forskellige skridt, der skal tages stilling til.

3.1 STOP sikkerhedshændelsen

Hvis det er muligt, skal sikkerhedshændelsen stoppes hurtigst muligt. Dette kan gøres på forskellige måder afhængigt af, hvilken sikkerhedshændelse der er tale om.

Det kan være et spørgsmål om at afbryde netværk for at forhindre spredning af malware eller uautoriseret adgang eller at lukke systemer ned for at undgå yderligere skade. Det kan også være, at der er behov for at blokere al adgang til det kompromitterede system.

3.2 Vurdér om der er tale om en krisesituation

Det skal altid vurderes, om der er tale om en krisesituation i forhold til, om der skal iværksættes relevant beredskab.

*[Oplist eventuelt eksempler på, hvad en krisesituation kan være, eller hvilke parametre, der skal vurderes. Her kan også henvises til en eventuel kriseberedskabsplan eller it-beredskabsplan i forhold til vurderingen af, om der er tale om en krisesituation, hvor beredskabet skal aktiveres.]*

3.3 Vurder og analyser sikkerhedshændelsen

Det er *[indsæt relevant team/kontaktpunkt, der vurderer og håndterer sikkerhedshændelser]*, der vurderer og analyserer sikkerhedshændelsen for at finde ud af, hvordan situationen skal håndteres og hvordan sådan en situation fremadrettet kan undgås.

Er der tale om en sikkerhedshændelse, som involverer personoplysninger, skal dette vurderes af *[indsæt kontaktoplysninger på fx DPO eller andet relevant kontaktpunkt].*

Det er vigtigt, at de løbende vurderinger dokumenteres, se pkt. 5.

3.4 Risikovurdering

På baggrund af håndtering af sikkerhedshændelser bør det altid vurderes, om der skal foretages en risikovurdering eller om den eksisterende og aktuelle risikovurdering skal opdateres.

3.5 Implementer udvalgte foranstaltninger

I forbindelse med vurderingen af sikkerhedshændelsen identificeres konkrete sikkerhedsforanstaltninger, der skal implementeres. Der skal udarbejdes en plan for den konkrete implementering, herunder hvem der er ansvarlig for implementeringen og tidsfrist. Dette bør indgå i dokumentationen af sikkerhedshændelsen.

3.6 Underretning / rapportering

I takt med at sikkerhedshændelsen vurderes og håndteres, skal der også tages stilling til, om sikkerhedshændelsen er af en sådan karakter, at der skal foretages en indberetning til fx Center for Cybersikkerhed eller Datatilsynet.

|  | **Eksempler på krav til underretning / rapportering**  *I kan med fordel beskrive, hvilke ordninger, der er relevante for jeres virksomhed.*  Større sikkerhedshændelser  Har din organisation været ramt af en sikkerhedshændelse, kan der være krav om, at du underretter CFCS. Siden den 1. september 2014 har alle statslige myndigheder været forpligtet til at underrette CFCS om større sikkerhedshændelser.  Underretning om sikkerhedshændelser til CFCS sker via virk.dk  Frivillig underretning  Virksomheder har mulighed for frivilligt at underrette CFCS om større sikkerhedshændelser. Den frivillige underretning sker også via virk.dk.  Virksomheder omfattet af NIS-direktivet  Der gælder særlige krav til underretning for de myndigheder og virksomheder, der er omfattet af det nuværende NIS direktiv.  Sådanne underretninger af sikkerhedshændelser skal ske til CFCS, der er national CSIRT, og til de sektoransvarlige myndigheder.  I forhold til den kommende NIS2-lovgivning  I *udkast til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau* foreslås det, at væsentlige og vigtige enheder uden unødigt ophold skal underrette den relevante kompetente myndighed og CSIRT’en om enhver væsentlig hændelse, og at kravene til fremgangsmåden og fristerne for underretningerne indholdsmæssigt svarer til kravene i NIS2-direktivet (artikel 23).  Indberetning til Datatilsynet  Som udgangspunkt skal alle brud på persondatasikkerheden anmeldes til Datatilsynet. Det er således kun, hvis det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, at der ikke skal ske anmeldelse. |  |
| --- | --- | --- |

3.7 Orientering af ledelsen og andre interessenter

Ledelsen orienteres løbende om nye og igangværende sikkerhedshændelser.

|  | **Eksempler på krav til underretning / rapportering**  *I kan med fordel beskrive, hvilke ordninger, der er relevante for jeres virksomhed.*  Det er vigtigt at inddrage ledelsen i vurdering og håndtering af sikkerhedshændelser, da det i sidste ende er ledelsens ansvar at sikkerhedshændelsen bliver håndteret korrekt, og derudover kan ledelsen ofte bidrage med prioritering i forhold til ressourcer. |  |
| --- | --- | --- |

Det vurderes løbende, om der er andre interessenter, der skal orienteres i forhold til den konkrete sikkerhedshændelse. Denne vurdering dokumenteres.

**4. Dokumentation**

Vurdering og håndtering af en sikkerhedshændelse eller et sikkerhedsbrud dokumenteres løbende. Dokumentation af forløbet er meget vigtig - særligt som understøttende dokumentation, hvis hændelsen eller bruddet resulterer i en retslig efterforskning. Derudover støtter en grundig dokumentation også de overvejelser, der har været undervejs, f.eks. i forhold til mitigerende tiltag.

**5. Evaluering**

Efter en hændelseshåndtering foretages en evaluering af forløbet, herunder erfaringsopsamling og en vurdering af, om der bør iværksættes yderligere forebyggende foranstaltninger.

Der foretages også en løbende vurdering af, om processen omkring hændelseshåndtering er effektiv. Evalueringen dokumenteres også.

### **Dokumentinformation**

| Dokumentversion |  |
| --- | --- |
| Dato for udgivelse af denne version |  |
| Ansvarlig |  |
| Status |  |