**Vejledning til virksomheder og myndigheder**Denne vejledning skal ses i sammenhæng med ”Vejledning til anmeldelse af sikkerhedsbrister” og beskriver samlet set god skik ved anmeldelse af sikkerhedsbrister.

Har en borger fulgt de procedurer som kodekset rummer, forpligter virksomheden sig som underskriver af kodekset til at behandle henvendelsen fortroligt, samt til ikke at melde personen til politiet medmindre lovgivningen måtte kræve dette.

Man kan således eksempelvis ikke sætte sig ud over straffelovens principper om anmeldepligt i henhold til Straffelovens § 141.

Hvis I modtager henvendelser om sikkerhedsbrister, der ikke (alene) vedrører jeres egen virksomhed, forpligter I jer endvidere til, uden ugrundet ophold, at meddele rette systemejer eller it-leverandør om sikkerhedsbristen.

**Hjælp til vejledning på hjemmesiden**

Virksomheder og myndigheder, der har tilsluttet sig kodekset, skal placere ”Vejledning til anmeldelse af sikkerhedsbrister” på virksomhedens/myndighedens hjemmeside.

IT-Branchen anbefaler at vejledningen kan tilgås via kodeksets logo, placeret et logisk sted på hjemmesiden.

Det er nødvendigt at tage aktiv stilling til flere elementer i den eksterne anmeldervejledning. Disse steder er markeret med gult (se Vejledning til anmeldelse af sikkerhedsbrister).

**Hvem skal modtage anmeldelser om sikkerhedsbrister?**

* I vejledningen skal det klart fremgå, hvor man skal rette henvendelse.
* Det bør også fremgå, hvor man retter henvendelse ved almindelige fejl, hvor der ikke er risiko for utilsigtet adgang til persondata eller virksomhedsfølsomme oplysninger (alm. support).

**Har i et bug-bounty program?**

* Nogle fejl opdages ved et tilfælde. I andre tilfælde er det professionelle, der leder efter sårbarheder. En række softwarevirksomheder har anvendt bug-bounty programmer til at skabe et incitament til at indrapportere fejl og sikkerhedsbrister. Hvis I har et sådant program, skal det beskrives i vejledningen. Alternativt kan punktet slettes.

**Hvor hurtigt melder I tilbage til anmelder?**

* I vejledningen indgår to frister. En for kvittering for modtagelsen og en for endelig tilbagemelding til anmelderen. Det er op til den enkelte virksomhed/organisation at definere egne frister. IT-Branchen anbefaler korte svarfrister – f.eks. to dage for kvittering og to uger for endelig eller foreløbig tilbagemelding

Husk, at en henvendelse om sikkerhedsbrister kan indeholde oplysninger, der skal reageres på jf. gældende lovgivning, f.eks. Persondataforordningens regler om underretningspligt ved databrud – [Læs evt. mere her](https://itb.dk/news/hvordan-skal-du-reagere-ved-databrud).

**Overholdelse af kodeks**

IT-Branchen vedligeholder en liste over de virksomheder, der har tilsluttet sig. Det er alene jeres ansvar at sikre at kodekset overholdes. Der er ikke tale om en certificering eller godkendelsesproces. IT-Branchen fører ikke aktivt tilsyn med om mærkningsordningen overholdes. IT-Branchen forbeholder sig dog retten til at fjerne virksomheder fra listen, der ikke overholder kodekset.