*Denne skabelon vedr. sikring af digitale beviser er udarbejdet i samarbejde mellem politiet, Center for Cybersikkerhed og en række IT-sikkerhedsfirmaer. Har du brug for, at politiets IT-eksperter vejleder dig i, hvordan du anmelder et cyberangreb eller sikrer relevante digitale spor, kan du ringe 114 og blive viderestillet til politiets First Response Team.*

**Datasikringsskabelon**

**Hvad skal man være opmærksom på ved sikring af digitale beviser?**

Ved sikring af data og potentielle beviser kan din virksomhed eller et IT-sikkerhedsfirma følge nedenstående principper.

1. Data sikres **hurtigst muligt**, så det ikke går tabt. Husk at sikre en kopi af dit system, inden du fortsætter behandlingen af data, da der ellers er risiko for, at du kompromitterer potentielle beviser.
2. Alle datasæt tildeles **et ID-nummer**, så politiet kan identificere, hvor data stammer fra.
3. Der anvendes **anerkendte datasikringsformater** (fx E01, AFF4, L01 eller åbne formater som fx DD, DMG og KAPE), så data kan anvendes i politiets forensic-værktøjer.
4. Der foretages en **hash-beregning** (fx MD5 eller SHA1) pr. sikret datasæt. Dette skal sikre, at data er intakt fra sikringstidspunktet og ved senere undersøgelser.
5. Der anvendes **ubrugte eller wipede** **modtagermedier** til datasikringen. På den måde risikerer data ikke at blive kontamineret med anden data.
6. I forbindelse med datasikringen anbefales det at **dokumentere** en række forhold. Til dette kan du bruge skemaet nedenfor. Beskriv gerne, hvorfor du mener, at de sikrede data kan bidrage til at bevise hændelsesforløbet, og hvem der har foretaget sikringen.

**GENEREL INFORMATION >**

|  |  |  |
| --- | --- | --- |
| **Dato for datasikring** / /  | **Virksomhed** | **Arknummer** (hvis flere ark) |
| **Eventuel bemærkning**  | **Antal datasikrede enheder** |
| **Hvem har datasikret?** (navn og titel) |
| **Datasikringslokation** (hvis relevant) |

I de følgende felter kan du dokumentere fire datasikrede enheder. Har du flere enheder, kan du printe flere ark. I feltet kan du registrere enhedens medie, indhold på enheden, hvilket format der bliver datasikret i og hashværdi. Der er også mulighed for at registrere eventuelle loginoplysninger eller dekrypteringskoder. Ved fysiske enheder er det en god idé at påføre ID-nummeret.

**INFO OM DEN DATASIKREDE ENHED >**

|  |  |  |
| --- | --- | --- |
| **ID-nummer** | **Enhedsmedie** (USB, harddisk, bærbar e.l.) | **Datasikringsformat** |
| **Indhold på mediet**  |
| **Hashing algoritme** | **Hashværdi** |
| **Login** (hvis relevant) | **Kodeord** (hvis relevant) |
| **Kryptering & kode til dekryptering** (hvis relevant) | **Recoverykode** (hvis relevant) |

**INFO OM DEN DATASIKREDE ENHED >**

|  |  |  |
| --- | --- | --- |
| **ID-nummer** | **Enhedsmedie** (USB, harddisk, bærbar e.l.) | **Datasikringsformat** |
| **Indhold på mediet**  |
| **Hashing algoritme** | **Hashværdi** |
| **Login** (hvis relevant) | **Kodeord** (hvis relevant) |
| **Kryptering & kode til dekryptering** (hvis relevant) | **Recoverykode** (hvis relevant) |

**INFO OM DEN DATASIKREDE ENHED >**

|  |  |  |
| --- | --- | --- |
| **ID-nummer** | **Enhedsmedie** (USB, harddisk, bærbar e.l.) | **Datasikringsformat** |
| **Indhold på mediet**  |
| **Hashing algoritme** | **Hashværdi** |
| **Login** (hvis relevant) | **Kodeord** (hvis relevant) |
| **Kryptering & kode til dekryptering** (hvis relevant) | **Recoverykode** (hvis relevant) |

**INFO OM DEN DATASIKREDE ENHED >**

|  |  |  |
| --- | --- | --- |
| **ID-nummer** | **Enhedsmedie** (USB, harddisk, bærbar e.l.) | **Datasikringsformat** |
| **Indhold på mediet**  |
| **Hashing algoritme** | **Hashværdi** |
| **Login** (hvis relevant) | **Kodeord** (hvis relevant) |
| **Kryptering & kode til dekryptering** (hvis relevant) | **Recoverykode** (hvis relevant) |

**INFO OM DEN DATASIKREDE ENHED >**

|  |  |  |
| --- | --- | --- |
| **ID-nummer** | **Enhedsmedie** (USB, harddisk, bærbar e.l.) | **Datasikringsformat** |
| **Indhold på mediet**  |
| **Hashing algoritme** | **Hashværdi** |
| **Login** (hvis relevant) | **Kodeord** (hvis relevant) |
| **Kryptering & kode til dekryptering** (hvis relevant) | **Recoverykode** (hvis relevant) |