|  |
| --- |
| **Risikovurdering av personopplysninger** |
| **Virksomhet:**  | **Avdeling:**  |
| **Tjeneste-/systemeier (risikoeier):**  | **Telefon/epost:** |
| **Hva er risikovurdert:** | **Hva er lagret hvor (personopplysninger):**(Dokumentet bør lagres som en del av internkontrollen i virksomheten) |
| **Vurdert av:** **Dato:**  | **Avdeling:** | **Telefon/epost:** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Forhold (uønsket hendelse) som er vurdert** Legg til de forhold som er vurdert.Hendelse 1 til 6 er eksempler som kan endres. | **Betydning****for**Sett kryss | **Risikonivå (L,M,H)**Sannsynlighet (horisontalt)Konsekvens (vertikalt)Sett ett kryss. | **Nødvendig med tiltak****(Ja/Nei)** |
| **1** | Uvedkommende kan kjenne igjen opplysninger i filen, da den ikke er tilstrekkelig avidentifisert | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **2** | Koblingsnøkkel er ikke forsvarlig sikret | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **3** | Uønsket utlevering av personopplysninger  | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **4** | Tap eller tyveri av fil lagret på bærbart utstyr | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **5** | Data er utilgjengelig for saksbehandler over en lengre periode | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **6** | Uønsket endring som ikke er sporbar | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **7** |  | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **8** |  | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **9** |  | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **10** |  | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **11** |  | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **12** |  | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **13** |  | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **14** |  | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **15** |  | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |
| **16** |  | \_\_Konfidensialitet\_\_Integritet\_\_Tilgjengelighet |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

 |  |

|  |  |  |
| --- | --- | --- |
| **Beskrivelse av tiltak***(I prioritert rekkefølge. Føy til flere linjer ved behov)* | **Ref. linjenummer over** | **Betydning/Kommentar** |
| **1** |  |  |   |
| **2** |  |  |  |
| **3** |  |  |  |
| **4** |  |  |  |
| **5** |  |  |  |
| **6** |  |  |  |
| **7** |  |  |  |
| **8** |  |  |  |
| **9** |  |  |  |
| **10** |  |  |  |

**Veiledning for enkel risikovurdering av personopplysninger**

Før personopplysninger behandles skal du foreta en risikovurdering.

På grunnlag av risikovurderingen skal du iverksette sikringstiltak som sørger for at opplysningene er godt nok beskyttet.

Risikovurderinger av informasjonssikkerheten handler om to ting:

* å identifisere hendelser som kan føre til at personopplysninger blir utsatt for brudd på:
	+ **Konfidensialitet:** uvedkommende får tilgang til personopplysninger
	+ **Integritet:** uønsket endring, sletting eller manipulering av personopplysninger og
	+ **Tilgjengelighet:** sikre brukere tilgang til personopplysninger når de har behov for det.
* å vurdere sannsynlighet og konsekvens ved at hendelsen inntreffer som:
	+ lav
	+ moderat
	+ høy

I kolonnen for risikonivå setters ett kryss ruten som angir hendelsens konsekvens og sannsynlighet:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Konsekvens | Høy |  | X |  |
| Moderat |  |  |  |
| Lav |  |  |  |
|  | Lav | Moderat | Høy |
|  |  | Sannsynlighet |

Man kommer da frem til risikonivået for hendelsen: Lav (grønn), Moderat (gul) og Høy (rød).

Hvis risikonivået er høyt må man alltid sette inn tiltak. Dette kan vurderes hvis nivået er moderat.

Både tilsiktede (hacking, virus etc.) og utilsiktete hendelser (teknisk og menneskelige feil) må tas med i vurderingen.

Dette er eksempler på faktorer med betydning for risikovurderingen:

* type opplysning (f.eks. om det er sensitive personopplysninger)
* grad av personidentifisering (direkte eller indirekte personopplysninger)
* antall registrerte
* oppbevaringstid
* den tekniske sikkerheten til systemet eller tjenesten som brukes
* kvaliteten på driften av den digitale tjenesten med underliggende systemer, for eksempel:
	+ sikkerhet hos driftsleverandør og eventuelle underleverandører
	+ datalokasjon

Etter at risikovurderinger er gjennomført skal det iverksettes sikringstiltak som forebygger hendelser med uakseptabel høy risiko. Tiltakene kan være tekniske, organisatoriske eller menneskelige.