**IT-säkerhetsredovisning**

**fristående arbetsstation**

|  |  |  |
| --- | --- | --- |
| Företagets sekretessmarkering | FMV:s diariemarkering | FMV:s sekretessmarkering |

|  |
| --- |
| **Företagsnamn** |
| Klicka här för att ange text. |
| **Verksamhetsställe (gatuadress)** |
| Klicka här för att ange text. |
| **Verksamhetsställe (postnr, postort)** |
| Klicka här för att ange text. |

**Innan Du börjar fylla i redovisningen: tag del av instruktionen längst bak i detta dokument.**

Innehållsförteckning

[1. Verksamhetsställe 3](#_Toc195607139)

[1.1. Adress och telefon 3](#_Toc195607140)

[1.2. IT-säkerhetsorganisation 3](#_Toc195607141)

[2. Systemets högsta säkerhetsskyddsklass 3](#_Toc195607142)

[3. Analys (§ 6.1. i ISM 2022) 3](#_Toc195607143)

[4. Autentisering (§ 6.2.3. i ISM 2022) 3](#_Toc195607144)

[5. Administrativa krav (§ 6.2.2. i ISM 2022) 4](#_Toc195607145)

[6. Specifika krav (§ 6.2.3. i ISM 2022) 4](#_Toc195607146)

[7. Rekommendationer (§ 6.2.4. i ISM 2022) 6](#_Toc195607147)

[8. Övrigt 6](#_Toc195607148)

[9. Bilagor 6](#_Toc195607149)

[9.1. Obligatoriska bilagor 6](#_Toc195607150)

1. Verksamhetsställe

## Adress och telefon

|  |
| --- |
| **Organisationsnummer** |
| Klicka här för att ange text. |
| **Företagsnamn** |
| Klicka här för att ange text. |
| **Postadress** |
| Klicka här för att ange text. |
| **Verksamhetsställe (besöksadress)** |
| Klicka här för att ange text. |
| **Telefonnummer (växel)** |
| Klicka här för att ange text. |

## IT-säkerhetsorganisation

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **IT-säkerhetschef** | **Telefon** | **E-postadress** | | | | |
| Klicka här för att ange text. | Klicka här för att ange text. | Klicka här för att ange text. | | | | |
| **IT-administratör/motsv.** | **Telefon** | **E-postadress** | | | | |
| Klicka här för att ange text. | Klicka här för att ange text. | Klicka här för att ange text. | | | | |
| **IT-administratör/motsv.** | **Telefon** | **E-postadress** | | | | |
| Klicka här för att ange text. | Klicka här för att ange text. | Klicka här för att ange text. | | | | |
| **Finns befattningsbeskrivningar för samtliga roller?** | | | **Ja** |  | **Nej** |  |

1. Systemets högsta säkerhetsskyddsklass

|  |  |  |  |
| --- | --- | --- | --- |
| **KVALIFICERAT HEMLIG** |  | **HEMLIG** |  |
| **KONFIDENTIELL** |  | **BEGRÄNSAT HEMLIG** |  |

1. Analys (§ 6.1. i ISM 2022)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Har företaget gjort en dokumenterad särskild säkerhetsskyddsanalys**  **(säkerhetsskyddsbedömning) för IT-systemet** | **Ja** |  | **Nej** |  |

1. Autentisering (§ 6.2.3. i ISM 2022)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Uppfyller lösenorden kraven på längd och utformning?** | **Ja** |  | **Nej** |  |
| **Finns separat administratörskonto i det fall användaren är administratör?** | **Ja** |  | **Nej** |  |
| **Har alla användare och administratörer personliga (unika) konton och lösenord?** | **Ja** |  | **Nej** |  |
| **Används användarnamn och lösenord för behörighetskontroll (upp till och med informationssäkerhetsklass BEGRÄNSAT HEMLIG)?** | **Ja** |  | **Nej** |  |
| **Används TEID-kort och lösenord för behörighetskontroll (från och med informationssäkerhetsklass KONFIDENTIELL)?** | **Ja** |  | **Nej** |  |

1. Administrativa krav (§ 6.2.2. i ISM 2022)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Har företaget en skriftlig rutin för användare av arbetsstationen?** | **Ja** |  | **Nej** |  |
| **Har företaget en skriftlig rutin för support av arbetsstationen?** | **Ja** |  | **Nej** |  |
| **Innehåller rutinerna minst följande information?** | | | | |
| **Uppsättning och hantering av arbetsstation före överlämning** | **Ja** |  | **Nej** |  |
| **Uppdatering av programvara** | **Ja** |  | **Nej** |  |
| **Uppdatering av definitionsfiler till skyddet mot skadlig kod** | **Ja** |  | **Nej** |  |
| **IT-support** | **Ja** |  | **Nej** |  |
| **Behörighetstilldelning** | **Ja** |  | **Nej** |  |
| **Administrativa rättigheter** | **Ja** |  | **Nej** |  |
| **Hantering av in- och utdata inklusive utskrifter** | **Ja** |  | **Nej** |  |
| **Tillåtna lagringsmedier** | **Ja** |  | **Nej** |  |
| **Tillåtna externa anslutningar** | **Ja** |  | **Nej** |  |
| **Skydd mot röjande signaler (RÖS)** | **Ja** |  | **Nej** |  |
| **Backuptagning** | **Ja** |  | **Nej** |  |
| **Loggning** | **Ja** |  | **Nej** |  |
| **Logguppföljning** | **Ja** |  | **Nej** |  |
| **Säkerhetsincidenter** | **Ja** |  | **Nej** |  |
| **Hantering och förvaring** | **Ja** |  | **Nej** |  |
| **Destruktion** | **Ja** |  | **Nej** |  |
| **Är de skriftliga rutinerna lätt tillgängliga för all personal?** | **Ja** |  | **Nej** |  |

1. Specifika krav (§ 6.2.3. i ISM 2022)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Om arbetsstationen används av mer än en användare, är alla behöriga att ta del av all information som hanteras i arbetsstationen?** | **Ja** |  | **Nej** |  |
| **Hålls antalet administratörer för arbetsstationen till ett absolut minimum?** | **Ja** |  | **Nej** |  |
| **Är IT-supportpersonal säkerhetsprövad och registerkontrollerad för uppdraget?** | **Ja** |  | **Nej** |  |
| **Är stationens nätverkstjänster avstängda och är den inbyggda brandväggen konfigurerad att förhindra in- och utgående kommunikation?** | **Ja** |  | **Nej** |  |
| **Övervakas supportpersonalens arbete med arbetsstationen under hela tiden support pågår?** | **Ja** |  | **Nej** |  |
| **Är diskkryptering aktiverad?** | **Ja** |  | **Nej** |  |
| **Vilken typ av diskkryptering används?** | | | | |
| Klicka här för att ange text. | | | | |
| **Är BIOS lösenordskyddat och dess lösenord förvaltat och förvarat av säkerhetsorganisationen?** | **Ja** |  | **Nej** |  |
| **Är säkerhetsfunktionens logg aktiverad?** | **Ja** |  | **Nej** |  |
| **Är säkerhetsloggen endast tillgänglig för administratör/IT-support?** | **Ja** |  | **Nej** |  |
| **Redogör för säkerhetsloggens innehåll** | | | | |
| Klicka här för att ange text. | | | | |
| **Lagras loggdata i minst sex (6) månader?** | **Ja** |  | **Nej** |  |
| **Är arbetsstationens mjukvarubrandvägg påslagen?** | **Ja** |  | **Nej** |  |
| **Är användaren genom kvittens medveten om sitt ansvar för alla uppgifter som behandlas i stationen och alla händelser i detsamma?** | **Ja** |  | **Nej** |  |
| **Var och hur regleras detta ansvar?** | | | | |
| Klicka här för att ange text. | | | | |
| **Ansvarar användaren för säkerhetskopiering?** | **Ja** |  | **Nej** |  |
| **Var och hur regleras detta ansvar?** | | | | |
| Klicka här för att ange text. | | | | |
| **Är USB-gränssnitt blockerade så långt möjligt?** | **Ja** |  | **Nej** |  |
| **Hanteras och förvaras in- och utdata som säkerhetsskyddsklassificerad uppgift i enlighet med regelverket i Industrisäkerhetsskyddsmanualen (ISM)?** | **Ja** |  | **Nej** |  |
| **Hanteras och förvaras lagringsmedier som säkerhetsskyddsklassificerad uppgift i enlighet med regelverket i Industrisäkerhetsskyddsmanualen (ISM)?** | **Ja** |  | **Nej** |  |
| **Är användarens ansvar för kontroll av hårdvara reglerat, med avseende på manipulation av till exempel dockningsstation/motsvarande?** | **Ja** |  | **Nej** |  |
| **Är stationen försedd med godkänd skyddsfunktion mot skadlig kod?** | **Ja** |  | **Nej** |  |
| **Beskriv hur detta skydd är utformat** | | | | |
| Klicka här för att ange text. | | | | |
| **Är stationen försedd med godkänd skyddsfunktion mot RÖS?** | **Ja** |  | **Nej** |  |
| **Beskriv hur RÖS-skyddet är utformat. Om systemet endast skall hantera upp till och med säkerhetsskyddsklass BEGRÄNSAT HEMLIG skall detta anges tydligt.** | | | | |
| Klicka här för att ange text. | | | | |
| **Sker fortlöpande utbildning i IT-säkerhet och IT-stöd?** | **Ja** |  | **Nej** |  |
| **Är utbildningen inlagd i företagets utbildningsplan?** | **Ja** |  | **Nej** |  |
| **Beskriv utbildningens innehåll och genomförande** | | | | |
| Klicka här för att ange text. | | | | |
| **Dokumenteras alla förändringar i system och programvara?** | **Ja** |  | **Nej** |  |

1. Rekommendationer (§ 6.2.4. i ISM 2022)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Har endast IT-support administrativa rättigheter?** | **Ja** |  | **Nej** |  |
| **Finns särskild dator (”tvättmaskin”) för all hantering av in- och utdata?** | **Ja** |  | **Nej** |  |

1. Övrigt

|  |
| --- |
| Klicka här för att ange text. |

1. Bilagor
   1. Obligatoriska bilagor
2. Användarinstruktion för systemet (avsedd för användare av systemet)
3. Uppsättnings-, härdnings- och supportinstruktion för systemet (avsedd för IT-supportpersonal)

**Instruktion för ifyllnad**

IT-säkerhetsredovisningen utgör ett företags redovisning av sin IT-säkerhet med avseende på hantering av säkerhetskänslig verksamhet i IT-miljö, eller digital hantering och förvaring av säkerhetsskyddsklassificerad uppgift i fristående arbetsstation. Redovisningen skall alltid hållas aktuell och skall tillställas FMV på begäran.

Kraven på företagets säkerhetsskyddsverksamhet framgår av företagets säkerhetsskyddsavtal och av Industrisäkerhetsskyddsmanualen, ISM.

Redovisningen måste vara fullständigt ifylld. Rubriker får inte tas bort. Extra information kan, om företaget så önskar, anges under punkt 8.

Angivna obligatoriska bilagor skall bifogas redovisningen. Bilägg inga andra dokument än de som efterfrågas.

**Framsida**

Fyll i företagets fullständiga namn samt det verksamhetsställe redovisningen gäller. Om det finns flera byggnader som delar samma adress, till exempel inom ett industriområde, ange även vilken byggnad det gäller.

**Befordran**

Ifylld IT-säkerhetsredovisning med bilagor insändes med VÄRDE-post till FMV Säkerhetsskydd, 115 88 STOCKHOLM. Ett följebrev skall biläggas dokumentationen. Av följebrevet skall tydligt framgå FMV:s diarienummer för det aktuella ärendet.