IT-säkerhetskrav för fristående arbetsstation/enanvändarsystem

Innehållsförteckning

1. Definition

En fristående arbetsstation för hantering och förvaring av säkerhetsskyddsklassificerad uppgift är ett IT-system som utgörs av en dator, bärbar eller stationär, med eller utan löstagbar hårddisk. Arbetsstationen kan förekomma i fyra olika varianter:

1. en dator som används av bara en användare, utan åtkomst av servicetekniker eller liknande (enanvändarsystem).
2. en dator som används av bara en användare men med åtkomst av servicetekniker eller liknande.
3. en dator med flera användare som använder samma hårddisk, men med personlig autentisering.
4. en dator (dockningsstation/motsvarande) med flera användare, som dock tilldelats personlig hårddisk.

Vidare gäller för fristående arbetsstation att den:

- inte får vara ansluten till något kommunikationsnät och
- bara får använda lagringsmedier för regelbundet informationsutbyte med andra IT-system. För informationsutbyte skall så långt möjligt CD/DVD användas. USB-minnen får endast användas om CD/DVD av tekniska skäl inte kan nyttjas.

2. Allmänt

Om arbetsstationen används av flera användare, inklusive IT-supporttjänster som inte utförs av användaren själv, gäller regelverket för gemensam förvaring av säkerhetsskyddsklassificerad uppgift, det vill säga att alla användare skall vara behöriga till all information som hanteras och förvaras i arbetsstationen.

Kraven i denna handling omfattar alla fristående arbetsstationer och enanvändarsystem med information som placerats upp till och med säkerhetsskyddsklass HEMLIG.

Avsteg från dessa krav medges ej.

3. Autentisering

En fristående arbetsstation enligt definitionens punkt 1 ovan, skall minst förses med autentisering med starkt lösenord.

- Enskild användares lösenord skall innehålla gemener, versaler och siffror samt vara minst åtta (8) tecken långt.
- Lösenordet för administrativt konto (IT-support) skall innehålla gemener, versaler och siffror samt vara minst tolv (12) tecken långt.

En användare som själv ansvarar för support skall ha ett separat administrativt konto enligt ovan. Enskild användare får endast ha användarrättigheter. Om användaren även är

administratör av arbetsstationen (bör om möjligt undvikas), skall ett separat administratörskonto användas vid administration av den fristående arbetsstationen.

Alla användare och administratörer skall ha personliga (unika) konton och lösenord.

En fristående arbetsstation, som endast skall hantera och förvara säkerhetsskyddsklassificerad uppgift upp till och med säkerhetsskyddsklass BEGRÄNSAT HEMLIG, behöver endast förses med autentisering enligt ovan. Detta gäller även om flera användare delar på stationen enligt definitionens punkt 2-4 ovan.

För en fristående arbetsstation enligt variant 2-4 ovan, som skall hantera och förvara säkerhetsskyddsklassificerad uppgift från säkerhetsskyddsklass KONFIDENTIELL och uppåt, skall tvåfaktorsautentisering användas. Autentisering skall därvid ske med TEID-kort. Kort och programvara för tvåfaktorsautentisering beställs av FMV:s projektledare efter framställan från företaget.

4. Administrativa krav

Företaget skall ha skriftliga rutiner för all hantering av den fristående arbetsstationen. Rutinerna kan vara en del av företagets säkerhetsskyddsinstruktion. Rutinerna, som skall vara skrivna för det aktuella företaget och/eller verksamhetsstället, skall reglera ansvaret för arbetsstationen och skall minst omfatta (men ej begränsas till) följande områden:

- Uppsättning och härdning av arbetsstation före överlämning till användare
- Uppdatering av programvara
- Uppdatering av definitionsfil till skyddet mot skadlig kod
- Hur IT-support skall ske
- Behörighetstilldelning, samt skriftligt beslut om tilldelning av behörighet till arbetsstation. Behörighetsbegreppet förklaras i 2. kap 3 § Säkerhetsskyddsförordningen (2018:658) samt av Industrisäkerhetsskyddsmanualen (ISM).
- Administrativa rättigheter
- Hantering av in- och utdata inkl. utskrifter
- Tillåtna lagringsmedier
- Tillåtna anslutningar, till exempel skrivare och PC-projektor, skärmar, etc.
- Skydd mot röjande signaler (RÖS)
- Backuptagning
- Loggning
- Logguppföljning
- Säkerhetsincidenter
- Hantering och förvaring
- Destruktion

Rutinerna skall vara så utformade att de lätt kan följas av den enskilde användaren efter utbildning i IT-säkerhet och IT-stöd. De skall vara utformade som en utförandeinstruktion och beskriva vem som gör vad, när och hur. Rutinerna skall vara lätt tillgängliga för all personal.

Rutinerna får inte utgöra en kopia av detta kravdokument, utan skall vara utformade med företagets egna ord och beskriva den egna verksamheten.

Rutinerna skall delas upp i två olika rutiner; en för användaren som vederbörande får vid kvittens av arbetsstationen (inklusive lagringsmedia) och en rutin för IT-supporten som beskriver uppsättning, härdning och support.

5. Specifika krav

Om arbetsstationen används av mer än en användare skall alla användare vara behöriga att ta del av all information som lagras i arbetsstationen.

Antalet administratörer (IT-support) på arbetsstationen skall hållas till ett minimum.

IT-supportpersonal skall vara säkerhetsprövad och registerkontrollerad för uppdraget i enlighet med företagets säkerhetsskyddsavtal.

Alla nätverkstjänster skall stängas av och eventuell inbyggd brandvägg skall konfigureras till att inte tillåta inkommande och utgående kommunikation.

Om användaren, efter att denne börjat använda systemet för behandling av säkerhetsskyddsklassificerad uppgift, behöver hjälp av IT-support får användaren inte lämna datorn ifrån sig. Supportpersonalens arbete med systemet skall hela tiden övervakas av användaren.

Om Bitlocker eller motsvarande diskkryptering finns installerad, skall det aktiveras och användas som komplement till behörighetskontrollen i syfte att fungera som ett stöldskydd. Om Microsoft Windows används som operativsystem erfordras Windows Pro.

BIOS skall förses med lösenordsskydd. Endast behörig administratör får ha tillgång till detta lösenord, som skall förvaltas och förvaras av säkerhetsorganisationen vid företaget.

Ett enanvändarsystem bör innehålla säkerhetsfunktionen för säkerhetslogg. Om arbetsstationen används av mer än en användare skall säkerhetslogg finnas. Säkerhetsloggen skall endast kunna administreras och läsas av administratör/IT-support.

Krav på loggens innehåll framgår av Industrisäkerhetsskyddsmanualen (ISM) bilaga 3, Krav på säkerhetsfunktioner (KSF) 3.1. för respektive säkerhetsskyddsklass. Loggen skall anpassas till kraven enligt den högsta säkerhetsskyddsklass som arbetsstationen skall kunna hantera.

Loggdata skall lagras i minst sex (6) månader.

Arbetsstationens mjukvarubrandvägg skall vara påslagen.

Användaren är ansvarig för alla uppgifter som behandlas i IT-systemet och alla händelser i systemet och skall göras medveten om detta vid kvittens av arbetsstationen.

Användaren ansvarar för att genomföra säkerhetskopiering av de uppgifter som behandlas i enanvändarsystemet. Säkerhetskopian skall hanteras som säkerhetsskyddsklassificerad uppgift enligt regler för den högsta säkerhetsskyddsklass som någon information på säkerhetskopian har. Säkerhetskopiering kan ske till CD/DVD-skiva eller USB-minne.

USB-gränssnitt skall så långt möjligt blockeras, möjligen med undantag för anslutning av skärm, mus, tangentbord, CD-brännare/-läsare och skrivare samt ev. USB-minne för säkerhetskopiering och Bitlocker-nyckel.

All in- och utdata inklusive utskrifter som innehåller säkerhetsskyddsklassificerad uppgift skall hanteras och förvaras i enlighet med regelverket i ISM, till exempel registrering, märkning, kvittering, hantering, förvaring, inventering, återlämning, destruktion, befordran, medförande, transport, etc.

Alla lagringsmedier som innehåller säkerhetsskyddsklassificerad uppgift skall hanteras och förvaras i enlighet med regelverket i ISM, till exempel registrering, märkning, kvittering, hantering, förvaring, inventering, återlämning, destruktion, befordran, medförande, transport, etc.

Hårdvara som används för dockning av hårddisk och/eller motsvarande utrustning med samma användningsområde, skall hanteras och förvaras så att den skyddas mot tillgrepp och manipulation. För sådan hårdvara ansvarar säkerhetsorganisationen, men det åvilar varje användare att kontrollera hårdvaran med avseende på manipulation innan arbete med säkerhetsskyddsklassificerad uppgift sker.

Ett enanvändarsystem skall vara försett med en godkänd säkerhetsfunktion för skydd mot skadlig kod i enlighet med KSF-regelverket i ISM.

Ett enanvändarsystem som skall användas för behandling av säkerhetsskyddsklassificerad uppgift skall vara försett med en godkänd säkerhetsfunktion för skydd mot röjande signaler (RÖS) om en analys enligt KSF 3.1. ger vid handen att RÖS-skydd erfordras. RÖS-skydd erfordras ej om arbetsstationen hanterar information som placerats i högst säkerhetsskyddsklass BEGRÄNSAT HEMLIG.

Fortlöpande utbildning i IT-säkerhet och IT-stödet skall ske och utgöra en del av företagets årligen uppdaterade utbildningsplan.

Dokumentation skall föras över alla förändringar som görs i systemet och i de använda programvarorna.

6. Redovisning

Företaget skall redovisa sitt IT-säkerhetsskydd genom insändande av bilaga 4 till säkerhetsskyddsrevisionen, kallad granskningsunderlag IT-system. För ändamålet finns en mall tillgänglig via FMV:s webbplats. Mallen är obligatorisk och skall användas. FMV äger rätt att begära ytterligare dokumentation om så erfordras.

7. Rekommendationer

Endast IT-support bör ha administrativa rättigheter.

Om arbetsstationen skall hantera information med säkerhetsskyddsklass KONFIDENTIELL eller högre bör en separat dator finnas för all hantering av in- och utdata inklusive kontroll mot skadlig kod och loggning av all in- och utdata i arbetsstationen. Syftet är att säkerställa att programuppdateringar, etc. inte för med sig skadlig kod in i arbetsstationen. Denna dator skall hanteras och förvaras som säkerhetsskyddsklassificerad uppgift och med samma behörighetskrav som arbetsstationen.