Datum
2018-05-14

Diarienr/Projektnr
Ä 2018-82

Upprättad av
Gunnar Wennerholm

Godkänd av
Lena Carlsson

Version
2.0

Tillväxtverkets interna regler (2017:4) om informationssäkerhet

Tillväxtverkets tillämpning av MSBFS 2016:1 och ISO/IEC 27001:2014 och 27002:2014

Detta styrdokument konkretiserar Tillväxtverkets informationssäkerhetspolicy och beskriver myndighetens tillämpning av föreskriften MSBFS 2016:1 och standarderna ISO/IEC 27001:2014 och ISO/IEC 27002:2014. Målet för Tillväxtverkets informationssäkerhetsarbete är att säkerställa konfidentialitet, riktighet och tillgänglighet i verksamhetens information.

Dokumentet innehåller dels interna regler som ska följas av respektive ansvarig, dels plan med uppföljningsbara krav och mål för att säkra att informationssäkerhetsarbetet är ändamålsenligt. Både interna regler samt krav och mål är sorterade under de säkerhetsområdena som anges i ovan nämnda standarder. Interna regler har paragrafnumrering. Krav och mål identifieras med löpnummer inom aktuellt avsnitt.

De interna reglerna och kraven vänder sig till chefer och medarbetare på Tillväxtverket och berör även externa användare samt leverantörer av it-tjänster och it-produkter. Reglerna har beslutats av Lena Carlsson. Gunnar Wennerholm har varit föredragande.

Inledning

En säker informationsförsörjning är avgörande för Tillväxtverkets förmåga att uppnå verksamhetsmålen. Informationssäkerheten är den samlade effekten av organisatoriska, administrativa och tekniska åtgärder som vidtas för att skydda informationstillgångar. Informationssäkerhetsarbetet ska leda till ändamålsenliga säkerhetslösningar och vara anpassat till skyddsvärde, risk, lagkrav och standarder och möjliggöra för verksamheten att uppnå sina mål.

Utvecklingen av informationsteknik är snabb och dynamisk och säkerhetsarbetet bör baseras på ett synsätt med ständiga förbättringar utifrån fortlöpande riskbedömningar. De krav som sätts upp här ska följas upp och förbättringsåtgärder vidtas vid brister. Status på säkerhetsarbetet ska regelbundet gås igenom med Tillväxtverkets ledning.

Styrdokumentet utgår från vad som föreskrivs i Myndigheten för samhällsskydd och beredskaps (MSB) föreskrift MSBFS 2016:1, som anger att varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet, där standarderna ISO/IEC 27001:2014 och ISO/IEC 27002:2014 ska beaktas. En anpassning har gjorts utifrån Tillväxtverkets verksamhet men strukturen följer standardernas upplägg (avsnitt 1–14 här motsvaras av standardernas avsnitt 5–18). Standarderna kan konsulteras i de fall det behövs en precisering av vad som anges i detta styrdokument. Dataskyddslagstiftningen som följer av GDPR har också beaktats, men för mer specifika instruktioner hänvisas till andra dokument.

1 Styrdokument för informationssäkerhet

Krav och mål

1.1 Styrdokument för Tillväxtverkets informationssäkerhet ska vara godkända och kommunicerade till anställda och relevanta parter. De ska regelbundet kontrolleras så att de har god aktualitet.

2 Organisation av informationssäkerheten

Krav och mål

2.1 Ansvar för informationssäkerhet utgår från verksamhetsansvaret, där ägaren av en informationsresurs är ansvarig för dess säkerhet. Ytterst är generaldirektören ansvarig. Specifika ansvarsroller för informationssäkerhet ska vara definierade i arbetsordning. Ansvar och ansvarsområden som kan ha motstridiga intressen bör vara åtskilda. Informationssäkerhetsansvarig svarar för ledning och samordning och ska till sitt stöd ha en intern informationssäkerhetsgrupp. Av dataskyddslagstiftningen framgår dataskyddsombudets ansvar i att övervaka att dataskyddsförordningen följs. Av arbetsordningen ska framgå att it-chefen ansvarar för it-säkerheten, chefen för intern service ansvarar för fysisk säkerhet och att varje medarbetare utöver detta har ett ansvar för informationssäkerheten utifrån sitt arbets- och ansvarsområde.

2.2 Samverkan ska ske med relevanta myndigheter, specialister och andra externa grupper för att säkra aktualitet i informationssäkerhetsarbetet.

3 Personal och säkerhet

Intern regel

1 §	Ansvarig chef har ansvar för att nya och utomstående användare kontrolleras enligt rutin. Detta ska framgå av arbetsordningen.

Krav och mål

3.1 Det ska finnas rutiner för att upprätthålla en god nivå av säkerhetsmedvetande hos medarbetare vid nyanställning, under anställning och när en anställning upphör, liksom för extern personal och utomstående användare. Medarbetare ska ha genomgått grundläggande utbildning inom informationssäkerhet samt ytterligare utbildning där arbetsuppgifterna så kräver.

3.2 Det ska finnas rutiner för kontroll av nya och utomstående användare inför anställningens eller engagemangets start. Det ska finnas rutiner för att utrustning och passerkort återlämnas och behörigheter avslutas vid avslut av anställning eller engagemang. Ansvar efter ett engagemang ska tydliggöras.

3.3 Det ska finnas en formell disciplinär process för åtgärder mot anställda som har brutit mot regler som är kopplade till informationssäkerheten.

4 Hantering av tillgångar

Interna regler

System och informationsmängder

2 § Informationssäkerhetsansvarig ska tillse att Tillväxtverkets system finns förtecknade och har utsedda ansvariga.

3 § Systemägaren ska tillse att de informationsmängder som man har ansvar för informationsklassas enligt Tillväxtverkets angivna modell samt att riskanalyser regelbundet genomförs.

4 § Systemägaren ska tillse att det finns en aktuell förvaltningsplan och systemdokumentation för it-systemet.

5 § Om personuppgifter behandlas i ett land utanför EU/EES ska personuppgiftsansvarig se till att undantag från förbudet mot överföring till tredje land kan tillämpas. Externa tjänster bör som grundregel inte upphandlas om det är oklart var personuppgifter kommer att lagras eller bearbetas.

Användarens utrustning och information

6 § Tillväxtverkets dator och telefon är arbetsverktyg. Privat användning av dessa är tillåten under förutsättning att det inte negativt påverkar utförandet av arbetsuppgifterna och inte innebär extra kostnader eller andra negativa konsekvenser för Tillväxtverket.

7 §	Medarbetare ska i arbetet i första hand använda Tillväxtverkets utrustning. Användning av andra enheter är tillåten där it-enheten tillhandahåller eller har godkänt en teknisk lösning för detta (som RSA-dosa eller MDM-lösning).
8 §	Det är inte tillåtet att besöka webbplatser med diskriminerande, rasistiskt, pornografiskt eller annat olämpligt eller olagligt innehåll.
9 §	It-utrustningen ska hanteras så att risken minimeras att obehöriga får tillgång till den. Förlust av it-utrustning ska snarast anmälas till it-enheten. Vid stöld av utrustning ska polisanmälan också göras, i normalfallet av den anställde.
10 §	Användarna ska se till att datorer och mobila enheter är skärmlåsta när de är på men inte används. Information som är känslig får inte lämnas obevakad.
11 §	It-systemens skyddsmekanismer ska hållas uppdaterade och får inte avaktiveras. Mobila enheter ska vara anslutna till Tillväxtverkets MDM-lösning. Om skadlig kod eller andra hot på enheterna upptäcks ska it-enheten kontaktas.
12 §	Endast Tillväxtverkets egen utrustning får anslutas till det interna nätverket. Eventuella undantag ska valideras av it-enheten.
13 §	Information med högt skyddsvärde för konfidentialitet ska inte förmedlas, lagras eller hanteras i någon extern tjänst, såvida inte särskilda skyddsåtgärder vidtagits som kryptering, säkrad åtkomstkontroll och juridiskt kvalitetssäkrade avtal med leverantören. Detta gäller följande: *sekretessreglerad information enligt OSL, känsliga personuppgifter eller information som kan skada Tillväxtverket eller tredje man om den sprids*.
14 §	Medarbetare ska hålla en tydlig åtskillnad mellan arbetsrelaterad och privat information. E-postadressen på Tillväxtverket bör inte användas i privata sammanhang.
15 §	Personuppgifter ska behandlas enligt tillämplig dataskyddslagstiftning och enligt Tillväxtverkets regler och anvisningar.
16 §	Tillväxtverkets regler för dokumenthantering ska följas. Allmänna handlingar får enbart gallras enligt gallringsplaner eller efter särskilt beslut. Arbetsmaterial och liknande dokument kan rensas vid behov.

Krav och mål

4.1	Information i samarbeten med externa aktörer, som inte är känslig och som betraktas som offentlig handling, får hanteras i molntjänst, med normal aktsamhet men utan formella restriktioner. E-post ska betraktas som oskyddad och med risk att andra än avsedd mottagare tar del av innehållet. Arbetsmaterial som görs tillgängligt utanför Tillväxtverket blir normalt allmän handling. Arbetsmaterial som bör behålla sin status som arbetsmaterial/internt material ska därför inte göras tillgängligt utanför Tillväxtverket.
4.2	Det ska finnas anvisningar för hantering av informationen utifrån informationsklassningen. Informationens skyddsvärde bestäms utifrån beskrivningen av den konsekvens som kan uppstå vid en brist i hanteringen.
4.3	I förvaltningsplanen eller i annan dokumentation ska systemets ändamål samt informationens klassning framgå. Dokumentation som innehåller känslig information ska förvaras så att den endast är åtkomlig för behörig personal.
4.4	Säkerheten ska bibehållas för den information som görs åtkomlig för eller styrs av utomstående parter.

4.5 Av dataskyddsförordningen framgår att den personuppgiftsansvarige, dvs. i detta fall Tillväxtverket, ska föra en förteckning över de personuppgiftsbehandlingar som myndigheten utför. Dessutom ska ett personuppgiftsbiträde föra en förteckning över den behandling som de utför för någon annans räkning. I samband med insamling av personuppgifter ska den enskilde informeras om sina rättigheter.

4.6 Personuppgifter bör användas i begränsad omfattning och endast utifrån rättslig grund och fastställt ändamål. Detta gäller oavsett medium och teknik och exempelvis även för fritext i e-post, chatt och i dokumentfiler. Personuppgifter bör raderas när deras syfte och ändamål inte längre är aktuellt, såvida det inte finns krav på att de ska sparas och arkiveras.

4.7 För att uppfylla Dataskyddsförordningens krav kan Tillväxtverket komma att genomsöka medarbetarnas information avseende personuppgifter.

4.8 Tillväxtverket ska upprätthålla god kvalitet och säkerhet i informations- och dokumenthanteringen. Allmänna handlingar ska registreras och sparas i enlighet med gällande lagstiftning och internt fastställda rutiner.

4.9 Loggning av händelser och datatrafik görs för driftövervakning och felsökning och medarbetarnas omfattning av användning av olika verktyg kan därmed komma att följas upp i syfte att förbättra drifteffektiviteten. Obehörig informationsbehandling, liksom andra hot ska kunna upptäckas i loggar. Medarbetares användning av it-system kan därför komma att följas upp vid misstanke om brott mot lag eller andra oegentligheter.

4.10 Ändringar i it-system ska planeras noga. Beslut fattas av systemägare i egenskap av behörig chef, i samråd med tekniskt ansvarig. Vid större och mer generella ändringar ska frågan lyftas till utvecklingsråd för rekommendation inför beslut.

5 Styrning av åtkomst

Krav och mål

5.1 Regler för styrning av åtkomst till data och system ska dokumenteras, exempelvis i det aktuella systemets förvaltningsplan. Åtkomstreglerna ska beskrivas för de typer av användare och aktörer som är berörda.

5.2 Registrering av användare och tilldelning av rättigheter, liksom för ändring och upphörande av dessa, ska ske enligt fastställda processer. Användarnas åtkomsträttigheter ska regelbundet följas upp.

5.3 Användarkonton ska vara personliga. Säkra lösenord ska användas. Endast i undantagsfall får opersonliga konton (eller motsvarande tillämpning) användas.

5.4 Åtkomst med utvidgade rättigheter, såsom administratörsrättigheter, ska begränsas till så få personer som möjligt.

5.5 Medarbetarnas datorer och mobila enheter ska vara inställda på att låsas automatiskt efter en viss tids inaktivitet, liksom utloggning ur system.

5.6 Mobil utrustning ska ha åtkomstskydd utifrån informationstillgångarnas skyddsbehov.

5.7 System för lösenordshantering ska vara interaktiva och säkerställa kvalitativa lösenord.

5.8 Rättsliga frågor, arbetssätt och åtkomstrestriktioner ska vara tydliggjorda för personal som arbetar med system med känslig information, exempelvis när det gäller sekretess, s.k. Eget utrymme mm.

6 Kryptering

Krav och mål

6.1 Kryptografiska säkerhetsåtgärder ska utnyttjas utifrån informationsmängdens skyddsvärde. Regler för användning, skydd och giltighetstid för kryptografiska nycklar ska finnas där krypto tillämpas.

7 Fysisk och miljörelaterad säkerhet

Krav och mål

7.1 Tillträdeskontroll ska finnas till lokaler där Tillväxtverkets information hanteras. Tillträde ska vara behovsbaserat och behörighetsstyrt. Besökare till Tillväxtverket utan egen behörighet ska ha en ansvarig besöksmottagare.

7.2 Informationsbehandling i Tillväxtverkets infrastruktur och servermiljö (dvs. inte medarbetares utrustning) får endast ske i lokaler med säkra tekniska försörjningssystem, och med redundans där så krävs, oavsett om det är drift i egen regi eller utkontrakterad.

7.3 Utrustning ska placeras och skyddas för att minska risker för hot, obehörig åtkomst samt störningar på grund av fel i tekniska försörjningssystem.

7.4 Utrustning ska underhållas korrekt för att säkerställa fortsatt funktionalitet.

7.5 Medarbetarnas utrustning med lagringsmedia ska före kassering eller återanvändning granskas av it-enheten så att känsliga data och program har avlägsnats eller överskrivits.

8 Driftsäkerhet

Krav och mål

8.1 Administration, drift och underhåll av it-system ska ske på ett strukturerat och systematiskt sätt, enligt en fastställd modell för systemförvaltning. Rutiner bör anges i en systemförvaltningsplan. Risk- och sårbarhetsanalyser bör genomföras regelbundet och inför viktiga förändringar.

8.2 Samma säkerhetsregler för drift ska gälla oavsett leverantör och driftplats. Vid nyttjande av extern leverantör ska Tillväxtverket ha rätt att genomföra revision av informationssäkerheten, alternativt att leverantören tillhandahåller dokumentation från annan part som genomfört säkerhetsrevision.

8.3 Driftsrutiner ska dokumenteras och finnas tillgängliga för användare som behöver dem. Det ska finnas rutiner för att styra installation i driftsystem. Förändringar av produktionsmiljön ska vara testade, godkända och dokumenterade. Leverantörers säkerhetsuppdateringar ska installeras skyndsamt.

8.4 Drift och användning av it-system ska övervakas för att säkerställa nödvändig prestanda och för att upptäcka hot. Loggar ska skyddas mot radering, manipulation och obehörig åtkomst.

8.5 It-system som skapar, levererar eller sparar logginformation ska vara tidssynkroniserade.

8.6 Utvecklings-, test- och driftmiljöer ska vara separerade på adekvat sätt.
8.7 Informationssystemen ska ha fullgott skydd mot skadlig kod.
8.8 Säkerhetskopior ska tas och testas regelbundet. Förvaring ska ske fysiskt åtskilt från original. Eventuell sekretess ska beaktas vid hantering av säkerhetskopior.

9 Kommunikationssäkerhet

Krav och mål

9.1 Säkerheten ska bibehållas hos information som utbyts inom Tillväxtverket och med extern part och, där så krävs, vara reglerad genom avtal.
9.2 Styrning, säkerhetsmekanismer och tjänstenivåer för nätverkstjänster ska identifieras och dokumenteras samt inkluderas i avtal om tjänsterna tillhandahålls av extern leverantör.

10 Anskaffning, utveckling och underhåll av system

Krav och mål

10.1 Informationssäkerhet ska vara en integrerad del av it-systemen. Inför nya eller förändrade informationssystem ska bedömning av säkerhetskrav ingå i kravanalysen. Utvecklings- och förändringsarbete ska ske enligt Tillväxtverkets angivna metoder eller enligt särskilt beslut om metod.
10.2 Planering för framtida avveckling av system bör göras i ett tidigt skede, där en bedömning bör göras om hur informationen ska hanteras vid systemets avveckling. Tillvägagångssätt framgår i Tillväxtverkets styrdokument för dokumenthantering.
10.3 Det ska finnas lämpliga skydd och tillämpningar för att förhindra fel, förlust, obehörig förändring eller missbruk av informationen i systemen. Åtkomst till databaser, filer och källkod till programmen ska styras.
10.4 Utvecklings- och testmiljöer ska styras så att säkerhetskraven är säkerställda på systemens program och den information som hanteras. Förändringar i driftsatta system ska styras i en formell dokumenterad ändringshantering. Detta gäller för såväl internt som externt utvecklingsarbete.
10.5 Testdata ska väljas ut noggrant, skyddas och styras. Produktionsdata med identifierbara personuppgifter ska avidentifieras innan de får återanvändas som exempelvis testdata i testmiljöer.
10.6 Avtal ska utformas så att Tillväxtverket erhåller ägande och övriga immateriella rättigheter till resultat i uppdrag. Om detta inte är möjligt bör avtal finnas om deponering av källkod.

11 Leverantörsrelationer

Krav och mål

11.1 Risker på grund av leverantörsberoende ska minimeras. Bedömning och lämpliga åtgärder bör ingå i en riskanalys.

11.2 Säkerhetskrav ska avtalas med leverantörer för att reducera risker kopplade till leverantörers åtkomst till Tillväxtverkets tillgångar. Ändringar i avtal och leverans ska styras och dokumenteras.
11.3 Tillväxtverket ska regelbundet övervaka och granska leverantörernas tjänsteleverans.

12 Hantering av incidenter

Interna regler

17 §	Anställda och leverantörer som använder Tillväxtverkets system ska rapportera uppkomna incidenter och hot enligt rutin för incidentrapportering. Rutinen omfattar både informationssäkerhets- och personuppgiftsincidenter

Krav och mål

12.1 Det ska finnas rutiner för rapportering av incidenter och svagheter hos informationssystemen samt rutiner för korrigerande åtgärder. Det ska finnas rutiner för insamling av information som kan tjäna som bevis.
12.2 Hanteringen av incidenter ska vara proaktiv. Kunskap baserade på hanterade incidenter ska användas för att minska risk och effekter av framtida incidenter.

13 Kontinuitetsplanering

Krav och mål

13.1 Planering ska göras för att minimera sannolikheten för skador i it-miljön och minimera konsekvenserna för verksamheten. I planeringen bör riskanalyser göras för att identifiera hot.
13.2 Det ska finnas planer och rutiner för att kunna återskapa tillgängligheten till informationstillgångarna inom den tid verksamheten kräver. Planerna bör regelbundet testas.
13.3 Verksamheten bör upprätthålla egna planer och manuella rutiner för att så långt möjligt klara avbrott i system och infrastruktur.

14 Efterlevnad

Krav och mål

14.1 Den informationssäkerhetsansvarige har ett övergripande ansvar för uppföljningen av informationssäkerhetsarbetet.
14.2 Informationssystem ska granskas regelbundet avseende efterlevnad av organisationens informationssäkerhetspolicy och regler.
14.3 Ägaren av en informationsresurs, som system eller informationsmängd, är ansvarig för uppföljning och efterlevnad av informationssäkerhetskraven för sin specifika informationsresurs.
14.4 Ledningen ska regelbundet granska efterlevnaden av informationssäkerhetspolicy och gällande regler.

Referenser

Tillväxtverkets styrdokument och vägledningar (urval)

- Informationssäkerhetspolicy
- It-strategi
- Vägledning för systemförvaltning

Lagar och förordningar (urval)

- Tryckfrihetsförordningen (1949:105)
- Offentlighets- och sekretesslagen (2009:400)
- Förvaltningslagen (2017:900)
- Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (GDPR).
- Förordningen (1995:1300) om statliga myndigheters riskhantering
- Säkerhetsskyddslagen (1996:627)
- Säkerhetsskyddsförordningen (1996:633)
- Arkivlagen (1990:782)
- Arkivförordningen (1991:446)

Föreskrifter och allmänna råd (urval)

- Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2016:1) om statliga myndigheters informationssäkerhet
- Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2016:2) om statliga myndigheters rapportering av it-incidenter
- Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2016:7) om statliga myndigheters risk- och sårbarhetsanalyser.
- Riksarkivets föreskrifter och allmänna råd (RA-FS 2009:1) om elektroniska handlingar (upptagningar för automatiserad behandling)
- Riksarkivets föreskrifter och allmänna råd (RA-FS 2009:2) om tekniska krav för elektroniska handlingar (upptagningar för automatiserad behandling)
- Riksarkivets föreskrifter och allmänna råd (RA-FS 1991:1) om arkiv hos statliga myndigheter

Standarder, utredningar och vägledningar (urval)

- ISO/IEC 27001:2014 och ISO/IEC 27002:2014 om informationssäkerhet, SIS
- Nationell strategi för samhällets informations- och cybersäkerhet, Regeringen 2017
- Webbplatsen *informationssakerhet.se*, MSB
- Rapport med förslag till fortsatt arbete 2017-2018, eSams expertgrupp för säkerhet. (Här ingår en översikt över intressanta rapporter och utredningar.)
- Vägledning för fysisk informationssäkerhet i it-utrymmen (Publ.nr. MSB629)

Begrepp

Begrepp	Förklaring
Allmän handling	Handling som har inkommit till eller upprättats av en myndighet och som förvaras där. En allmän handling kan i sin tur vara offentlig eller sekretessbelagd.
Arbetsmaterial	Utkast, tidiga versioner och annat underlag vid exempelvis förberederande av beslut kan i regel betraktas som arbetsmaterial och inte allmän handling. (Om det arkiveras, på annat sätt färdigställs eller skickas till annan myndighet blir det ändå normalt en allmän handling.)
Behandling av personuppgifter	Åtgärd som någon vidtar med personuppgifter, vare sig det görs på automatiserad väg eller inte.
Behörighet	Tilldelad åtkomsträttighet i IT-system.
Dataskydds-förordningen	Reglerar personuppgiftsbehandling inom EU. Också benämnd GDPR. Ersatte den 25 maj 2018 PUL.
Förvaltningsplan	Styrdokument för förvaltningsorganisationens arbete.
Gallring	Att fullständigt ta bort och förstöra information. För att få förstöra en allmän handling krävs gallringsbeslut och stöd i lag och föreskrift. Gallring är ofta nödvändig för upprätthålla god informationskvalitet. (Se även *Rensning*.)
Handling	Framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. En handling kan vara *allmän*. En allmän handling är *offentlig* om den inte är *sekretessbelagd*.
Information	Generell beteckning för det meningsfulla innehåll som överförs vid kommunikation i olika former.
Informationsklassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss informationsmängd.
Informationsmängd	Information som är avgränsad för ett visst ändamål.
Informationssäkerhet	Bevarande av *konfidentialitet, riktighet* och *tillgänglighet* hos information.
Incident	Händelse som kan innebära allvarliga konsekvenser för verksamheten.
Informations-säkerhetspolicy	Övergripande avsikt och viljeinriktning formellt uttryckt av en organisations ledning. Anger mål och inriktning för samt styr informationssäkerhetsarbetet inom organisationen.
Informationstillgång	All information, oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.
Informationsägare	Ansvarig för en informationstillgång oavsett i vilket system informationen behandlas. Sammanfaller ibland med systemägare. Ofta en chef för ett verksamhetsområde.
It-system	Teknik där man använder datorer och telekommunikation för att samla in, bearbeta och överföra information.
Konfidentialitet	Att information inte görs tillgänglig eller avslöjas för obehöriga personer, enheter eller processer.
Kontinuitetsplan	Dokumenterad plan som beskriver hur verksamheten ska bedrivas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas under en längre, specificerad tidsperiod

Begrepp	Förklaring
Kryptering	Omvandling av klartext till kryptotext i syfte att förhindra obehörig åtkomst av konfidentiell information
Känslig information (begreppet används i vid bemärkelse)	Information som, utöver sekretessreglerade uppgifter och vissa personuppgifter, av andra skäl behöver hanteras med försiktighet och där man bör undvika spridning, exempelvis arbetsmaterial i pågående ärenden
Känsliga person-uppgifter / Särskilda kategorier	Enligt dataskyddsförordningen uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.
Ledningssystem för informationssäkerhet	Ett systematiskt sätt för ledingen att styra, genomföra, följa upp och förbättra arbetet med informationssäkerhet.
MDM-lösning	Mobile device management. System för att administrera mobila enheter.
Offentlig handling	En allmän handling som inte är sekretessbelagd.
OSL	Offentlighets- och sekretesslagen (2009:400)
Personuppgifter	Information som direkt eller indirekt kan knytas till en fysisk person som är i livet. Även bild- och ljuduppgifter, krypterade uppgifter och olika elektroniska identiteter är personuppgifter om de kan kopplas till fysiska personer.
Rensning	Vid rensning tas överflödig information bort, exempelvis arbetsmaterial. Man kan rensa arbetsmaterial men inte allmänna handlingar. (Se även *Gallring*.)
Risk	Produkten av sannolikheten och konsekvensen för att ett givet hot realiseras.
Riskanalys	Metodisk process som identifierar säkerhetsrisker, bestämmer deras betydelse och identifierar skyddsåtgärder.
RSA-dosa	Säkerhetslösning för säker inloggning.
SAMFI-myndigheter	Samverkansgruppen för informationssäkerhet, där FMV, FRA, Försvarsmakten, MSB, Polisen, PTS och Säpo, ingår.
Samtycke	Otvetydig viljeyttring genom vilken den registrerade godtar att personuppgifter som rör honom eller henne behandlas.
Sekretess	Sekretess innebär förbud att röja en uppgift. OSL reglerar vilka handlingar som kan skyddas av sekretess. Finns inte stöd i OSL för sekretess är en handling som regel offentlig
Systemägare	Ansvarar för ett systems omfattning, ekonomi, större förändringar (efter samråd med Tekniskt ansvarig) samt om förvaltningsorganisationen. Ansvar och befogenheter följer i regel ett chefsansvar. Systemägaren kan även vara informationsägare, men rollerna sammanfaller inte alltid.
Tekniskt ansvarig	Tekniskt ansvarig är som regel it-chefen med övergripande ansvar för resurser för drift, systemutveckling och support.
Utvecklingsråd	Rådgivande grupp för Tillväxtverkets inriktning på it-verksamhet och it-miljö.
Ärende	Avgränsad fråga som tas upp till formell behandling. I myndigheter registreras vanligen ärenden i diarium med unika diarienummer. I ärenden ingår oftast handlingar.