Terminologi – Informationssäkerhet

Termer och definitioner i detta dokument är gällande inom ramen för universitetets informationssäkerhetsarbete, styrande dokument (ledningssystem) samt annan dokumentation och kommunikation.

Ägare och ansvarig för innehåll och förvaltning: ingegerd.wirehed@rektor.lu.se, CISO

Nya termer och ev. förändringsförslag sänds till informationssakerhet@lu.se

Term	Definition
administratör (IT-system)	Användare som har högre eller andra rättigheter än en vanlig användare, t.ex. systemadministratör, säkerhetsadministratör
analysobjekt	En informationstillgång som ska analyseras
användare (IT, information)	Person som utnyttjar information eller en tjänst
användarnamn	Namn som en användare anger för att identifiera sig (logga in) och få tillgång till ett datornät, datorprogram eller en webbsida
assurans	Tilltro till att ett systems eller en produkts säkerhetsfunktioner uppfyller specificerade säkerhetskrav
auktorisation	Fastställande av åtkomsträttigheter för en användare till olika systemresurser
autenticitet	Äkthet
autentisering	Kontroll av användares eller systems identitet för att säkerställa att denne verkligen är den han eller hon utger sig för att vara
back-up	Se säkerhetskopia
behandling (av information)	En åtgärd eller kombination av åtgärder beträffande information oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring. Notera att dataskyddslagstiftningen är tillämplig på all *helt eller delvis automatiserad* behandling av personuppgifter samt på *manuell behandling av personuppgifter som ingår i eller är avsedda att ingå i ett register.*
behörighet	Den hierarki av rättigheter i ett datorsystem som är knutna till arbetsuppgifter, befattningar och roller. Behörighet är knuten till identitet, så behörighetskontroll sker efter att användarens identitet har kontrollerats (autentiserats).
botnet	Logiskt nät av datorer som smittats av sabotageprogram som gör det möjligt för utomstående att fjärrstyra dem i syfte att sabotera eller utnyttja dem för egen vinning
brandvägg	Nätverkskomponent som enligt given konfiguration begränsar och övervakar trafik mellan nätverk
certifikat	Ett digitalt certifikat är en fil som verifiera certifikatinnehavarens identitet.
certifikatutfärdare	Av flera användare betrodd instans som har till uppgift att skapa och utge användarcertifikat eller andra typer av certifikat
CISO	Chief Information Security Officer. CISO har det övergripande ansvaret att leda och samordna arbetet med informationssäkerhet i en organisation. Huvudansvaret för informationssäkerheten följer verksamhetsansvaret, och ligger därmed på ledningen. Ref MSBs rollbeskrivning.
cybersäkerhet	En delmängd av informationssäkerhet där cybersäkerhet bara handlar om digital information. Cybersäkerhetsbegreppet är mer strategiskt och fokuserar mer på nationella och internationella nätverk samt hot från externa antagonister. Noteras bör att när man talar om digital information blir det en mix av information och bärare – när man exempelvis klassar information är det inte mediet som klassas utan informationsinnehållet.

cyberrymden	Den del av informationsmiljön som består av de sammanlänkade och av varandra beroende IT-infrastrukturer, som möjliggör kommunikation av data och information. Den inkluderar internet, intranät, telekommunikationssystem, IT-system samt inbyggda processorer och styrenheter. Cyberrymden ses som den gemensamma tekniska infrastrukturen men inte informationen i sig.
Dataskyddsförordningen	Alla verksamheter som hanterar personuppgifter måste följa dataskyddsförordningen. Det innebär bland annat att verksamheten behöver följa de grundläggande principerna, se till att behandlingen har en rättslig grund och informera de registrerade om hur deras personuppgifter hanteras. (Engelskan General Data Protection Regulation GDPR)
Dataskyddsombud	Utses av den som behandlar personuppgifter. Kontrollerar att dataskyddsförordningen (GDPR) följs inom organisationen t.ex. genom att samla in information om hur organisationen behandlar personuppgifter, kontrollera att organisationen följer bestämmelser och interna styrdokument, informera och ge råd om organisationen. Ska också ge råd om konsekvensbedömningar, vara kontaktperson för IMY, de registrerade och personalen inom organisationen.
dekryptering	Omvandling av en kryptotext, en oläslig text, till en läslig klartext med hjälp av ett kryptosystem och en krypteringsnyckel.
DoS attack, DDoS attack	Denial of Service attack (överbelastningsattack, tillgänglighetsattack) är en typ av sabotage där någon överbelastar en server eller router genom att sända enorma mängder felaktiga datapaket så att den till slut kraschar. Distributed Denial of Service Attack är en distribuerad överbelastningsattack där anropen sker från många olika datorer, ofta fjärrstyrda via maskar, virus eller trojaner som infekterat dessa datorer utan ägarnas vetskap.
e-legitimation	Elektronisk legitimationshandling som används för säker identifiering på Internet, t.ex. e-legitimation, elektronisk legitimation, e-leg, eID, BankId.
elektronisk signering, digital signering	En signatur är resultatet av en matematisk beräkning som validerar äktheten och integriteten hos ett meddelande eller ett program och som läggs till meddelandet eller programmet.
federerad identitet	En användaridentitet som kan användas inom olika organisationer, eftersom man har enats om hur man ska hantera identiteter över organisationsgränserna. En användare som autentiserat sig hos en organisation kan med automatik bli autentiserad hos en annan organisation som ingår i federationen. Resultatet kan bli en samlad inloggning (engelsk term: singel sign-on) som överskrider organisationsgränserna.
förvaltningsobjekt (se även analysobjekt)	Ett eller flera IT-system som förvaltas gemensamt, omfattande såväl applikation som it-teknik. När det gäller förvaltning av IT-infrastruktur består förvaltningsobjektet oftast enbart av it-teknik. Förvaltningsobjekt, IT-system och system har samma betydelse i detta sammanhang. Ett annat förvaltningsobjekt kan vara en fastighet eller en process.
förvaltningsorganisation	En grupp människor som under organiserade former sköter förvaltningen av ett specifikt förvaltningsobjekt
förvaltningsplan	Årligt styrdokument för förvaltningen av ett specifikt förvaltningsobjekt
gapanalys	Identifiering av skillnaden mellan befintliga, införda säkerhetsåtgärder och identifierat behov av säkerhetsåtgärder dvs. skyddsnivån
grundskydd	En grundnivå med olika säkerhetsåtgärder som verksamheten beslutat att införa. Grundskyddet kan t.ex. bestå av krav på utbildning innan viss information får hanteras, bakgrundskontroll före anställning eller att ett IT-system måste ha infört vissa tekniska säkerhetsåtgärder om inte informationsklassningen och riskbedömningen kommer fram till att en lägre nivå är tillräcklig
hoax	En lögn, en falsk varning eller uppmaning som ser ut att vara sann.

hot	Något som orsakar eller bidrar till att orsaka att en incident inträffar. Oavsiktligt hot: existerar trots att illasinnad avsikt saknas. Avsiktligt hot: syftar till att skada verksamheten Inre hot: orsakas av individer inom organisationen Yttre hot: har sitt ursprung utanför organisationen
hotbild	Hot som bedöms förekomma mot en viss verksamhet dess tillgångar och resurser
identifiering	Att knyta en person med uppgiven identitetsbeteckning (namn, personnummer eller liknande) till en på förhand registrerad identitet. I de flesta fall förutsätts någon form av identitetskontroll (autentisering).
identitet	Unik beteckning för en viss entitet (person, process, fysisk enhet eller liknande) i ett visst system
information	Kunskap gällande objekt, såsom fakta, händelser, saker, processer eller idéer, inklusive begrepp, som i ett givet sammanhang har en bestämd mening
informationsbärare (se även objekt)	Bär, lagrar eller kommunicerar information. Kan exempelvis vara papper, IT-resurser, människor, system, lagringsmedia, telefoni
Informationsmängd	En gruppering av information som innehåller flera informationstyper t.ex. i form av ett dokument eller en databas.
informationsriskägare	Ansvarar för informationstillgångar och beslutar om informationshantering inom ramen för befintlig lagstiftning och interna regelverk. Informationsriskägare är ansvariga för att den egna informationen klassas och har ett tillräckligt skydd genom riskbedömning och ställa krav på hanteringen av informationen. Ägaren har även mandat att fatta beslut om riskacceptans.
Informationsklassning	Syftar till att analysera informationstillgångar utifrån identifierade interna och externa krav för att förstå vilka konsekvenser som uppstår om konfidentialitet, riktighet eller tillgänglighet inte kan uppnås för informationen.
informationsmodell	grafisk beskrivning av de informationsobjekt en viss verksamhet behöver och hur de relaterar till varandra
informationssystem	Applikationer, tjänster eller andra komponenter som hanterar digital information. I begreppet ingår också nätverk och infrastruktur. Ref MSBs definition i MSBFS2020:7
informationssäkerhet	Bevarande av konfidentialitet, riktighet och tillgänglighet (och spårbarhet) hos information. Informationssäkerhet är en kombination av administrativ och teknisk säkerhet, där fysisk säkerhet och IT-säkerhet ingår i den tekniska säkerheten
informationssäkerhets-incident	En enskild eller en serie oönskade eller oväntade informationssäkerhetshändelser vilka med stor sannolikhet kan äventyra informationssäkerheten
informations-klassning	Att genom konsekvensanalys värdera sin information utifrån aspekterna konfidentialitet, riktighet och tillgänglighet (samt spårbarhet). Denna klassning ska ske av alt. godkännas av beslutade informationrisksägare.
informationssäkerhetskrav	De VAD-krav som respektive ägare och förvaltare av informationsbärare ska ta ställning till huruvida man uppfyller för t ex ett enskilt objekt . Status för kravuppfyllnad/regelefterlevnad ligger till grund för handlingsplan om vad som bör åtgärdas.
informationstillgångar	All skyddsvärd information som verksamheten hanterar inklusive de resurser som behandlar informationen genom att ta emot, lagra, bearbeta, visa eller kommunicera den.
informationstyp	Ett visst slag av information t.ex. personuppgifter, forskningsdata, ritningar, källkod etc.
Integritet	Okränkbarhet med förmåga att upprätthålla sitt värde genom skydd mot oönskad förändring, påverkan eller insyn. Kan avse såväl ett tekniskt system (systemintegritet) som en person (personlig integritet)
interoperabilitet	Förmåga och möjlighet hos system, organisationer eller verksamhetsprocesser att fungera tillsammans och kunna kommunicera med varandra genom att överenskomna regler följs
intrång	Att utan tillstånd skaffa sig tillgång till information i datorer eller att utan tillstånd ändra, ta bort eller lägga till information
IT-system/ informationssystem	Ett system för insamling, lagring, bearbetning och spridning av information för ett visst ändamål. Ärver klassning från informationsinnehållet. Systemperspektivet hjälper till att hitta ägarskap. Fokus är dock på informationen som hanteras i systemet. Uppsättning av applikationer, tjänster, informationsteknologiska tillgångar och andra informationshanteringskomponenter

IT-systemförvaltare/ IT-systemägare	Verksamhetsspecialist, ansvarar på daglig basis för funktionaliteten och säkerhetsnivå i systemet.
IT-systemförvaltning	De aktiviteter som görs för att hantera ett system i drift, så att det effektivt bidrar till att uppfylla verksamhetens mål. En systemförvaltningsmodell är ett ramverk som beskriver hur ett förvaltningsarbete kan utföras och organiseras. Modellen ger en normgivande bild av de aktiviteter som utförs för att styra, administrera, utföra förändringsarbeten och stödja användandet av ett förvaltningsobjekt.
IT-säkerhet	IT-relaterade tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet dvs. med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid såväl kommunikation som lagring och bearbetning av data.
konfidentialitet	Egenskapen att information inte tillgängliggörs eller avslöjas till obehöriga individer, enheter eller processer. Not: Konfidentialitet medför inte automatiskt sekretess, även om det kan finnas en koppling. Därför ska begreppen konfidentialitet och sekretess hållas åtskilda. Sekretess är enbart en benämning på den del av informationen som sorterar under OSL
konsekvens	Resultat av en händelse med negativ inverkan
konsekvensnivå	Avser nivån som gäller utifrån de tre olika perspektiven (konfidentialitet, riktighet och tillgänglighet). Normalt utgår man från en modell med t ex fyra nivåer, där 0 är lägst och 3 är högst. 3 används bara i speciella omständigheter. 0 representerar få eller inga större negativa konsekvenser på verksamhet eller omvärld.
kontinuitetshantering	Förmågan och beredskapen att hantera avbrott i verksamheten, att minska skador pga. avbrott samt att sörja för att kontinuitet i verksamhetens kritiska processer ligger på en accepterad lägsta nivå.
krypteringsalgoritm	En matematisk procedur som används vid kryptering och dekryptering av meddelande. Bygger på att bokstäver i ett meddelande behandlas som tal och byts ut och flyttas om enligt ett matematiskt mönster.
kryptering	Omvandling av klartext till en, för obehöriga, oläslig kryptotext med hjälp av ett kryptosystem och en krypteringsnyckel.
kryptosystem	Utrustning eller ett program som innehåller av en krypteringsalgoritm som används för kryptering och dekryptering av meddelande, funktionalitet för att autentisera avsändaren av ett meddelande samt funktionalitet för att generera och hantera krypteringsnycklar.
kryptotext	Text som krypterats. Motsats är klartext.
ledningssystem för Informationssäkerhet (LIS)	System (ej IT-systems) för att fastställa en organisationsprocess för styrning och ledning av informationssäkerhetsarbetet. Det omfattar bl.a. grundprinciper för ledning av arbetet, kunna ställa upp mål samt för att uppnå dessa mål, organisation, resurser samt tekniska respektive administrativa säkerhetsåtgärder. LISet är ett stöd för hur informationssäkerhetsarbetet styrs av ledningen i verksamheter. En central del i ett ledningssystem är ledningens uttalade stöd. Översta nivån är den policy som styrelsen antar för informationssäkerhetsarbetet. I styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledning till chefer och övriga medarbetare. Ref: Standard SS-ISO/IEC 27001:2017 som fastställer krav som en organisation behöver uppfylla när det gäller ledningssystem för informationssäkerhet.
Logg	Förteckning över händelser, samt olika attribut kopplade till dessa, noterade i den ordning de inträffar.
logiskt gränssnitt	Del av en tjänstebeskrivning som beskriver gränsytor som ska implementeras av producent och konsument i form av anrop, meddelanden och sekvenser. Jämför Tekniskt gränssnitt.
metadata	Beskriver innehåll och/eller strukturen för en viss datasamling ur något perspektiv
lösenord	Kombination av tecken som tillsammans med användarnamn anges för att verifiera användaridentitet
mask	Program som mångfaldigar sig själv i ett distribuerat system och fyller alla minnesutrymmen i drabbade datorer med kopior av sig själv tills både datorer och nätverk blir överbelastade och slutar att fungera. En mask förstör ingenting.
molntjänst	Tjänst som tillhandahålls via internet från ett nätverk av servrar. Kräver inget speciellt operativsystem eller program utom en webbläsare, inte gjord för någon speciell kund, antal användare kan enkelt ökas eller minskas och kundens information lagras på tjänsteleverantörens server.
obehörig åtkomst	Åtkomst av system, resurs eller annat objekt i strid med behörighetsregler

oförnekbarhet	Hinder för avsändaren av ett elektroniskt meddelande att förneka att han/hon är avsändaren och för mottagaren att förneka att han/hon har tagit emot samma meddelande. (engelsk term; non-repudiation)
omvärldsanalys	Omvärldsanalysen är en del av riskprocessen där syftet är att identifiera allt som ligger utanför verksamhetens direkta kontroll men som påverkar eller påverkas av organisationens informationssäkerhet. Resultatet användas för att utforma informationssäkerheten så att verksamheten lever upp till de rättsliga krav som gäller genom att koppla vissa säkerhetsåtgärder till en viss typ av information och använda den i samband med informationsklassning.
outsourcing	Utkontraktering av någon del av intern verksamhet, process eller IT-relaterad tjänst som tidigare utfördes internt, till en extern leverantör
personuppgifter	All slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet. 1) Ordinära personuppgifter Exempel på ordinära personuppgifter är namn, adress, telefonnummer, e-postadress. Det är personuppgifter som inte ingår i kategori 2 eller 3. 2) Känsliga personuppgifter Vad som utgör känsliga personuppgifter är reglerat i lag. Det är uppgifter om etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som används för att entydigt identifiera en person. 3) Extra skyddsvärda personuppgifter Exempel på extra skyddsvärda personuppgifter är personnummer och värderande uppgifter om en person, t ex uppgifter från utvecklingssamtal eller uppgifter om resultat från personlighetstester. Det är personuppgifter som bedömts mer skyddsvärda än ordinära personuppgifter men som inte ingår i kategori 2.
personuppgiftsansvarig	Organisation, stiftelse, förening eller myndighet som bestämmer för vilka ändamål personuppgifter ska behandlas och hur behandlingen ska gå till. Den personuppgiftsansvarige måste se till att behandlingen av personuppgifter sker i enlighet med dataskyddsförordningen.
personuppgiftsbiträde	Den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvariga.
personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats
phishing, nätfiske	Attack som via epost söker locka mottagaren att besöka en till synes äkta webbsida (för t.ex. en bank eller kreditkortsföretag) och där uppge inloggningsinformation eller andra känsliga uppgifter
PIN-kod	Förkortning av engelskans Personal Identification Number, som är ett numeriskt lösenord.
policy	Övergripande avsikt och viljeinriktning formellt uttryckt av ledningen
process	Ett eller flera arbetssteg, som logiskt hänger samman och som medverkar till att ett resultat kan levereras
ransomware, kryptovirus	Skadlig kod som krypterar hela eller delar av innehållet i systemet. Det kan vara kryptering av viss typ av filer (crypto ransomware) eller att alla filer krypteras och att datorn inte kan startas upp (locker ransomware). Angriparen begär en lösensumma för att lämna ut det lösenord som låser upp krypteringen.
riktighet	Egenskapen att skydda exaktheten och fullständigheten gällande tillgångar
risk	En systematisk sammanvägning av förväntad sannolikhet för och konsekvens av att en oönskad händelse inträffar till följd av ett visst hot, kopplat till en definierad verksamhet, en specifik skyddsvärd tillgång och en specifik konsekvensskala. Organisationen identifierar vilka risker som finns (ibland används termen bruttorisk) och bedömer effekten av att risken inträffar (sannolikhet * konsekvens). Därefter Identifiera och utvärdera existerande kontroller/åtgärder för att bedöma kvarvarande risk (ibland används termen nettorisk). En handlingsplan upprättas för att begränsa de nettorisker som man bedömer ligger för högt, trots implementerade kontroller/åtgärder. Efter att brutto- och nettorisker har identifierats behöver verksamheten fatta beslut om vilka aktuella risknivåer som kan accepteras eller om motverkande kontroller behöver stärkas. (Detta moment ingår och beskrivs i sin helhet i metodiken för riskhantering avseende informationssäkerhet).

riskmatris	Riskmatrisken är ett visuellt hjälpmedel som hjälper till i riskhanteringen. För varje hot bedöms konsekvensen i händelse av att hotet inträffar utifrån en fastställd konsekvensskala (y-axel) och sannolikheten att hotet inträffar bedöms på motsvarande sätt med hjälp av sannolikhetsskalan (x-axel). När konsekvensen och sannolikheten är bestämda, kan hotet plottas ut i riskmatrisen.
riskacceptans	Ett av flera sätt att hantera en risk. I detta fall innebär det att inget görs åt risken t.ex. för att påverkan är minimal, åtgärderna för kostsamma eller för att risken inte går att åtgärda för att den helt beror på externa händelser. Kallas även för att behålla risken. Mandat att fatta beslut har informationsriskägaren.
riskanalys	Process som identifierar hot mot verksamheten och uppskattar storleken hos relaterade risker
riskbedömning	Övergripande process för riskidentifiering, riskanalys och riskutvärdering.
riskbegränsning	Ett av flera sätt att hantera en risk. Begränsningen uppnås genom att t.ex. skadeförebyggande eller skadebegränsande åtgärder sätts in.
riskdelning/risköverföring	Ett av flera sätt att hantera en risk. Betyder att risken överförs till en eller flera andra intressenter som är mer kapabla eller villiga att ta sig an risken alternativt så kan en försäkring tecknas (försäkringen tar då hand om konsekvensen). OBS! Ansvaret för en risk kan aldrig överföras till någon annan.
riskeliminering	Ett av flera sätt att hantera en risk. I detta fall innebär det att risken helt tas bort, d.v.s. att de elimineras.
riskhantering	Samordnade aktiviteter för att bedöma (identifiera, analysera och utvärdera) och behandla risker. Vid behandling av risker skapas förebyggande åtgärder för att reducera risken. Två huvudmetoder används. A) Riskreducering genom att skapa en förebyggande åtgärd. Här kan kostnad beräknas, typ anges, ansvarig för åtgärden, koppling till andra risker som denna åtgärd reducerar, tidsram. B) Riskreducering genom att koppla till en säkerhetsåtgärd. Åtgärden väljs ur en för organisationen beslutad mängd säkerhetsåtgärder. När risken har hanterats finns möjlighet att göra en ny riskbedömning efter att planerade åtgärder är införda. Detta kallas ibland nettorisk och den ursprungliga bedömningen bruttorisk.
riskidentifiering	Process för att upptäcka, kartlägga/känna igen och beskriva risker
riskutvärdering	Process för att jämföra resultaten från riskanalysen med riskkriterierna för att avgöra om risken och/eller dess storlek är acceptabel eller godtagbar
riskägare	Person som ansvarar för och har befogenhet att hantera en risk
samlad inloggning	En metod för att hantera användare med aspekt på autentisering och auktorisering, så att dessa användare endast behöver logga in en enda gång på flera lösenordskyddade program eller webbsidor under en arbetsdag för att nå de system som är anpassade till tjänsten. (Engelska: single sign-on (SSO)
sekretessbelagd uppgift	Ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. En sekretessreglerad uppgift för vilken sekretess gäller i ett enskilt fall, enligt OSL, Offentlighets- och Sekretesslagen
skyddsnivå	Ett antal säkerhetsåtgärder, som ger ett tillräckligt skydd för information som klassas till en viss konsekvensnivå, samlade i en skyddsnivå.
spökprogram	Ett spökprogram ger angripare möjlighet att ta över en dator eller nätverk genom att installeras på ett sätt som inte går att upptäcka för datorns ägare och sedan samla in användarnamn och lösenord. De insamlade uppgifterna skickas sedan till angriparen via datorns Internetanslutning. När programmet har hittat inloggningsuppgifter till en systemadministratör kan angriparen ta över nätverket (engelskans: Rootkit)
systemrättighet	Användares rätt att utföra olika handlingar på en dator eller i ett nätverk. Rättigheterna gäller sådant som att köra, installera och radera program, hämta, läsa, ändra och lägga till information, ändra inställningar, komma åt, använda och sprida information över nätverket och över internet.
sabotageprogram	En överordnad term för oönskade datorprogram, framför allt virus, maskar, trojaner, spökprogram, tangentloggare (engelskans key-logger) och hybrider.
sekretess, sekretessbelagd uppgift	Ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. En sekretessreglerad uppgift för vilken sekretess gäller i ett enskilt fall, enligt Offentlighets- och Sekretesslagen (OSL).
skadeprogram	Program som är till för att ändra eller radera data, stjäla information, öppna en bakdörr, göra så att ett IT-system fungerar dåligt eller slutar fungera eller att infekterade dator kan fjärrstyras att delta i angrepp på andra datorer och IT-

	system.
skydd	Effekt av handlingar, rutiner och tekniska arrangemang som syftar till att minska sårbarheten. Motsats till sårbarhet.
skyddsvärde	En verksamhets olika värden (tillgångar) mot vilka det kan riktas risker. Det kan vara information, material, renommé, byggnader, beställningar, nyckelpersoner, beroenden, instrument osv.
sniffer	Anordning eller program som samlar in data som skickas över ett nätverk.
social engineering	Manipulering genom använda olika sociala knep för att skapa förtroende och senare tillgång till känslig eller hemlig information
spam	Massutskick av oönskad, icke beställd e-post eller textmeddelanden (SMS), ofta med kommersiellt budskap och utan mottagarens samtycke. Skräppost.
spionprogram	Spionprogram som körs på en dator utan användarens godkännande, och samlar och vidarebefordrar information (användaruppgifter, lösenord, besökta websidor etc) till annan part. (engelskans spyware)
spårbarhet	Möjlighet att entydigt kunna härleda utförda aktiviteter i systemet till en identifierad användare vid en viss tidpunkt.
systemägare	Som systemägare utses normalt den person som är verksamhetsansvarig (dekan, prefekt/motsv.) för att automatiskt få en koppling mellan verksamhetens nytta och krav på systemet. Systemägaren har det övergripande ansvaret för visioner och ramar och ska ansvara för att systemet stöttar verksamheten och dess processer på ett ändamålsenligt sätt. Systemägaren ska säkerställa de resursmässiga förutsättningarna och fatta beslut inom systemets budget. Vidare ska systemägaren ansvara för att initiera utvecklingsprojekt. Systemägaren ansvarar för att informationssystemet lever upp till ställda informationssäkerhetskrav. Dessa krav ställs genom utsedd/a informationrisksägares klassning av den information som systemet används för.
systemförvaltare	Systemförvaltaren arbetar på uppdrag av systemägaren med förvaltning av systemet. Systemförvaltaren arbetar utifrån de mål och aktiviteter som definierats i beslutade planer och inom de ramar som tilldelats för perioden. Systemförvaltaren ska genomföra aktiviteter för att samla in krav och behov från verksamheten och rapportera dessa till systemägaren. Systemförvaltaren leder arbetet i förvaltningsgrupp och referensgrupper.
sårbarhet	Svaghet eller avsaknad av något som skulle kunna förhindra att en incident inträffar, och oönskad konsekvens av en incident. Dessa gäller en tillgång eller grupp av tillgångar, vilken kan utnyttjas av ett eller flera hot.
säkerhet (eng)	Security - egenskap eller tillstånd som innebär skydd mot risk för oönskad insyn, förlust eller påverkan. Oftast i samband med medvetna försök att utnyttja eventuella svagheter/sårbarheter Safety - egenskap eller tillstånd som innebär skydd mot skada för liv och lem (personsäkerhet)
säkerhetskopia	Kopia av en informationsmängd som skapats för att kunna utnyttjas vid förlust av hela eller delar av den ursprungliga informationsmängden. Se back-up
säkerhetsskydd (Ref: Säkerhetsskyddslagen)	Med säkerhetsskydd avses 1. skydd mot spioneri, sabotage och andra brott som kan hota rikets säkerhet, 2. skydd i andra fall av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet, och 3. skydd mot terroristbrott enligt 2 § lagen om straff för terroristbrott (terrorism), även om brotten inte hotar rikets säkerhet.
tangentloggare	Program eller hårdvara som i smyg registrerar alla knapptryckningar på en dator. Används för att samla in användaruppgifter och lösenord och vilka websidor som har besökts. Kan vara ett program eller en liten skarvkoppling som kopplas mellan datorn och tangentbordet. (englskans keylogger)
tekniskt gränssnitt	Del av en tjänstebeskrivning som beskriver teknikval för olika implementationer i form av exempelvis protokoll och standarder
tillgänglighet	Egenskapen att vara åtkomlig och användbar vid begäran av en behörig enhet, t.ex. användare
tillgänglighetsförlust	Övergång till ett tillstånd hos ett system där det inte i erforderlig utsträckning eller inom önskad tid kan leverera önskade tjänster

tjänst	Paketerad service eller lösning som erbjuds för att tillgodose ett behov
tjänstemeddelande	Den information som förmedlas mellan deltagare i en tjänsteinteraktion
tjänstekatalog	En logisk plats för att söka, hitta, ge åtkomst till, publicera, administrera och lagra beskrivningar av tjänster
trojan	Ett program som utger sig för att vara till nytta eller nöje, men är någon skadlig programkod
tvåfaktors/ flerfaktors-autentisering	Identitetskontroll genom två (eller flera) av faktorerna något man har, något man vet och något man är (t ex kort, lösenord, biometri). Var för sig är kort, kod eller biometri oanvändbar i inloggningssyfte men två tillsammans ger autentisering.
upphandlingskrav	Upphandlingskrav avseende informationssäkerhet utifrån de VAD-krav som fastställts baserat på informationsklassning och kravanalys.
uttalande om tillämplighet	En rapport som innehåller det samlade resultatet från omvärlds-, verksamhet-, risk- och gapanalysen och som visar nuvarande informationssäkerhetsstatus, de åtgärder som ska tillämpas, motivering för att de skall tillämpas, deras status, om de fungerar på ett tillfredställande sätt för att säkerställa en god informationssäkerhet. (engelskans Statement of Applicability (SoA))
verksamhetsanalys	Verksamhetsanalysen är en del av riskprocessen, där syftet är att identifiera väsentliga informationstillgångar, kartlägga interna intressenters behov, förväntningar och förutsättningar, vilket ska tas hänsyn till i samband med utformning och klassning av informationstillgångar.
virus	Illasinnad kod som sprider sig genom att lägga en kopia av sig själva utan en användares inblandning inuti andra program, värdprogram, på sådant sätt att koden körs då värdprogrammet körs
åtgärd/säkerhetsåtgärd	Handling, procedur eller tekniskt arrangemang som genom att minska sårbarheten möter identifierat hot. Exempel på typer av säkerhetsåtgärder: Organisatorisk: att man fördelar ansvar, roller och mandat i organisationen så att informationen skyddas mot felaktig hantering (vem gör vad för att undvika att saker hamnar mellan stolarna). Administrativ: att man skapar styrdokument, rutiner eller liknande samt genomför utbildningar som stöd för säker informationshantering. Fysisk: att ha lås, larm, dörrar, fönster och motsvarande som skyddar information och informationssystem mot obehörig fysisk åtkomst. Teknisk: att olika IT-lösningar används för att skydda informationen, till exempel antivirus, behörighetssystem, säkerhetsloggning och säkerhetskopiering.
överföring till tredje land (Ref IMY, GDPR)	Överföring av personuppgifter till tredje land är när personuppgifter blir tillgängliga för någon i ett land utanför EU/EES-området. Detta sker vid universitetet, t ex • När ni skickar dokument som innehåller personuppgifter per e-post till någon i ett land utanför EU/EES. • När ni anlitar ett personuppgiftbiträde i ett land utanför EU/EES. • När ni ger någon utanför EU/EES tillgång, exempelvis läsbehörighet, till personuppgifter som finns lagrade inom EU/EES. • När ni lagrar personuppgifter i en molntjänst som är baserad utanför EU/EES. • När ni lagrar personuppgifter, till exempel på en server, i ett land utanför EU/EES.