Riktlinjer för informationssäkerhet

Innehåll

1 Bakgrund

I detta dokument fastställs riktlinjer för informationssäkerhet vid Linköpings universitet (LiU). Riktlinjerna är en del av LiU:s ledningssystem för informationssäkerhet. Andra dokument som ingår i ledningssystemet listas i inledningen till kapitel 2.

Ordet riktlinje ska tolkas i en strikt bemärkelse. Riktlinjerna är obligatoriska och utgör huvuddelen av Linköpings universitets riskbehandlingsplan för informationssäkerhetsrisker. Varje riktlinje har dock en riskägare som kan besluta om alternativ riskbehandling; former för detta preciseras i avsnitt 2.3 och i Rutiner för alternativ riskbehandling (LiU-2023-00881).

Riktlinjerna publiceras även i en version där kommentarer infogats med referenser till motivering av respektive riktlinje (t.ex. författningskrav, ISO 27002 och riskanalyser). Den kommenterade versionen av riktlinjerna finns tillgänglig för nedladdning på https://go.liu.se/infosec.

Ordlista och definitioner av huvudsakligen tekniska termer återfinns i slutet av dokumentet.

Till skillnad från tidigare beslut omfattar riktlinjerna för informationssäkerhet inte längre massutskicka av e-post eller riktlinjer för kontoadministratörer. För aktuella riktlinjer härvid hänvisas till Riktlinjer för massutskick av e-post (LiU-2023-03471) samt Riktlinjer för tillgång till IT- och tekniska resurser vid LiU (LiU-2023-03285).

2 Översikt över informationssäkerhetsarbetet

2.1 Styrdokument om informationssäkerhet

Dessa riktlinjer utgör en del av LiU:s ledningssystem för informationssäkerhet (LIS). Utöver riktlinjerna finns inom ledningssystemet bland annat följande dokument som kan vara relevanta för läsaren:

LiU-2018-02237	Informationssäkerhetspolicy
LiU-2023-00877	LIS – Ramverk
LiU-2023-00878	LIS – Rutiner för att utse informationsägare samt inventering av vissa informationstillgångar
LiU-2023-00880	LIS – Rutiner för riskanalys
LiU-2023-00881	LIS – Rutiner för alternativ riskbehandling

2.2 Riskbaserat arbetssätt

LiU:s informationssäkerhetsarbete utgår från ett riskbaserat arbetssätt med stöd av standarderna SS-EN ISO/IEC 27001:2017 samt SS-EN ISO/IEC 27002:2017. Dessa riktlinjer utgör LiU:s generella riskbehandlingsplan för informationssäkerhetsrisker.

2.3 Roller i informationssäkerhetsarbetet

Varje individ som hanterar information vid LiU har en viktig roll i skyddet av informationen. Ansvar för informationssäkerhet utgår från delegationsordningen såväl som lokal arbetsordning. För att tydliggöra och konkretisera roller och beslutsmandat inom informationssäkerhet är det praktiskt (och nödvändigt) att definiera följande roller:

Informationsägare

Informationsägaren ansvarar för hur information som är i LiU:s vård skyddas mot obehörig åtkomst, obehörig förändring eller förlust. Informationsägaren klassar informationen och anvisar hur informationen ska hanteras för att säkerställa att dessa riktlinjer efterlevs.

Prefekt/motsvarande[1] kan utse informationsägare för information där ansvar återfinns inom dennes institution. Om prefekten inte beslutar om särskild ordning ska den informationsägare som anges för respektive handlingstyp i LiU:s dokumenthanteringsplan[2] tillämpas inom institutionen.

[1] Exempelvis prefekt, dekan, centrumchef eller avdelningschef vid universitetsförvaltningen
[2] https://go.liu.se/dokp

Systemägare

Systemägaren ansvarar för att system ger tillräckligt skydd för den information som hanteras. Systemägare ska gentemot informationsägare deklarera vilka informationsklasser som normalt kan hanteras i systemet. Vilka specifika säkerhetskrav som ska tillämpas styrs huvudsakligen av avsedd informationsklass. För system som inte är avsedda att behandla särskilt skyddsvärd information och som endast används inom forskning och undervisning vid en eller ett mindre antal institutioner gäller riktlinjerna enligt kapitel 6. För andra system gäller dessutom riktlinjerna enligt kapitel 7.

Riskägare

Varje riktlinje i detta dokument är knuten till en riskägare som i situationer där en riktlinje inte är ändamålsenlig kan besluta om annan hantering enligt Rutiner för alternativ riskbehandling (LiU-2023-00881).

Alternativ riskbehandling kan omfatta införandet av särskilda tekniska eller administrativa skyddsåtgärder som minskar sannolikheten eller konsekvensen av att en risk realiseras. Det kan också innebära att riskägaren väljer att acceptera en informationssäkerhetsrisk.

2.4 Informationsklassning

2.4.1 Informationsklassning i tre dimensioner

Syftet med informationsklassning är att underlätta val av relevanta tekniska och administrativa skyddsåtgärder för LiU:s information samt underlätta för medarbetare att bedöma hur olika typer av information får hanteras, t.ex. hur en viss IT-tjänst får användas eller i vilka system viss information får hanteras.

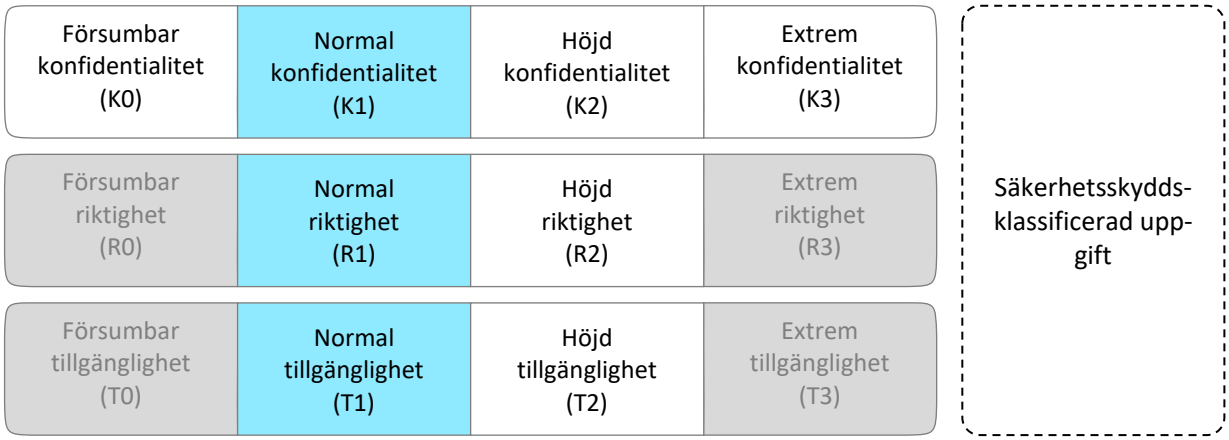
Information vid LiU klassas enligt tre dimensioner:

- **konfidentialitet**: konsekvenserna av obehörigt röjande
- **riktighet**: konsekvenserna av förvanskning
- **tillgänglighet**: konsekvenserna av förlust.

Varje dimension är indelad i nivåer: **försumbar**, **normal**, **höjd** och **extrem** för **konfidentialitet**; **normal** och **höjd** för **riktighet** och **tillgänglighet**. Nivåerna motsvarar den skada som kan uppstå för LiU, våra samarbetsparters eller enskilda individer om informationen röjs, förvanskas eller förloras.

Som framgått under föregående avsnitt är det informationsägaren som ansvarar för att klassa en uppgift. Klassningen påverkar hur informationen får hanteras och måste göras med omsorg för att informationen ska få tillräckligt skydd utan att de som hanterar den drabbas av onödig administrativ börda.

Vid andra lärosäten och myndigheter förekommer det att man använder nivåerna K0 till K4 för konfidentialitet, R0 till R4 för riktighet, och T0 till T4 för tillgänglighet. Ofta motsvaras nivå 0 i LiU:s modell av försumbar nivå, nivå 1 av normal nivå, nivå 2 av höjd nivå och nivå 3 av extrem nivå. Nivåerna K4, R4, och T4 motsvarar säkerhetsskyddsklassificerade uppgifter. En jämförelse med andra myndigheter ska dock göras med försiktighet eftersom inte alla myndigheter använder samma ställningstaganden för klassning.



Figur 1: LiU:s informationsklassningsmodellen med nivån "normal" framhävd. Observera att riktighet och tillgänglighet aldrig klassas på nivåerna försumbar eller extrem.

2.4.2 Säkerhetsskyddsklassificerade uppgifter

Säkerhetsskyddsklassificerade uppgifter avser uppgifter som rör säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585), det vill säga uppgifter som är av betydelse för Sveriges säkerhet. I den mån sådana uppgifter förekommer vid LiU ska dessa hanteras enligt särskilda rutiner som fastställs i en säkerhetsskyddsanalys.

Säkerhetsskyddsklassificerade uppgifter får under inga omständigheter lagras, bearbetas eller kommuniceras i LiU:s ordinarie IT-utrustning, system eller nätverk. Eventuell förekomst av säkerhetsskyddsklassificerade uppgifter ska inte heller inventeras eller förtecknas i enlighet med riktlinjerna för informationssäkerhet. Förekomsten av sådana uppgifter ska i stället meddelas muntligen till säkerhetsskyddschefen vid ett fysiskt möte.

2.4.3 Extrem nivå (konfidentialitet)

Extrem nivå tillämpas vid förekomst av stora mängder uppgifter som var och en uppfyller kriterierna för **höjd** nivå (se nedan), för uppgifter vars röjande skulle leda till allvarlig fara för liv eller hälsa, samt för information som uppfyller kriterierna för **höjd** nivå och som bedöms vara mål för utländsk underrättelseverksamhet eller motsvarande. **Extrem** nivå tillämpas normalt även för information som kan omfattas av absolut sekretess enligt offentlighets- och sekretesslagen (2009:400, OSL).

Exempel på uppgifter som klassas med **extrem konfidentialitet**:

- journalsystem (samling av känsliga personuppgifter)
- forskningsdata som omfattas av statistiksekretess (24 kap. 8 § OSL)

- hemadress till person i utsatt ställning (risk för liv och hälsa)
- information om enskilda dissidenter i totalitära regimer (mål för underrättelseverksamhet).

2.4.4 Höjd nivå (konfidentialitet, riktighet och tillgänglighet)

För dimensionerna konfidentialitet, riktighet och tillgänglighet ska **höjd** nivå tillämpas om allvarlig skada kan drabba LiU, dess samarbetspartner eller enskild individ om **konfidentialiteten** bryts, information förvanskas (**riktighet**) eller information förloras (**tillgänglighet**). **Höjd** nivå bör endast tillämpas då risk för allvarlig skada föreligger. Allvarlig skada ska tolkas i ett LiU-övergripande och inte uteslutande ekonomiskt perspektiv. Det kan exempelvis röra sig om en stor ekonomisk skada eller minskat anseende för LiU, eller att en individ lider skada till följd av att uppgifter om denne röjs.

Vidare ska **höjd konfidentialitet** gälla information som kan omfattas av stark sekretess (sekretess med omvänt skaderekvisit) enligt OSL samt för känsliga personuppgifter (se avsnitt 2.5.2). Se *LiU:s vägledning om offentlighet och sekretess* för stöd vid bedömning av sekretess och konfidentialitet.

Vid användning av **höjd tillgänglighet** ska det alltid vara möjligt att ange konkreta krav på tillgänglighet.

Exempel på uppgifter som klassas med **höjd** nivå:

- information om personliga förhållanden som framkommer vid besök hos kurator, psykolog, eller studievägledning (höjd konfidentialitet)
- lärplattform (höjd tillgänglighet)
- register över studieresultat (höjd riktighet)
- lista över anställdas bostadsadresser (höjd konfidentialitet).

2.4.5 Normal nivå (konfidentialitet, riktighet och tillgänglighet)

Om nivån inte är **höjd** eller **extrem** används i de allra flesta fall nivån **normal**, som ska ge ett grundskydd. Notera att normal konfidentialitet inte innebär avsaknad av konfidentialitet utan att det räcker med grundskyddet; motsvarande gäller för övriga dimensioner.

Exempel på uppgifter som klassas på **normal** nivå:

- lista med namn eller personnummer på studenter
- lista med anställdas namn och personnummer
- handling som omfattas av svag sekretess (sekretess med rakt skaderekvisit).

2.4.6 Försumbar nivå (konfidentialitet)

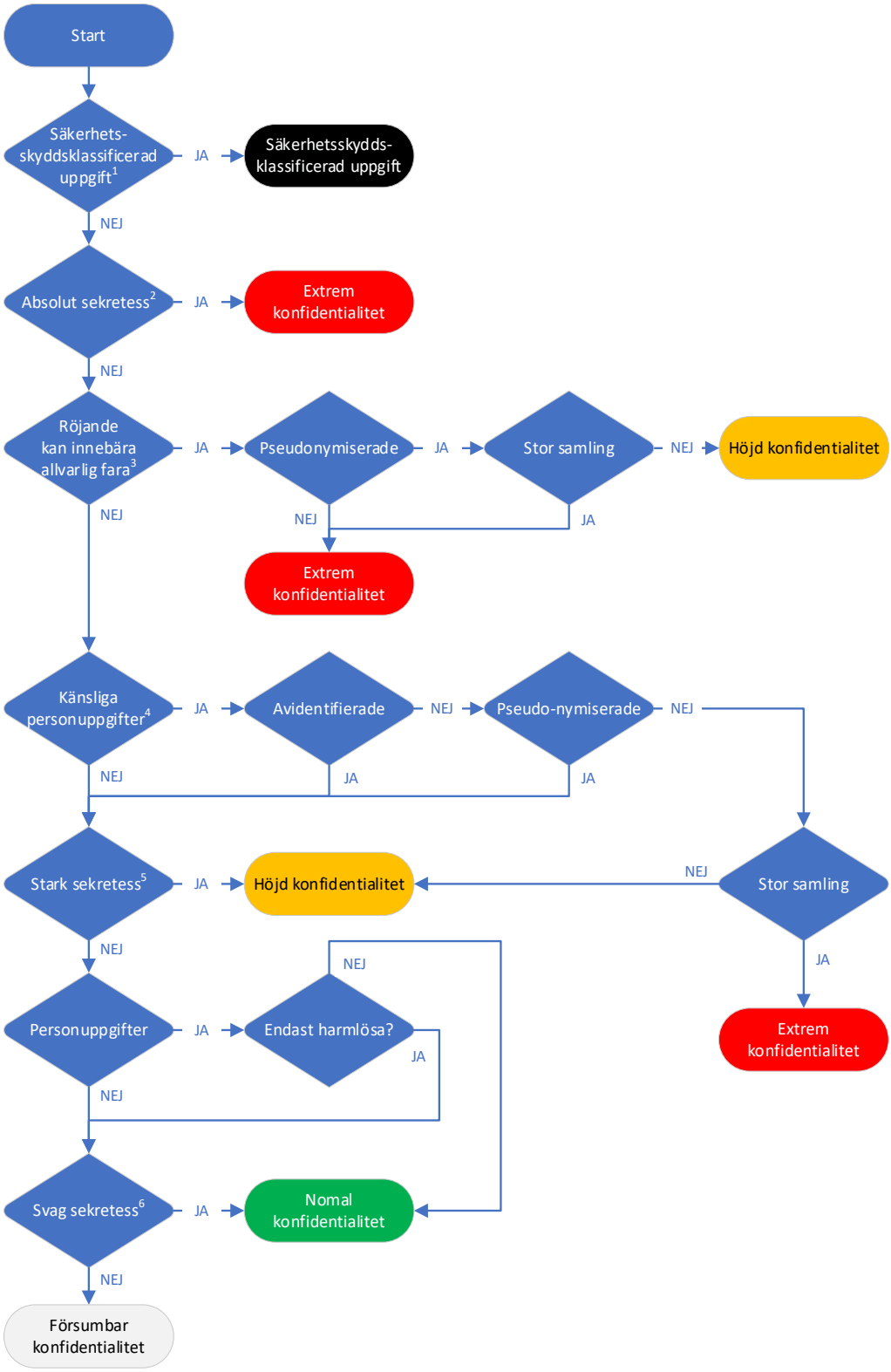
Försumbar konfidentialitet får tillämpas på informationstillgångar där kraven på konfidentialitet är synnerligen små eller obefintliga och där det endast förekommer **harmlösa personuppgifter** (se avsnitt 2.5.4). Hanteringen av sådana tillgångar kräver inte alla de skyddsmekanismer som tillämpas för normal nivå eller högre. Notera dock att lag och andra regelverk kring exempelvis personuppgifter och dokumenthantering måste följas.

Exempel på uppgifter som vanligtvis klassas med **försumbar konfidentialitet**:

- presentation av LiU som lärosäte
- publicerade vetenskapliga artiklar
- manuskript under bearbetande (om författaren önskar).

2.4.7 Flödesschema för informationsklassning

Flödesschemat på följande sida kan användas som stöd vid klassning av konfidentialitet. Notera att informationsägare efter analys kan välja en högre eller lägre klass baserat på konsekvensen för LiU och enskild vid ett eventuellt röjande av informationen.



[1]Säkerhetsskyddsklassificerad uppgift såsom den definieras i SFS 2021:955
[2]Sekretess enligt SFS 2009:400 som gäller ovillkorligen, utan krav på skadebedömning
[3]Känslig personuppgift vars röjande kan leda till allvarlig föra för liv och hälsa.
[4]Personuppgift enligt dataskyddsförordningens definition av särskilda kategorier av personuppgifter.
[5]Sekretess enligt SFS 2009:400 som gäller med omvänt skaderekvisit (sekretess i första hand).
[6]Sekretess enligt SFS 2009:400 som gäller med rakt skaderekvisit (offentlighet i första hand)

2.4.8 Särskilt skyddsvärd information

Begreppet särskilt skyddsvärd information används för att snabbare referera till information klassad med någon av nivåerna höjd eller extrem konfidentialitet, höjd riktighet, höjd tillgänglighet. Det finns flera riktlinjer som är tillämpliga för samtliga dessa informationsklassningar.

2.5 Personuppgifter

2.5.1 Allmänt

En personuppgift är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Vilka kategorier av personuppgifter som behandlas får stor påverkan på val av informationsklass. I detta avsnitt presenteras aspekter som påverkar just klassning. För mer utförlig vägledning kring behandling av personuppgifter hänvisas till *LiU:s vägledning för dataskydd*.

2.5.2 Känsliga personuppgifter

Känsliga personuppgifter är enligt dataskyddsförordningen[3] uppgifter om:

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening
- hälsa
- en fysisk persons sexualliv eller sexuella läggning
- genetiska eller biometriska uppgifter som entydigt identifierar en fysisk person.

Vidare likställs uppgifter som berör fällande domar i brottsmål samt lagöverträdelser med känsliga personuppgifter. Känsliga personuppgifter klassas vanligen med minst höjd konfidentialitet och större samlingar känsliga personuppgifter klassas typiskt med extrem konfidentialitet. Pseudonymisering kan dock påverka klassningen (se avsnitt 2.5.5).

Uppgifter om barn förtjänar särskilt skydd och det kan i många fall vara motiverat att klassa dem med höjd konfidentialitet.

2.5.3 Normala personuppgifter

Personuppgifter som inte är känsliga, inklusive personnummer, refereras fortsättningsvis till som normala personuppgifter. Personnummer är extra skyddsvärda och användningen är särskilt reglerad genom den så kallade dataskyddslagen[4] men vid informationsklassning betraktas personnummer som en normal personuppgift.

---

[3] 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)

[4] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

2.5.4 Harmlösa personuppgifter

Begreppet harmlösa personuppgifter, som används i vissa riktlinjer och beslut, omfattar normala personuppgifter som tack vare sin natur och sammanhang har ett lägre skyddsvärde än andra normala personuppgifter. Bedömningen påverkas också av i vilken utsträckning och hur de är tillgängliga i övrigt.

För att en uppgift ska kunna betraktas som harmlös måste den vara, och avsedd att vara, enkelt och allmänt tillgänglig. Den som berörs ska vara medveten om att uppgifterna är tillgängliga och kan komma att spridas. Uppgiften ska vara av en sådan art och användas på ett sådant sätt att den som berörs inte rimligen kan antas motsätta sig användningen eller spridningen. Slutligen ska uppgiften användas i ett sammanhang som innebär att den inte kombineras med andra uppgifter, där kombinationen inte kan betraktas som harmlös.

I de flesta fall är namn, yrkesmässiga kontaktuppgifter, författarskap, professionell anknytning och forskningsområde enkelt och allmänt tillgängliga, och används ofta i sammanhang och på sätt som uppfyller villkoren för att kunna betraktas som harmlösa.

Observera att begreppet harmlösa personuppgifter inte definieras i lag. Dataskyddsförordningen gäller även för dessa. Genom användning av begreppet harmlösa personuppgifter kan mer precisa krav ställas för hanteringen av universitetets information och onödigt belastande skyddsåtgärder undvikas, där så är befogat med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter.

Exempel på harmlösa personuppgifter:

- **Namn och kontaktuppgifter i författar- och referenslistor i vetenskaplig produktion.** Uppgifterna betraktas i normalfallet som harmlösa. Författarskap i akademiska sammanhang är generellt allmänt och enkelt tillgänglig information och författare motsätter sig i allmänhet inte att associeras med sin tidigare produktion.

Exempel som inte är harmlösa personuppgifter:

- **Namn och kontaktuppgifter till en person inom polis eller socialförvaltning.** Uppgiften betraktas inte som harmlös eftersom det rimligen kan antas att personen eller myndigheten skulle motsätta sig spridningen av uppgiften.
- **Deltagarlistor för en kurs eller konferens.** Uppgifterna betraktas inte som harmlösa eftersom information om var en viss person varit vid ett givet tillfälle tillförs genom sammanhanget.

2.5.5 Pseudonymisering av personuppgifter

Pseudonymisering av personuppgifter innebär att en uppgift inte längre kan tillskrivas en specifik person utan att kompletterande uppgifter används. Ett exempel är att uppgifter som kan identifiera en enskild person kodas på ett sådant sätt att det i en datamängd inte längre är möjligt att härleda informationen till en specifik individ utan tillgång till kodnyckel (pseudonymiseringsnyckel). En pseudonymiserad datamängd är fortfarande att betrakta som personuppgifter. Om det ingår känsliga personuppgifter, t.ex. uppgift om hälsa, i datamängden så omfattas den av all lagstiftning som berör känsliga personuppgifter. Rätt använd kan pseudonymisering vara en mycket effektiv skyddsåtgärd, vilket innebär att åtgärden påverkar vilken konfidentialitetsnivå som kan väljas (se flödesschemat under avsnitt 2.4.7).

För att pseudonymisering ska nå full effekt och motivera en förändring av konfidentialitetsnivå får det inte finnas kvar indirekta identifierande uppgifter i den pseudonymiserade datamängden.

Vid informationsklassning av kodnyckel (pseudonymiseringsnyckel) ska konfidentialiteten klassas enligt de kriterier som skulle berört den ursprungliga datamängden om pseudonymisering inte hade använts som skyddsåtgärd.

2.5.6 Anonymiserade uppgifter

Om identifierande uppgifter helt elimineras från en datamängd med personuppgifter så att uppgifterna inte längre direkt eller indirekt kan kopplas till en person så är uppgifterna anonymiserade. Uppgifterna är då inte personuppgifter och omfattas därför inte av de krav som exempelvis dataskyddsförordningen ställer.

Observera att data aldrig kan anses vara anonymiserat om det finns någon möjlighet för någon person eller organisation att enskilt eller tillsammans, direkt eller indirekt, härleda uppgiften till en fysisk person.

2.6 Skyddsnivåer för arbetsdatorer

Beroende på klassning krävs olika nivå på de skyddsåtgärder som säkrar LiU:s informationshantering. Olika medarbetare har dessutom olika krav på flexibiliteten i IT-miljön. För att underlätta avvägningen mellan skyddsåtgärder kontra flexibilitet och användbarhet klassas även den IT-utrustning som medarbetare vid LiU använder i skyddsnivåer.

Skyddsnivåerna bygger på färgerna **guld**, **silver**, **brons**, **vit** och **svart**. För normala IT-enheter (telefoner, surfplattor samt stationära och bärbara datorer) används färgerna **guld**, **silver** och **brons**. **Guld** ger starkast skydd och innebär lägst risk och lägre grad av flexibilitet, **silver** ger fortfarande ett mycket starkt skydd men tillåter högre flexibilitet medan **brons** ger svagast skydd och innebär högre risk och högre grad av flexibilitet.

Viss IT-utrustning verkar i speciella miljöer och tillåter inte normala säkerhetsåtgärder. För dessa används färgen **vit**. För annan IT-utrustning, exempelvis privatägda datorer, används färgen **svart**.

Guld	Enhet som hanteras, underhålls och inventeras av Digitaliseringsavdelningen. Högsta skydd aktiverat.
Silver	Som guld men med möjlighet för innehavaren att tillfälligt administrera utrustningen själv.
Brons	Möjlighet för innehavaren att inaktivera ytterligare skyddsåtgärder. Användaren kan själv ha administrativa behörigheter till utrustningen med ordinarie inloggning.
Vit	Enhet som inventeras, men inte hanteras eller underhålls, av Digitaliseringsavdelningen. Exempel på sådana enheter är datorer som styr eller är inbyggda i vetenskapliga instrument eller andra maskiner. Innehavaren av sådan enhet har ett särskilt ansvar för dess säkerhet.
Svart	Enhet som inte inventeras av Digitaliseringsavdelningen, exempelvis privatägd dator.

3 Riktlinjer för anställda och uppdragstagare

3.1 Inledning

I detta kapitel fastställs riktlinjer för anställda och andra uppdragstagare vid LiU som har ett användarkonto i LiU:s IT-miljö. Exempel på uppdragstagare är konsulter, inhyrd personal från bemanningsföretag, gästforskare, adjungerade, emeriti och arvodister. Riktlinjerna är obligatoriska att känna till och följa. Eventuella avsteg får göras endast efter skriftligt beslut av behörig beslutsfattare.

Förutom dessa riktlinjer ska hänsyn tas till flera andra regelverk och vägledningar, bland andra *LiU:s anvisningar rörande dokumenthantering*[5], *Vägledning om offentlighet och sekretess* och *Vägledning för personuppgiftsbehandling*.

Studenter (grundnivå och avancerad nivå) vid LiU omfattas normalt inte av dessa riktlinjer. För dem gäller i stället *Regler för studenters användning av IT-resurser vid Linköpings universitet (LiU-2018-01846)*.

3.2 Användning av IT-resurser och informationstillgångar

Vid LiU gäller följande riktlinjer för användning av IT-resurser och informationstillgångar:

1. Användare av LiU:s IT-resurser ska i användningen följa svensk lag. Vidare ska användning ske i enlighet med dessa riktlinjer såväl som andra riktlinjer publicerade i *LiU:s regelsamling*[6]. 3.2, p. 1 (1)
2. Det är inte tillåtet att i användningen förtala, förolämpa, förnedra eller kränka andra. 3.2, p. 2 (2)
3. Användare av LiU:s IT-resurser är skyldiga att följa anvisningar från Digitaliseringsdirektören, IT-säkerhetsgruppen (IRT) och systemadministratör med ansvar för respektive resurs. 3.2, p. 3 (3)
4. Det är inte tillåtet att utan uttryckligt skriftligt medgivande från systemägaren försöka höja sina behörigheter eller kringgå skyddsåtgärder i LiU:s IT-system. Det är inte heller tillåtet att använda LiU:s IT-resurser i syfte att försöka skaffa sig behörigheter man inte har rätt till i andra system. 3.2, p. 4 (4)
5. LiU:s IT-resurser är avsedda för användning i tjänsten. Privat användning är tillåten i sådan omfattning att det inte inkräktar på arbetet eller utsätter LiU för ökade risker. LiU:s IT-resurser får inte upplåtas eller lånas ut för privat användning av familjemedlemmar, bekanta eller andra. 3.2, p. 5 (5)
6. LiU:s IT-resurser får inte användas till affärsverksamhet, undantaget godkänd bisyssla där användningen inte medför kostnader för LiU, bryter mot avtals- eller licensvillkor eller på annat sätt orsakar skada eller risker. 3.2, p. 6 (6)

[5] https://go.liu.se/dok
[6] https://go.liu.se/styr

7. När LiU:s IT-utrustning används, transporteras eller förvaras utanför tjänstemiljön ska innehavaren vidta lämpliga åtgärder för att skydda utrustningen. Observera särskilt *Riktlinjer för säkert resande (dnr LiU-2018-00399)* samt *Vägledning för säkert distansarbete*[7]. 3.2, p. 7 (7)
8. Anställda och motsvarande uppdragstagare ska ta del av och följa anvisningar gällande hanteringen av information som de ges tillgång till genom sin anställning eller uppdrag. För privat användning av sådan information ska man begära ett utlämnande av informationen hos registrator eller hos den som har vården om den aktuella handlingen så att en objektiv sekretessprövning kan genomföras, om inte informationen är av uppenbart allmän karaktär, redan har offentliggjorts, eller om man har rätt att förfoga över den som privatperson[8]. 3.2, p. 8 (8)

3.3 Användarkonton och lösenord

Vid LiU gäller följande riktlinjer för användarkonton och lösenord:

1. Behörigheter till IT-resurser är personliga och får inte upplåtas till någon annan annat än under direkt överinseende. 3.3, p. 1 (10)
2. Det är inte tillåtet att lämna ut sitt lösenord till någon annan. Vid behov av att delge annan användare åtkomst till lagrad fil, e-post eller annan IT-resurs ska Digitaliseringsavdelningens kundcenter kontaktas. 3.3, p. 2 (11)
3. Det är inte tillåtet att begära att någon annan ska uppge sitt lösenord. 3.3, p. 3 (12)
4. Det är inte tillåtet att använda någon annans inloggningsuppgifter oavsett om denne själv har lämnat ut inloggningsuppgifterna eller inte. 3.3, p. 4 (13)
5. Lösenord som används för åtkomst till LiU:s IT-resurser får inte användas för någon extern tjänst. 3.3, p. 5 (14)
6. Vid registrering av e-postadress eller skapande av konto i externa tjänster för universitetets räkning ska e-postadress i universitets e-postsystem anges. 3.3, p. 6 (15)
7. Lösenord ska väljas så att de är svårgissade. Se även *Tips för säkra lösenord*[9]. Använd gärna en lösenordshanterare för lagring av personliga lösenord. Se även *Rekommendation om lösenordshanterare*[10]. 3.3, p. 7 (16)
8. Lösenord ska omgående bytas när det finns misstanke om att de blivit kända av någon obehörig. 3.3, p. 8 (17)

[7] https://go.liu.se/dist
[8] Närmast avses här till exempel sådana patenterbara uppfinningar som en anställd lärare vid LiU förfogar över i enlighet med lag (1949:345) om rätten till arbetstagares uppfinningar, eller sådana verk som en medarbetare förfogar över i enlighet med LiU:s tolkning och tillämpning av 1§ lag (1960:729) om upphovsrätt till litterära och konstnärliga verk såsom framgår av Allmänna råd om universitetets nyttjanderätt till upphovsrättsligt skyddat material (LiU-2017-03903).
[9] https://go.liu.se/lost
[10] https://go.liu.se/losh

3.4 Grundläggande IT- och informationssäkerhet

Vid LiU gäller följande riktlinjer för grundläggande IT- och informationssäkerhet:

1. Lagring av filer ska normalt ske på en LiU-gemensam lagringsserver (fillager eller OneDrive for business). Lagring enbart på lokal hårddisk bör undvikas. 3.4, p. 1 (19)
2. **Särskilt skyddsvärd** information får endast lagras och bearbetas på system som är godkända för berörd informationsklass. 3.4, p. 2 (235)
3. **Särskilt skyddsvärd** information får endast hanteras på utrustning som ägs av någon annan än LiU om informationen är avsedd att delas med denna. I övrigt får **särskilt skyddsvärd** information endast hanteras på IT-utrustning som ägs och underhålls av LiU. 3.4, p. 3 (205)
4. Utskrift av dokument bör hämtas med LiU-kort. Vid utskrift av **särskilt skyddsvärd** information ska utskrift omgående hämtas med LiU-kort eller göras på skrivare som övervakas under hela utskriften. 3.4, p. 4 (21)
5. Pappersdokument som slängs ska destrueras med dokumentförstörare av säkerhetsklass 4 eller högre om dokumentet innehåller **särskilt skyddsvärd** information. 3.4, p. 5 (22)
6. När lagringsmedia som innehållit **särskilt skyddsvärd** information inte längre ska användas för sitt ändamål ska detta lämnas till Digitaliseringsavdelningen för destruktion, eller så ska lagringsmediets innehåll raderas på ett sådant sätt att informationen inte kan återskapas. 3.4, p. 6 (23)
7. Användare av datorer ansvarar för att låsa datorn när vederbörande lämnar den utan uppsikt. Datorer eller andra enheter ska inte lämnas obevakade där stöldrisken inte är försumbar. 3.4, p. 7 (25)
8. Användare av mobila enheter ansvarar för att skydda enheten med skärmlås (minst sexställig PIN-kod, lösenord eller fingeravtryck). 3.4, p. 8 (26)
9. Medarbetare och andra uppdragstagare bör kontrollera riktigheten i begäran om åtgärder som de misstänker kan komma från en obehörig källa, exempelvis i form av nätfiske eller andra bedrägeriförsök. 3.4, p. 9 (27)
10. Ej betrodda tillbehör ska inte anslutas till LiU:s datorer. Sådana tillbehör innefattar t.ex. USB-minnen och utrustning för skärmavbildning som utomstående ber att få ansluta. 3.4, p. 10 (28)
11. Den som upptäcker eller får kännedom om säkerhetsbrister i informationssystem eller IT-tjänster som LiU använder eller ansvarar för ska omgående rapportera dessa till universitetets IT-säkerhetsgrupp på e-postadress infosec@liu.se. 3.4, p. 11 (29)

3.5 Förlust av nycklar och passerkort

Vid LiU gäller följande riktlinjer för förlust av nycklar och passerkort:

1. Vid förlust av passerkort ska kortet omgående spärras genom Infocenter eller integra@liu.se. Om kortet gett tillgång till känsliga miljöer, t.ex. där **särskilt** 3.5, p. 1 (210)

skyddsvärd information förvaras, ska förlusten även anmälas till integra@liu.se för att säkerställa att kortet inte använts av obehörig person.

2. Förlust av nycklar ska omgående anmälas till den man kvitterat ut nycklarna från. 3.5, p. 2 (216)

3.6 Molntjänster

Vid LiU gäller följande riktlinjer för molntjänster:

1. Användning av molntjänster där extern part är huvudman och styr ändamål och medel med behandlingen är tillåten under förutsättning att gällande lagstiftning följs. 3.6, p. 1 (30)
2. Information där LiU är huvudman får endast hanteras i molntjänst efter beslut av Digitaliseringsdirektören om inte annat framgår av dessa riktlinjer. Den aktuella listan över godkända molntjänster finns publicerad på *Användning av molntjänster*[11]. 3.6, p. 2 (32)
3. Informationsägare kan under de förutsättningar som beskrivs i avsnitt 4.5, p. 2 fatta beslut om användning av molntjänster. 3.6, p. 3 (31)
4. Lärare kan under de förutsättningar som beskrivs i avsnitt 4.5, p. 3 fatta beslut om användning av molntjänster i sin undervisning. 3.6, p. 4 (180)

3.7 E-post

Vid LiU gäller följande riktlinjer för e-post:

1. All e-postkorrespondens som sker i tjänsten ska hanteras i det e-postsystem som anvisas av Digitaliseringsdirektören och med e-postadress som har formen förnamn.efternamn@liu.se eller funktionsadress@[domän.]liu.se. Privat utrustning får ansluta till e-postsystemet endast genom LiU:s webbmail. Se även avsnitt 3.10, p. 1 för hantering av nycklar till krypterad e-post. 3.7, p. 1 (34)
2. Det är inte tillåtet att automatiskt vidarebefordra e-post till externa e-postleverantörer. Det är inte heller tillåtet att skicka e-post med avsändaradress som slutar på liu.se från externa e-postleverantörer. 3.7, p. 2 (35)
3. **Särskilt skyddsvärd** information som hanteras via e-post ska krypteras och signeras genom S/MIME, PGP eller annan tillförlitlig metod. Annan behandling av **särskilt skyddsvärd** information via e-post är förbjuden med de undantag som fastställs nedan. Vid tillämpning av undantagen ska uppgiften antingen diarieföras och sedan raderas ur e-posten eller gallras inom en vecka från det att aktuellt ärende är avslutat. 3.7, p. 3 (36)

   Om en individ tillhandahåller känsliga uppgifter om sig själv via e-post, utan föregående uppmaning från LiU, får dessa fortsätta behandlas i okrypterad e-post enbart om det är nödvändigt och rimliga alternativ saknas; om möjligt ska andra kommunikationssätt användas. Behandling i okrypterad e-post måste upphöra så snart ärendet är avslutat eller om berörd individ begär att den ska upphöra.

[11] https://go.liu.se/moln

Uppgift om en persons facktillhörighet får hanteras okrypterad via e-post om personuppgiftsbehandlingen är nödvändig för att säkerställa personens rättigheter inom arbetsrätten, okrypterad e-post är det enda rimliga kommunikationssättet, och både avsändare och mottagare av e-postmeddelandet använder e-postadress som slutar på liu.se.

3.8 Stöld och förlust av IT-utrustning

Vid LiU gäller följande riktlinjer för stöld och förlust av IT-utrustning:

1. Stöld eller annan förlust av dator, surfplatta, mobiltelefon eller annan IT-utrustning ska polisanmälas av berörd medarbetare. Förlusten ska även anmälas till Digitaliseringsavdelningen tillsammans med eventuellt ärendenummer från Polisen. Digitaliseringsavdelningen kommer i sin tur att meddela universitetets säkerhetschef. Om personuppgifter förekommit på utrustningen ska en anmälan av personuppgiftsincident göras enligt webbsidan *Personuppgiftsincident*[12]. 3.8, p. 1 (46)

3.9 Avyttring av IT-utrustning

Vid LiU gäller följande riktlinjer för avyttring av IT-utrustning:

1. Avyttring av datorer, telefoner, surfplattor och andra enheter samt lagringsmedia görs normalt av Digitaliseringsavdelningen. Den som ombesörjer avyttringen ska beakta riktlinjerna i avsnitt 6.9. 3.9, p. 1 (47)
2. Vid donation av IT-utrustning ska utrustningen först lämnas in till Digitaliseringsavdelningen för fabriksåterställning, rensning av lagringsmedia, licenser, konfiguration och dylikt. 3.9, p. 2 (166)

3.10 Användning av privat utrustning

Vid LiU gäller följande riktlinjer för användning av privat utrustning:

1. **Särskilt skyddsvärd** information får inte hanteras på privat utrustning. Detta inkluderar nycklar för dekryptering av **särskilt skyddsvärd** information, t.ex. för dekryptering av e-post krypterad med S/MIME eller PGP. 3.10, p. 1 (48)
2. Den som ansluter privat utrustning till LiU:s datornät eller använder privat dator för att hantera LiU:s information ansvarar för att underhålla utrustningen så att den inte utgör ett IT-säkerhetshot. Operativsystem och programvara ska hållas uppdaterad och datorn ska ha uppdaterade skydd mot skadlig programvara (antivirusskydd). 3.10, p. 2 (49)
3. Privat utrustning ansluten till LiU:s datornät kan komma att utsättas för säkerhetstester av universitetets IT-säkerhetsgrupp. Utrustning där sårbarheter upptäcks utgör en informationssäkerhetsrisk och kan komma att blockeras. Det är inte tillåtet att försöka kringgå sådan blockering. 3.10, p. 3 (50)

[12] https://go.liu.se/pui

3.11 Övervakning av IT-resurser och åtgärder vid regelbrott

Vid LiU gäller följande riktlinjer för övervakning av IT-resurser och åtgärder vid regelbrott:

1. Systemadministratörer kan komma att övervaka system och datornät, inklusive ta del av nätverkstrafik och lagrade data, för att säkerställa en tillförlitlig drift och godtagbar säkerhetsnivå i LiU:s IT-system och för att utreda IT-incidenter eller misstänkta brott mot LiU:s regelverk. 3.11, p. 1 (51)
2. Vid brott mot LiU:s regelverk eller användarinstruktioner kan enskilds tillgång till IT-resurser komma att begränsas. Sådan begränsning kan också ske för att hindra pågående IT-angrepp (exempelvis dataintrång eller skadlig kod). 3.11, p. 2 (52)
3. Brott mot dessa riktlinjer kan komma att överlämnas till prefekt/motsvarande eller hanteras enligt *LiU:s riktlinjer för hantering av misstänkta oegentligheter, missförhållanden och brott*. Misstänkta lagbrott kan komma att polisanmälas. 3.11, p. 3 (53)
4. Vid allvarliga brott mot dessa riktlinjer, utredning av misstänkt oegentlighet eller lagbrott kan IT-utrustning som ägs av LiU komma att omhändertas och granskas av universitetets IT-säkerhetsgrupp. Granskningen kan komma att inkludera all data som lagras på utrustningen eller i LiU:s IT-system. 3.11, p. 4 (54)

3.12 Särskilda situationer

I detta avsnitt samlas riktlinjer som endast blir aktuella för ett begränsat antal individer med mer tekniskt orienterade arbetsuppgifter (exempelvis den som administrerar IT-utrustning som inte underhålls av Digitaliseringsavdelningen, utvecklar egna IT-system, m.m.):

1. Anskaffning av domännamn ska ske genom Digitaliseringsavdelningen som säkerställer att DNSSEC används samt att LiU registreras som innehavare. Undantag kan ske om extern part är huvudman. 3.12, p. 1 (78)
2. Innehavaren av en dator eller annan IT-utrustning som inte underhålls av IT-avdelningen (skyddsnivå vit eller **svart** som ägs av universitetet) ska säkerställa att en systemägare finns utsedd. Systemägaren ansvarar för att riktlinjer i kapitel 6 samt, i tillämpliga fall, kapitel 7 efterlevs. 3.12, p. 2 (238)
3. Vid utveckling av IT-system ska säkerhetsaspekter beaktas på ett systematiskt sätt. Den som kravställer eller genomför systemutveckling ska säkerställa 3.12, p. 3 (217)
   - att riktlinjer i kapitel 6 som är tillämpliga under utvecklingsfasen efterlevs,
   - att riktlinjer i kapitel 7 som är tillämpliga under utvecklingsfasen efterlevs om IT-systemet som utvecklas är avsett att hantera **särskilt skyddsvärd** information eller om användningen inte är begränsad till forskning och undervisning vid ett mindre antal institutioner,
   - att behandling av personuppgifter minimeras och begränsas till den mängd och de kategorier av uppgifter som krävs för att systemet ska kunna användas för avsett syfte,
   - att det är möjligt att ta fram registerutdrag samt korrigera och radera personuppgifter, samt
   - att det finns en systemägare utsedd innan systemet börjar användas.

4. Vid analys eller annat arbete med skadlig programvara (t.ex. datavirus) ska särskilt skyddad IT-miljö användas som minimerar risken för LiU:s övriga verksamhet. Innan arbete med skadlig kod inleds ska universitetets IT-säkerhetsgrupp (infosec@liu.se) informeras. 3.12, p. 4 (167)

4 Riktlinjer för anskaffning

4.1 Inledning

I detta kapitel samlas riktlinjer som ska användas vid all anskaffning av produkter eller tjänster där universitetets information kan komma att behandlas.

4.2 Allmänt

Vid LiU gäller följande allmänna riktlinjer för anskaffning:

1. Innan anskaffning påbörjas ska en informationsklassning göras av den information som leverantören, systemet eller tjänsten kommer att hantera. Kravställning i anskaffningen ska göras med hänsyn till identifierad informationsklass. 4.2, p. 1 (190)
2. Om en leverantör kommer att behandla information klassad med **höjd konfidentialitet** eller högre ska en lämplighetsbedömning av leverantören göras. Leverantören ska normalt betraktas som olämplig om denne omfattas av ett annat lands lagstiftning som kan innebära att uppgifterna röjs. 4.2, p. 2 (211)
3. Information som omfattas av sekretess får behandlas av extern leverantör endast om denne är bunden av sekretess enligt svensk lag eller avtal. 4.2, p. 3 (209)

4.3 Anskaffning som innebär att leverantör behandlar personuppgifter

Riktlinjer i detta avsnitt ska tillämpas vid anskaffning där en leverantör kommer att behandla personuppgifter för LiU:s räkning. I tillägg till dessa riktlinjer finns ett antal riktlinjer under i avsnitt 5.6 som informationsägare måste beakta innan en anskaffning påbörjas. Observera särskilt riktlinjerna 5.6, p. 5 och 5.6, p. 7 som kan påverka valet av personuppgiftsbiträde.

Vid LiU gäller följande riktlinjer för anskaffning som innebär att leverantör behandlar personuppgifter:

1. Vid anskaffning av tjänster som innebär att personuppgifter behandlas av tredje part för LiU:s räkning ska personuppgiftsbiträdesavtal upprättas. 4.3, p. 1 (208)
2. Personuppgifter som behandlas av en leverantör ska före överföring till leverantören avidentifieras eller pseudonymiseras om det är möjligt med hänsyn till tjänstens syfte och verksamhetens behov. 4.3, p. 2 (212)
3. Leverantören ska endast ges tillgång till de uppgifter som krävs för att utföra tjänsten. Vidare ska leverantören ha förmågan att tillhandahålla registerutdrag samt korrigera och radera uppgifter. 4.3, p. 3 (214)

4.4 Anskaffning av IT-system

Vid LiU gäller följande riktlinjer för anskaffning av IT-system:

1. Vid upphandling och annan anskaffning av nya IT-system ska krav på informationssäkerhet ställas för att säkerställa efterlevnad av tekniska aspekter i dessa riktlinjer. Digitaliseringsavdelningen underhåller en katalog med baskrav för IT. Genom användning av denna katalog säkerställs att samtliga riktlinjer i kapitel 6 4.4, p. 1 (77)

och 7 som är möjliga att adressera under anskaffningen beaktas. Se *Baskrav vid upphandling av system och tjänster med IT-komponenter*[13].

2. I samband med att upphandling eller utveckling av IT-system inleds ska en planering av förvaltningsfasen genomföras. En systemägare ska utses innan införandet påbörjas. Detta gäller även system som är avsedda för test eller utvärdering. 4.4, p. 2 (189)

4.5 Anskaffning av molntjänster

Under detta avsnitt samlas särskilda aspekter som gäller vid anskaffningen av molntjänster. Notera att användning av en molntjänst där en extern part är huvudman och styr ändamål och medel med behandlingen inte anses som anskaffning. Användning av sådan tjänst är tillåten under förutsättning att gällande lagstiftning följs; se avsnitt 3.6, p. 1.

Vid LiU gäller följande riktlinjer för anskaffning av molntjänster:

1. Information där LiU är huvudman får endast hanteras i en molntjänst efter beslut av Digitaliseringsdirektören om inte annat framgår av dessa riktlinjer. 4.5, p. 1 (83)
2. Informationsägare kan själv fatta beslut om användning av en molntjänst om informationen som ska hanteras i tjänsten är klassad med **försumbar konfidentialitet**, **normal riktighet** och **normal tillgänglighet**. Informationsägaren ska före ett sådant beslut säkerställa att gällande lagstiftning efterlevs, särskilt avseende personuppgifter, offentlighet och sekretess samt arkivering. Beslut om att godkänna en molntjänst ska sändas till IT-säkerhetsgruppen. 4.5, p. 2 (206)
3. Lärare kan själva fatta beslut om användning av en molntjänst i sin undervisning förutsatt att användning kan ske utan att personuppgifter sprids till den som tillhandahåller tjänsten, samt att informationen som hanteras är klassad med **försumbar konfidentialitet**, **normal riktighet** och **normal tillgänglighet**. Om registrering krävs för användning av tjänsten ska läraren upplysa deltagarna om hur registrering kan göras anonymt. Beslut om att godkänna en molntjänst ska sändas till IT-säkerhetsgruppen. 4.5, p. 3 (207)

4.6 Riskägare

Nedan anges riskägare för riktlinjer i detta kapitel.

4.2, p. 1	Informationssäkerhetssamordnaren
4.2, p. 2	Informationssäkerhetssamordnaren
4.2, p. 3	Rektor
4.3, p. 1	Rektor
4.3, p. 2	Rektor
4.3, p. 3	Rektor
4.4, p. 1	Informationssäkerhetssamordnaren
4.4, p. 2	Informationssäkerhetssamordnaren
4.5, p. 1	Rektor
4.5, p. 2	IT-direktören
4.5, p. 3	IT-direktören

[13] https://go.liu.se/krav

5 Riktlinjer för informationsägare

5.1 Inledning

Riktlinjerna i detta avsnitt utgör skyddsåtgärder för information som ska tillämpas av informationsägaren. Kapitel 2 beskriver rollen informationsägare översiktligt. Informationsägare utses enligt *Rutiner för att utse informationsägare samt inventering av vissa informationstillgångar (dnr LiU-2023-00878)*.

Detta kapitel innehåller huvudsakligen organisatoriska skyddsåtgärder. Tekniska skyddsåtgärder berör oftast ett specifikt informationssystem. Genom att omsorgsfullt klassa information och välja system baserat på klassning säkerställer informationsägare att även tekniska skyddsåtgärder tillämpas.

5.2 Informationsägarens övergripande ansvar

Vid LiU gäller följande riktlinjer avseende informationsägarens övergripande ansvar:

1. Informationsägaren ska klassa information som denne ansvarar för enligt LiU:s klassningsmodell, som beskrivs i kapitel 1. 5.2, p. 1 (198)
2. Informationsägaren ansvarar för att välja och anvisa IT-system som uppfyller erforderligt behov av informationssäkerhet. Informationsägaren ska beakta vilka informationsklasser systemet är avsett att hantera samt eventuell särskild riskbehandling systemägaren informerat om (se avsnitt 6.2, p. 2). 5.2, p. 2 (197)
3. Informationsägare ska säkerställa att alla som arbetar med **särskilt skyddsvärd** information har god kompetens gällande dess hantering, t.ex. de IT-system som används. 5.2, p. 3 (106)
4. Innan externa uppdragstagare, samarbetspartner eller andra aktörer ges tillgång till information vid LiU, ska det säkerställas att vederbörande är bunden att ta del av och följa lämpliga anvisningar gällande hantering av information som denne ges tillgång till i sitt uppdrag eller annat samarbete. Se även *LiU:s vägledning om offentlighet och sekretess*[14]. 5.2, p. 4 (107)

5.3 Förteckning av informationstillgångar

Vid LiU gäller följande riktlinjer för förteckning av informationstillgångar:

1. Informationstillgångar ska inventeras, klassificeras och förtecknas enligt de former som fastställs i *Rutiner för att utse informationsägare samt inventering av vissa informationstillgångar (dnr LiU-2023-00878)*. 5.3, p. 1 (74)

5.4 Åtkomstkontroll

Exempel på åtkomstkontroll är lås till förvaring eller lokaler där information förvaras eller verifiering av användaridentitet och auktorisation i ett IT-system.

[14] https://go.liu.se/vosl

Vid LiU gäller följande riktlinjer för åtkomstkontroll:

1. Tillgång till **särskilt skyddsvärd** information ska ges endast den som behöver tillgången för utförandet av sina arbetsuppgifter eller sitt uppdrag vid LiU. Tillgång till annan information bör begränsas på samma sätt. 5.4, p. 1 (84)
2. Behörigheter ska återtas när behov av behörighet inte längre kvarstår. Efter avslutad anställning, uppdrag eller motsvarande ska behörigheter återtas om det inte finns synnerligen starka skäl att de kvarstår. 5.4, p. 2 (89)
3. Behörigheter till **särskilt skyddsvärd** information ska granskas regelbundet, för att upptäcka och korrigera felaktigheter. 5.4, p. 3 (88)
4. Vid indikation på att nycklar, koder, lösenord eller liknande röjts ska dessa ändras omgående. Röjande av lösenord ska rapporteras till universitetets IT-säkerhetsgrupp. 5.4, p. 4 (85)

5.5 Fysisk säkerhet

Vid LiU gäller följande riktlinjer för fysisk säkerhet:

1. Tillträde till lokaler där **särskilt skyddsvärd** information förvaras ska vara begränsad till personer som behöver åtkomsten för att utföra sina arbetsuppgifter. Sådana tillträden ska inventeras regelbundet. 5.5, p. 1 (108)
2. Tillträde till utrymme där **särskilt skyddsvärd** information förvaras ska loggas, t.ex. genom passersystem. 5.5, p. 2 (109)
3. Personer utan eget tillträde till lokal där **särskilt skyddsvärd** information förvaras och som behöver tillfällig åtkomst, t.ex. för att utföra en serviceåtgärd, ska eskorteras av en person som har tillträde till lokalen. 5.5, p. 3 (110)
4. Ändamålsenligt skydd ska används vid fysisk transport av **särskilt skyddsvärd** information. Information på elektroniska lagringsmedia ska vara krypterad med tillförlitlig metod. 5.5, p. 4 (111)
5. **Särskilt skyddsvärd** information eller system som behandlar sådan information ska förvaras i larmat utrymme vid LiU eller annat larmat utrymme som uppfyller krav gällande larmklass 2 enligt SSF 130.[15] 5.5, p. 5 (112)
6. Fysiskt utrymme där informationstillgång förvaras ska ha en ändamålsenlig miljö avseende exempelvis temperaturreglering, luftfuktighet, översvämningsskydd, brandskydd och elförsörjning. För utrymme där information klassad med **höjd riktighet** eller **höjd tillgänglighet** förvaras ska miljön vara övervakad för att möjliggöra snabb upptäckt av problem. 5.5, p. 6 (113)

[15] Övergripande beskrivning av SSF 130 finns beskriven i Vägledning för fysisk informationssäkerhet i it-utrymmen (MSB629). Låst och larmat utrymme vid LiU uppfyller normalt kraven för larmklass 2.

7. Fysiskt utrymme där **särskilt skyddsvärd** information förvaras ska uppfylla säkerhetsklass SSF 200, skyddsklass 2 avseende fysiskt intrång[16], alternativt ska informationen förvaras i värdeskåp. Värdeskåpets klass ska väljas efter värdet på den tillgång som ska skyddas. 5.5, p. 7 (114)
8. Fysiska informationstillgångar klassade med **höjd riktighet** eller **höjd tillgänglighet** ska i möjligaste mån dupliceras. Duplikat ska förvaras fysiskt separerat från original. 5.5, p. 8 (117)
9. Vid förvaring av **särskilt skyddsvärd** information utanför tjänstemiljö ska ändamålsenligt skydd finnas. 5.5, p. 9 (118)
10. För information klassad med **höjd konfidentialitet** eller högre bör informationsägaren fastställa anvisningar för hur och var man får kommunicera om informationen, t.ex. var man får tala om den, om man får diskutera den per telefon eller om man får skicka den via SMS. 5.5, p. 10 (119)

5.6 Särskilda krav vid behandling av personuppgifter

Behandling av personuppgifter medför omfattande krav utifrån dataskyddsförordningen. En utförlig vägledning till dataskyddsförordningen finns på intranätssidan *Vägledningar för personuppgiftsbehandling*[17]. Vid varje institution finns minst en kontaktperson för dataskyddsfrågor som kan ge stöd i frågor om tillämpningen av förordningen, se intranätssidan *Dataskydd*[18].

Vid LiU gäller följande riktlinjer för särskilda krav vid behandling av personuppgifter:

1. Den som ansvarar för en ny aktivitet där personuppgifter ska behandlas (normalt informationsägaren) ska säkerställa: 5.6, p. 1 (90)
   - att det är klarlagt vilken eller vilka organisationer som är personuppgiftsansvariga,
   - att det finns en rättslig grund för personuppgiftsbehandlingen,
   - att personuppgiftsbiträdesavtal tecknas vid anlitande av personuppgiftsbiträden eller om LiU är personuppgiftsbiträde,
   - att eventuellt delat personuppgiftsansvar är skriftligen dokumenterat,
   - att endast de som behöver uppgifterna ges tillgång till dem,
   - att uppgifter avidentifieras där så är möjligt utan att omöjliggöra eller avsevärt försvåra syftet med behandlingen, samt
   - att personuppgiftsbehandlingen anmäls till universitetets förteckning av personuppgiftsbehandlingar enligt vad som framgår av intranätssidan *Anmälan av personuppgiftsbehandlingar*[19].

[16] Övergripande beskrivning av SSF 200 finns beskriven i Vägledning för fysisk informationssäkerhet i it-utrymmen (MSB629). De flesta lokaler vid LiU uppfyller inte kraven på skyddsklass 2.
[17] https://go.liu.se/vdsk
[18] https://go.liu.se/dsko
[19] https://go.liu.se/fort

2. Vid behandling av känsliga personuppgifter ska, om möjligt, pseudonymisering tillämpas. 5.6, p. 2 (91)
3. Uppgifter ska vara korrekta och hållas uppdaterade. Riktlinjen är inte tillämpbar på arkiverade handlingar eller säkerhetskopior. 5.6, p. 3 (95)
4. Personuppgifter får endast behandlas så länge det behövs för att uppfylla det ändamål för vilka de samlades in. Så snart personuppgifterna inte längre behövs för sitt ändamål ska de arkiveras, gallras eller avidentifieras. Vid tveksamhet bör en arkivarie vid Dokument- och arkivenheten rådfrågas. 5.6, p. 4 (96)
5. Innan en ny personuppgiftsbehandling som sannolikt leder till en hög risk för de registrerade ska en konsekvensbedömning genomföras i samråd med LiU:s dataskyddsombud. Integritetsskyddsmyndigheten tillhandahåller en detaljerad vägledning kring vad som menas med ”sannolikt leder till hög risk”, se Integritetsskyddsmyndighetens webbsida *Vilka måste göra en konsekvensbedömning?*[20]. 5.6, p. 5 (97)
6. Personuppgiftsincidenter ska omgående rapporteras enligt gällande rutiner (se intranätssidan *Personuppgiftsincident*[21]). Notera även avsnitt 5.7, p. 1. 5.6, p. 6 (98)
7. Överföring av personuppgifter till land utanför EU/EES är förbjuden om inte landet har en adekvat skyddsnivå eller om minst en lämplig skyddsmekanism enligt dataskyddsförordningen används. Exempel på skyddsmekanismer är användning av EU-kommissionens standardavtalsklausuler eller att mottagaren är ansluten till en uppförandekod eller annan certifiering som godkänts av EU-kommissionen. Som alternativ till ovanstående kan undantagsvis överföring ske med stöd av artikel 49 i dataskyddsförordningen.[22] 5.6, p. 7 (99)

5.7 Incidentrapportering

Vid LiU gäller följande riktlinjer för incidentrapportering:

1. Informationsägare ska säkerställa att avvikelser rörande konfidentialitet, riktighet och tillgänglighet för **särskilt skyddsvärd** information omgående rapporteras till universitetets IT-säkerhetsgrupp. Notera även avsnitt 5.6, p. 6. 5.7, p. 1 (102)

5.8 Samverkan med externa aktörer

Vid LiU gäller följande riktlinjer för samverkan med externa aktörer:

1. Vid samarbeten där en extern part är ansvarig huvudman kan de IT-tjänster som huvudmannen anvisar normalt användas. Om personuppgifter behandlas och parterna är gemensamt personuppgiftsansvariga bör det framgå av en skriftlig överenskommelse vilken part som ansvarar för anvisning av IT-system för informationsbehandlingen. 5.8, p. 1 (231)

---

[20] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/vem-maste-gora-en-konsekvensbedomning/
[21] https://go.liu.se/pui
[22] Se PM - Genomgång av artikel 49 dataskyddsförordningen (dnr LiU-2022-01689) för mer information.

Om LiU är ansvarig huvudman ska systemval ske enligt samma principer som gäller för annan information vid LiU enligt 5.2, p. 2.

2. Information klassad med **höjd konfidentialitet** får överföras via e-post eller annan tjänst klassad för hantering av **normal konfidentialitet** under förutsättning att den först krypterats med tillförlitlig metod. 5.8, p. 2 (232)

5.9 Riskägare

Nedan anges riskägare för riktlinjer i detta kapitel.

5.2, p. 1	Informationssäkerhetssamordnaren
5.2, p. 2	Informationssäkerhetssamordnaren
5.2, p. 3	Informationsägaren
5.2, p. 4	Informationssäkerhetssamordnaren
5.3, p. 1	Informationssäkerhetssamordnaren
5.4, p. 1	Informationsägaren
5.4, p. 2	Informationsägaren
5.4, p. 3	Informationsägaren
5.4, p. 4	Informationssäkerhetssamordnaren
5.5, p. 1	Informationssäkerhetssamordnaren
5.5, p. 2	Informationssäkerhetssamordnaren
5.5, p. 3	Informationssäkerhetssamordnaren
5.5, p. 4	Informationsägaren
5.5, p. 5	Informationsägaren
5.5, p. 6	Informationsägaren
5.5, p. 7	Informationsägaren
5.5, p. 8	Informationsägaren
5.5, p. 9	Informationsägaren
5.5, p. 10	Informationsägaren
5.6, p. 1	Rektor
5.6, p. 2	Rektor
5.6, p. 3	Rektor
5.6, p. 4	Rektor
5.6, p. 5	Rektor
5.6, p. 6	Rektor
5.6, p. 7	Rektor
5.7, p. 1	Informationssäkerhetssamordnaren
5.8, p. 1	Rektor
5.8, p. 2	Informationsägaren

6 Riktlinjer för systemägare, alla IT-system

6.1 Inledning

Riktlinjerna i detta avsnitt utgör skyddsåtgärder för IT-system som ska tillämpas för **alla** IT-system vid LiU. Riktlinjerna omfattar alltså system oavsett vilken typ av uppgifter som hanteras och oavsett i vilken miljö systemet används.

I det fall en riktlinje inte är ändamålsenlig kan riskägare besluta om annan hantering av berörda informationssäkerhetsrisker i enlighet med *Rutiner för alternativ riskbehandling (dnr LiU-2023-00881)*.

6.2 Systemägare

Vid LiU gäller följande riktlinjer för systemägare:

1. Alla IT-system vid LiU ska ha en systemägare. Systemägare utses enligt de former som beskrivs i *Ledningssystem för informationssäkerhet - ramverk (dnr LiU-2023-00877)*. 6.2, p. 1 (171)
2. Systemägaren ska ta ställning till vilka informationsklasser som får behandlas i IT-systemet. Systemägaren ska säkerställa att systemet uppfyller de krav som ställs av dessa riktlinjer för valda informationsklasser alternativt att informationssäkerhetsrisker behandlas på annat sätt efter beslut av riskägare. Systemägaren ska kunna upplysa användare av systemet om vilka informationsklasser som är lämpliga att hantera i systemet samt eventuell alternativ riskbehandling som tillämpas. 6.2, p. 2 (172)
3. Om IT-systemet uteslutande används inom **forskning och undervisning** vid en eller ett mindre antal institutioner samt uteslutande hanterar information klassad med högst **normal konfidentialitet**, **normal riktighet** och **normal tillgänglighet** ska riktlinjerna i detta kapitel tillämpas. För andra IT-system ska ***även*** riktlinjerna i kapitel 7 tillämpas. 6.2, p. 3 (188)

6.3 Grundläggande säkerhet

Vid LiU gäller följande riktlinjer för grundläggande säkerhet:

1. IT-system som hanterar LiU:s information eller ansluts till LiU:s datornät ska löpande underhållas med de uppdateringar för säkerhet som tillhandahålls. Uppdateringar ska installeras så snart som möjligt och det ska finnas en rutin för omedelbar installation av akuta uppdateringar. 6.3, p. 1 (123)
2. Sårbarheter i IT-system ska åtgärdas skyndsamt då de blir kända eller påtalas. 6.3, p. 2 (125)
3. Systemägaren ska härda system genom att minst: 6.3, p. 3 (194)
   - byta eventuella standardlösenord,
   - aktivera grundläggande lokal brandvägg med lämpliga regler,
   - stänga av tjänster som inte används, och
   - se över säkerhetsinställningar och protokoll för aktiva tjänster.

4. Information bör överföras krypterad och signerad med tillförlitliga metoder vid elektronisk kommunikation. För **särskilt skyddsvärd** information se avsnitt 7.6, p. 2. För e-post se avsnitt 3.7. 6.3, p. 4 (223)
5. Information i IT-system och vid behov programvara för IT-system ska säkerhetskopieras så att den kan återskapas vid dataförlust. 6.3, p. 5 (127)
6. Systemloggar, webbserverloggar, och andra relevanta loggar ska skickas till Digitaliseringsavdelningens centrala loggserver, alternativt annan central logghanteringslösning, SIEM eller motsvarande. IT-säkerhetsgruppen ska på begäran ges tillgång till loggarna vid utredning av misstänkta incidenter. 6.3, p. 6 (240)
7. Utrustning ansluten till LiU:s datornät ska vara konfigurerade för att tillåta sårbarhetsscanning från IP-adresser som pekats ut av IT-säkerhetsgruppen. 6.3, p. 7 (155)
8. IT-system ska ha korrekt tid inställd. Tid ska synkroniseras med NTP eller motsvarande teknik från Digitaliseringsavdelningens tidskällor. 6.3, p. 8 (185)
9. IT-system ska enbart användas till sina avsedda syften. Det innebär t.ex. att servrar eller datorer avsedda för systemdrift inte ska användas för ordbehandling, att läsa e-post eller surfa på webben. Antalet installerade program ska hållas till ett minimum. 6.3, p. 9 (128)
10. Användning av datornät ska vara spårbar så att det utifrån IP-adress, tidstämpel och port går att härleda vilken användare som vid tillfället varit inloggad på respektive utrustning. För trådbundet nätverk ska det också vara möjligt att i efterhand avgöra vilket nätverksuttag som använts. 6.3, p. 10 (130)
11. Systemägaren ska informera universitetets IT-säkerhetsgrupp vid misstanke om säkerhetsbrister eller misstanke om inträffad informationssäkerhetincident i sina system. Vid misstanke om oegentligheter ska dessa dessutom hanteras i enlighet med *LiU:s riktlinjer för hantering av misstänkta oegentligheter, missförhållanden och brott*. 6.3, p. 11 (228)

6.4 Användarhantering och inloggning

Vid LiU gäller följande riktlinjer för användarhantering och inloggning:

1. Behörigheter, inklusive höga behörigheter, ska vara individuella. 6.4, p. 1 (86)
2. Identiteter med höga behörigheter, som inte är kopplade till en individ (t.ex. ”root” på Linux-system), ska enbart förekomma och användas när det är nödvändigt. Lösenord och andra autentiseringsuppgifter till sådana identiteter ska förvaras så att de skyddas mot obehörig åtkomst, och så att behörig åtkomst är spårbar. Autentiseringsuppgifter ska ändras när en person som tidigare haft tillgång till uppgifterna inte längre ska ha det. 6.4, p. 2 (227)

3. När lösenord används för inloggning ska de ha tillräcklig komplexitet. Digitaliseringsavdelningen fastställer krav på godtagbar komplexitet. Se *Krav på lösenordskomplexitet*[23]. När kraven på komplexitet ändras ska systemägaren säkerställa att samtliga lösenord uppfyller de nya kraven (t.ex. genom att användare byter lösenord). 6.4, p. 3 (133)
4. Lösenord ska överföras med tillförlitlig kryptering. 6.4, p. 4 (134)
5. Inloggningar och inloggningsförsök i IT-system ska loggas. Om möjligt ska även utloggningar loggas. Som minst ska tidpunkt, anslutande IP-adress och användarnamn loggas. Logg ska bevaras och gallras enligt LiU:s dokumenthanteringsplan. Loggen ska bevaras i mellan sex och arton månader om inte annat framgår av *LiU:s dokumenthanteringsplan*[24]. 6.4, p. 5 (186)
6. Inloggning till IT-system ska ske genom användning av LiU:s centrala kontodatabas, i första hand genom ADFS. Riktlinjen behöver inte tillämpas för system som riktar sig till färre än 100 studenter och medarbetare. 6.4, p. 6 (131)
7. Inloggning i webbaserade system ska inte ske genom autentisering direkt mot AD eller LDAP. 6.4, p. 7 (132)
8. Vid användning av lokal användardatabas ska lösenord lagras kodade på ett icke reversibelt sätt. LiU-ID bör inte ingå i användarnamnet. Lösenord bör kunna bytas av användaren själv. Observera att för system som omfattas av riktlinjer i kapitel 7 gäller striktare krav enligt avsnitt 7.4, p. 5. 6.4, p. 8 (230)

6.5 Webbaserade system

Dessa riktlinjer gäller webbaserade system som hanterar LiU:s information:

1. Webbaserade system ska fungera med den senaste versionen av de webbläsare som stöds. Användare förutsätts uppgradera webbläsare i takt med att nya versioner blir tillgängliga. 6.5, p. 1 (144)
2. System ska inte ställa krav på plugins i webbläsare och ska fungera med webbläsare med standardinstallation. Detta innebär att systemet exempelvis inte får kräva webbläsarplugin för Java, Flash, Silverlight, ActiveX eller liknande. 6.5, p. 2 (145)
3. Webbaserade system ska fungera utan särskilda inställningar eller säkerhetspolicys på klienten. Detta innebär att systemet ska fungera med webbläsare som stöds på en nyinstallerad dator eller enhet utan vidare justeringar. 6.5, p. 3 (146)
4. Webbaserade system som riktar sig till många användare ska vara åtkomliga under domänadress på formen *tjänst*.liu.se.[25] System som drivs i samarbete med extern part kan använda annan domänadress efter godkännande från Digitaliseringsdirektören. Omdirigering efter initial åtkomst är tillåten. 6.5, p. 4 (147)

[23] https://go.liu.se/kopx
[24] https://go.liu.se/dokp
[25] Hög grad av användning av interna domännamn ökar förutsättningarna för våra användare att identifiera nätfiske som nästan uteslutande använder externa domäner.

5. Certifikat för webbtjänster ska vara utfärdade av en betrodd certifikatutgivare. Certifikat för webbtjänst med domänadress som ägs av LiU (exempelvis alla domänadresser som slutar på .liu.se) ska utfärdas genom LiU CA (Sunet TCS), Let's Encrypt eller ”managed certificate” i Microsoft Azure. 6.5, p. 5 (148)
6. Webbaserade system ska vara åtkomliga med användning av HTTPS. System bör inte vara åtkomliga med HTTP utan bör i stället omdirigera till HTTPS. Vidare bör *HTTP strict transport security* (HSTS) användas. 6.5, p. 6 (150)
7. HTTPS för webbaserade system ska konfigureras enligt universitetets IT-säkerhetsgrupps rekommendationer, se *Teknisk beskrivning av kryptering*[26]. 6.5, p. 7 (151)

6.6 Serversäkerhet i nätverksbaserade tjänster

Nedanstående riktlinjer gäller såväl webbaserade system som andra system som kommunicerar över nätverket:

1. Det ska inte vara möjligt att använda tjänsten med protokoll med stora kända sårbarheter. Exempel på sådana protokoll är NTLM, SMBv1, SSL (version 1–3) och TLS version 1.0–1.1. 6.6, p. 1 (152)
2. Certifikat för TLS ska i förekommande fall hållas uppdaterade så länge tjänsten är i drift. Certifikat ska förnyas innan de förfaller. Förfallodatum för certifikat bör övervakas. 6.6, p. 2 (153)

6.7 IT-system med klient för persondator eller mobil enhet

Vid LiU gäller följande riktlinjer för IT-system med klient för persondator eller mobil enhet:

1. Klientprogramvara ska tillåta löpande uppdatering (patchning) av operativsystem och andra programvaror (webbläsare, Java, webbläsartillägg och liknande). 6.7, p. 1 (156)
2. Klientprogramvara ska inte kräva undantag i säkerhetsinställningar i operativsystem. Det innebär t.ex. att det inte får krävas gammal programvara, inställningar av betrodda webbplatser, undantag i säkerhetsprogram eller liknande. 6.7, p. 2 (157)
3. Klientprogramvara ska inte kräva att användaren har administratörsbehörighet på den dator där programvaran körs. 6.7, p. 3 (158)

6.8 Krav på användares IT-utrustning

Vid LiU gäller följande riktlinjer för krav på användares IT-utrustning:

1. Datorer och mobila enheter ska låsas automatiskt när de inte används. Låsning ska ske efter högst femton minuter för datorer och efter högst fem minuter för mobiltelefoner och surfplattor. Riktlinjen tillämpas inte under pågående föreläsning eller presentation. Permanenta undantag för exempelvis labbutrustning kan beviljas av riskägaren. 6.8, p. 1 (120)
2. Användares datorer ska ha ändamålsenligt skydd mot skadlig programvara. 6.8, p. 2 (199)

[26] https://go.liu.se/krypt

3. Bärbara datorer och andra mobila enheter ska vara konfigurerade för krypterad lagring med tillförlitliga metoder, se *Teknisk beskrivning av kryptering*[27]. Nyckel för dekryptering ska låsas till TPM eller motsvarande säkerhetsmodul. 6.8, p. 3 (239)
4. Bärbara datorer och andra mobila enheter ska kunna fjärraderas. 6.8, p. 4 (169)
5. Privat utrustning, utrustning som tillhör tillfälliga besökare och andra klienter på skyddsnivå **svart** som ansluts till LiU:s datornät ska anslutas separat från utrustning som ägs av LiU (logisk separation). 6.8, p. 5 (121)

6.9 Avveckling

Vid LiU gäller följande riktlinjer för avveckling:

1. Innan avveckling av IT-system som innehåller allmänna handlingar sker ska Dokument- och arkivenheten kontaktas för att upprätta en bevarandeplan för handlingarna eller revidera befintlig bevarandeplan, se *LiU:s strategi för bevarande av handlingar (dnr LiU-2018-01344)*. 6.9, p. 1 (79)
2. Det är inte tillåtet att avyttra utrustning utan att rensa eller förstöra lagringsmedia, konfigurationer och annan potentiellt känslig information. Vid avyttring av datorer, telefoner, surfplattor och andra enheter samt lagringsmedia ska *Linköpings universitets återbrukspolicy (dnr LiU-2015-02023)* beaktas. 6.9, p. 2 (81)
3. När lagringsmedia som innehåller **särskilt skyddsvärd** information inte längre ska användas för sitt ändamål ska innehåll raderas på ett sådant sätt att informationen inte kan återskapas. Alternativt ska lagringsmediet lämnas till Digitaliseringsavdelningen för destruktion. 6.9, p. 3 (80)

[27] https://go.liu.se/krypt

6.10 Riskägare

Nedan anges riskägare för riktlinjer i detta kapitel.

6.2, p. 1	Informationssäkerhetssamordnaren
6.2, p. 2	Informationssäkerhetssamordnaren
6.2, p. 3	Informationssäkerhetssamordnaren
6.3, p. 1	Informationssäkerhetssamordnaren
6.3, p. 2	Informationssäkerhetssamordnaren
6.3, p. 3	Systemägaren
6.3, p. 4	Systemägaren
6.3, p. 5	Systemägaren
6.3, p. 6	Informationssäkerhetssamordnaren
6.3, p. 7	IT-säkerhetsgruppen
6.3, p. 8	Informationssäkerhetssamordnaren
6.3, p. 9	Systemägaren
6.3, p. 10	IT-säkerhetsgruppen
6.3, p. 11	Informationssäkerhetssamordnaren
6.4, p. 1	Systemägaren
6.4, p. 2	Systemägaren
6.4, p. 3	Systemägaren
6.4, p. 4	Systemägaren
6.4, p. 5	Informationssäkerhetssamordnaren
6.4, p. 6	Informationssäkerhetssamordnaren
6.4, p. 7	IT-säkerhetsgruppen
6.4, p. 8	Systemägaren
6.5, p. 1	Informationssäkerhetssamordnaren
6.5, p. 2	Informationssäkerhetssamordnaren
6.5, p. 3	Informationssäkerhetssamordnaren
6.5, p. 4	Informationssäkerhetssamordnaren
6.5, p. 5	Informationssäkerhetssamordnaren
6.5, p. 6	Systemägaren
6.5, p. 7	Systemägaren
6.6, p. 1	Informationssäkerhetssamordnaren
6.6, p. 2	Informationssäkerhetssamordnaren
6.7, p. 1	Informationssäkerhetssamordnaren
6.7, p. 2	Informationssäkerhetssamordnaren
6.7, p. 3	Informationssäkerhetssamordnaren
6.8, p. 1	Informationssäkerhetssamordnaren
6.8, p. 2	Informationssäkerhetssamordnaren
6.8, p. 3	Informationssäkerhetssamordnaren
6.8, p. 4	Informationssäkerhetssamordnaren
6.8, p. 5	Informationssäkerhetssamordnaren
6.9, p. 1	Informationssäkerhetssamordnaren
6.9, p. 2	Informationssäkerhetssamordnaren
6.9, p. 3	Informationssäkerhetssamordnaren

7 Riktlinjer för systemägare, vissa IT-system

7.1 Inledning

Riktlinjerna i detta avsnitt utgör skyddsåtgärder för IT-system som ska tillämpas för system som

- är avsedda att behandla särskild skyddsvärd information, *eller*
- används vid ett flertal institutioner.

I det fall en riktlinje inte är ändamålsenlig kan riskägare besluta om annan hantering av berörda informationssäkerhetsrisker i enlighet med *Rutiner för alternativ riskbehandling (dnr LiU-2023-00881)*.

7.2 Dokumentation

Systemägaren ska dokumentera ställningstaganden enligt nedanstående riktlinjer. Dokumentationen bör göras genom att skapa en informationssäkerhetsplan i Digitaliseringsavdelningens förteckning över IT-system (se 7.2, p. 7).

1. Systemägaren ska dokumentera om systemet är centralt för LiU:s förmåga att utföra sitt uppdrag. Vid tveksamhet bör objektägaren fatta beslut i frågan. Om systemet saknar objektägare kan beslut fattas av Digitaliseringsdirektören. 7.2, p. 1 (220)
2. Systemägaren ska dokumentera vilken hård- och mjukvara som används i systemet. 7.2, p. 2 (219)
3. Systemägaren ska definiera mål för återställning i termer av RPO (recovery point objective) och RTO (recovery time objective): hur lång tids data som får gå förlorad respektive hur snabbt systemet måste vara återställt. 7.2, p. 3 (173)
4. Systemägaren ska identifiera behov av, och i förekommande fall definiera mål, för återställning av historiska data (point in time recovery). 7.2, p. 4 (174)
5. Systemägaren ska definiera mål för tillgänglighet, t.ex. i termer av tid över året, om målen överstiger ”best effort”. 7.2, p. 5 (175)
6. Systemägaren ska dokumentera systemets beroenden till andra interna och externa system. 7.2, p. 6 (192)
7. Systemägare ska anmäla förekomsten av IT-systemet till Digitaliseringsavdelningens förteckning över IT-system *Digitaliseringsavdelningens systemförteckning*[28]. 7.2, p. 7 (187)
8. Systemägaren ska dokumentera hur förändringar i systemet görs och hur risker i samband med förändring ska hanteras. 7.2, p. 8 (195)

[28] https://go.liu.se/sysinv

7.3 Separata driftsmiljöer och förändringshantering

Vid LiU gäller följande riktlinjer för separata driftsmiljöer och förändringshantering:

1. Systemägaren ska identifiera behov av, och i förekommande fall etablera, separata miljöer för produktion, utbildning av användare, test och utveckling. 7.3, p. 1 (176)
2. Förändringar som inte är av rutinmässig karaktär på IT-system som är centrala för LiU:s förmåga att utföra sitt uppdrag eller som hanterar **särskilt skyddsvärd** information ska prövas i en testmiljö innan de driftsätts i produktionsmiljö. 7.3, p. 2 (164)
3. Förändringar på IT-system som är centrala för LiU:s förmåga att utföra sitt uppdrag eller som hanterar **särskilt skyddsvärd** information ska göras på ett sätt som begränsar risken för att konfidentialitet, tillgänglighet eller riktighet påverkas på ett oönskat sätt. Detta kan exempelvis uppnås genom checklistor, granskningsprocess eller ändring av två personer i förening. 7.3, p. 3 (162)

7.4 Användarhantering och inloggning

Vid LiU gäller följande riktlinjer för användarhantering och inloggning:

1. Systemägaren ska ta ställning till vilka som ska ges åtkomst till systemet samt hur behörigheter tilldelas, granskas och återkallas. Behörigheter ska endast tilldelas den som behöver dem och återkallas när behovet upphör. Särskild vikt bör läggas vid hantering av privilegierade åtkomsträttigheter. 7.4, p. 1 (178)
2. Systemägare avgör vem som ska ha rollen systemadministratör för de system som denne ansvarar för. Systemägaren ska säkerställa att utpekade systemadministratörer bekräftar kännedomen om riktlinjerna för informationssäkerhet genom undertecknande av särskild blankett. 7.4, p. 2 (60)
3. Administrativa behörigheter ska tilldelas restriktivt och endast till användaridentiteter som uteslutande används för systemadministration. Användning av sådana identiteter ska kräva flerfaktorautentisering. 7.4, p. 3 (184)
4. Flerfaktorautentisering ska krävas vid åtkomst till information klassad med **extrem konfidentialitet**. Flerfaktorautentisering ska också krävas vid åtkomst från externt nätverk från klient med annan skyddsnivå än **silver** eller **guld**. Flerfaktorsautentisering behöver dock inte krävas för studenters åtkomst till information klassad med högst **normal konfidentialitet**. 7.4, p. 4 (202)
5. Vid användning av lokal användardatabas ska LiU-ID inte ingå i användaridentitet. Lösenord klassas med **höjd konfidentialitet** och **höjd riktighet**. Lösenord för lokal användardatabas ska lagras kodade på ett icke reversibelt sätt. Lösenord ska kunna bytas av användaren själv. Periodiskt återkommande tvingande lösenordsbyten ska undvikas.[29] 7.4, p. 5 (136)
6. Auktorisation av användare ska ske genom användning av grupper i LiU:s AD. Grupptillhörighet ska alltså kunna styra behörigheter i systemet. 7.4, p. 6 (137)

[29] Periodiskt återkommande lösenordsbyten bidrar totalt sett inte till en höjd IT-säkerhet då många användare kommer att välja enklare lösenord och i högre grad hantera sådana lösenord ovarsamt.

7. System som hanterar **särskilt skyddsvärd** information ska vid användning kräva klient med skyddsnivå **guld** eller **silver**. 7.4, p. 7 (122)

7.5 Loggning och behandlingshistorik

Vid LiU gäller följande riktlinjer för loggning och behandlingshistorik:

1. Aktivering av administrativa behörigheter i IT-system ska loggas. Systemägaren ska ta ställning till om andra aktiviteter som kräver administrativa behörigheter ska loggas. 7.5, p. 1 (203)
2. Åtgärder i IT-system som hanterar **särskilt skyddsvärd** information ska loggas. Loggen i sig klassas med **höjd riktighet**. Utöver vad som anges i avsnitt 6.4, p. 5 och 7.5, p. 1 ska minst följande händelser ska loggas: 7.5, p. 2 (139)
   - Läsning av information klassad med höjd eller **extrem konfidentialitet**.
   - Radering av information klassad med **höjd tillgänglighet** eller **höjd riktighet**.
   - Förändring av information klassad med **höjd riktighet**.
   - Förändringar av användare och behörigheter.
3. Logghändelser ska innehålla minst information om typ av händelse, tidpunkt för händelsen, subjekt (användare eller system) som initierade händelsen, samt uppgift som påverkades av händelsen. Tidpunkten ska vara korrekt och ha angiven eller känd tidszon. 7.5, p. 3 (140)
4. Loggar ska bevaras i mellan sex och arton månader om inte annat framgår av *LiU:s dokumenthanteringsplan*[30]. 7.5, p. 4 (141)

7.6 Kryptering och signering

Vid LiU gäller följande riktlinjer för kryptering och signering:

1. **Särskilt skyddsvärd** information ska överföras krypterad och signerad med tillförlitliga metoder vid elektronisk kommunikation. Information som inte är **särskilt skyddsvärd** *bör* överföras krypterad och signerad. För e-post se avsnitt 3.7. 7.6, p. 1 (142)
2. Lagring av information klassad med höjd eller **extrem konfidentialitet** ska ske i krypterad form. Information klassad med **höjd konfidentialitet** får dock lagras okrypterad i system som uppfyller riktlinjen 7.7, p. 8. Krypteringsnycklar för åtkomst av sådan lagring ska klassas med samma nivå som informationen. 7.6, p. 2 (143)

7.7 Systemförvaltning och drift

Vid LiU gäller följande riktlinjer för systemförvaltning och drift:

1. Vid säkerhetskopiering av information klassad med **höjd konfidentialitet** eller högre ska säkerhetskopian lagras krypterad. Krypteringsnycklar klassas med samma eller högre nivå som informationen. 7.7, p. 1 (165)

[30] https://go.liu.se/dokp

2. Säkerhetskopior ska förvaras skilda från original och skyddas på så sätt att en och samma person inte kan ändra eller utplåna både kopia och original. 7.7, p. 2 (170)

3. För system som är centrala för LiU:s förmåga att utföra sitt uppdrag eller som hanterar information klassad med **höjd tillgänglighet** eller **höjd riktighet** ska återläsningstest av säkerhetskopior genomföras årligen eller oftare. Återläsningstest ska säkerställa att återläsning är möjlig och kan ske inom förväntad tid avseende krav på tillgänglighet. 7.7, p. 3 (163)

4. IT-system som hanterar **särskilt skyddsvärd** information ska skyddas med nätverksbrandvägg med för ändamålet lämplig konfiguration. 7.7, p. 4 (154)

5. IT-system ska ha en ändamålsenlig driftsmiljö avseende temperaturreglering, luftfuktighet, översvämningsskydd, brandskydd och elförsörjning. För system som hanterar information klassade med **höjd tillgänglighet** ska driftmiljön vara övervakad för att möjliggöra snabb upptäckt av problem. 7.7, p. 5 (126)

6. IT-system med fysiska komponenter ska ha en plan för underhåll av dessa, anpassad till systemets krav på konfidentialitet, riktighet och tillgänglighet. 7.7, p. 6 (225)

7. IT-system och deras ingående fysiska komponenter ska övervakas på ett sätt som är ändamålsenligt med hänsyn tagen till systemets krav på tillgänglighet. 7.7, p. 7 (226)

8. IT-system ska placeras i utrymme som uppfyller SSF 200 skyddsklass 2 avseende fysiskt intrång[31] samt skyddas av larmsystem som uppfyller krav gällande larmklass 2 enligt SSF 130[32]. 7.7, p. 8 (201)

   Inpassering till sådant utrymme ska loggas, t.ex. genom passersystem. Tillträde till utrymmet ska endast ges personer som behöver åtkomsten för att utföra sina arbetsuppgifter. Personer med behov av tillfällig åtkomst, t.ex. för att utföra serviceåtgärd, ska eskorteras av någon med ordinarie tillträde.

9. Fjärradministration av IT-system ska göras genom säkra lösningar, t.ex. säker inloggningsserver eller privilegierad arbetsstation för administratör. 7.7, p. 9 (129)

[31] Övergripande beskrivning av SSF 200 finns beskriven i Vägledning för fysisk informationssäkerhet i it-utrymmen (MSB629). De flesta lokaler vid LiU uppfyller inte kraven på skyddsklass 2.
[32] Övergripande beskrivning av SSF 130 finns beskriven i Vägledning för fysisk informationssäkerhet i it-utrymmen (MSB629). Låst och larmat utrymme vid LiU uppfyller normalt kraven för larmklass 2.

7.8 Riskägare

Nedan anges riskägare för riktlinjer i detta kapitel.

7.2, p. 1	Informationssäkerhetssamordnaren
7.2, p. 2	Informationssäkerhetssamordnaren
7.2, p. 3	Informationssäkerhetssamordnaren
7.2, p. 4	Informationssäkerhetssamordnaren
7.2, p. 5	Informationssäkerhetssamordnaren
7.2, p. 6	Informationssäkerhetssamordnaren
7.2, p. 7	Informationssäkerhetssamordnaren
7.2, p. 8	Informationssäkerhetssamordnaren
7.3, p. 1	Informationssäkerhetssamordnaren
7.3, p. 2	Informationssäkerhetssamordnaren
7.3, p. 3	Informationssäkerhetssamordnaren
7.4, p. 1	Informationssäkerhetssamordnaren
7.4, p. 2	Informationssäkerhetssamordnaren
7.4, p. 3	Systemägaren
7.4, p. 4	Informationssäkerhetssamordnaren
7.4, p. 5	Systemägaren
7.4, p. 6	Systemägaren
7.4, p. 7	Informationssäkerhetssamordnaren
7.5, p. 1	Systemägaren
7.5, p. 2	Informationssäkerhetssamordnaren
7.5, p. 3	Informationssäkerhetssamordnaren
7.5, p. 4	Informationssäkerhetssamordnaren
7.6, p. 1	Informationssäkerhetssamordnaren
7.6, p. 2	Informationssäkerhetssamordnaren
7.7, p. 1	Systemägaren
7.7, p. 2	Systemägaren
7.7, p. 3	Informationssäkerhetssamordnaren
7.7, p. 4	Systemägaren
7.7, p. 5	Systemägaren
7.7, p. 6	Systemägaren
7.7, p. 7	Systemägaren
7.7, p. 8	Informationssäkerhetssamordnaren
7.7, p. 9	Informationssäkerhetssamordnaren

8 Riktlinjer för systemadministratörer

8.1 Inledning

I detta kapitel fastställs riktlinjer för informationssäkerhet för systemadministratörer. Vid konflikt med riktlinjer i kapitel 3 har kapitel 8 företräde.

Med systemadministratör menas här individ som har högre behörigheter än vanliga användare i ett IT-system och som har undertecknat särskild blankett för systemadministratörer (LiU-2022-01909).

8.2 Användning av konton för systemadministration

Vid LiU gäller följande allmänna riktlinjer för systemadministratörer:

1. Dedikerade administrationskonton, eller andra konton med höga behörigheter, ska inte användas annat än när arbetsuppgiften kräver det. 8.2, p. 1 (61)

8.3 Särskilda skyldigheter för systemadministratörer

Vid LiU gäller följande särskilda skyldigheter för systemadministratörer:

1. En systemadministratör ska iaktta tystnadsplikt gällande personuppgifter, uppgifter om andra personliga förhållanden samt sekretessbelagda uppgifter (inklusive uppgifter om skyddsåtgärder) som denne får kännedom om i sin roll som systemadministratör. 8.3, p. 1 (62)
2. En systemadministratör ska informera universitetets IT-säkerhetsgrupp vid misstanke om säkerhetsbrister eller misstanke om inträffad informationssäkerhetsincident. Vid misstanke om oegentligheter ska dessa dessutom hanteras i enlighet med *LiU:s riktlinjer för hantering av misstänkta oegentligheter, missförhållanden och brott*. Informationsskyldigheten gäller upptäckter som görs inom hela universitetets IT-miljö. 8.3, p. 2 (63)
3. En systemadministratör som får kännedom om en misstänkt personuppgiftsincident ska rapportera enligt gällande rutin. Se *Personuppgiftsincident*[33]. 8.3, p. 3 (64)
4. En systemadministratör som får kännedom om att IT-resurser används i strid med gällande regelverk ska påtala detta för berörda personer. Vid upprepade eller allvarliga förseelser, t.ex. misstänkta lagbrott, ska universitetets IT-säkerhetsgrupp informeras. 8.3, p. 4 (65)
5. En systemadministratör ska ha god kännedom om dessa riktlinjer för informationssäkerhet i sin helhet. 8.3, p. 5 (66)

[33] https://go.liu.se/pui

8.4 Särskilda rättigheter för systemadministratörer

Vid LiU gäller följande särskilda rättigheter för systemadministratörer:

1. En systemadministratör har rätt att övervaka användningen av system samt ta del av nätverkstrafik i syfte att hantera den löpande driften. Användares personliga integritet ska värnas så långt det är möjligt. Systemadministratören ska därför vidta de åtgärder som är möjliga för att minimera risken att se enskilda användares data. 8.4, p. 1 (67)
2. Åtkomst till studenters lagrade data (t.ex. på fillager, OneDrive eller i e-post) får endast ske som led i rent teknisk bearbetning eller efter medgivande från berörd individ, eller efter godkännande av IT-säkerhetsgruppen. Om systemadministratör som led i teknisk bearbetning uppmärksammar allvarlig överträdelse av LiU:s regelverk eller lagbrott, ska detta rapporteras enligt 8.3. 8.4, p. 2 (68)
3. En systemadministratör har rätt att vidta åtgärder i de system vederbörande ansvarar för i syfte att säkerställa en tillförlitlig funktion och tillräcklig säkerhet. Exempel på sådana åtgärder kan vara att rensa lagrade data, avbryta körande program, eller avsluta pågående sessioner. Berörda användare ska informeras om åtgärderna, om möjligt i förväg. 8.4, p. 3 (236)
4. En systemadministratör har rätt att vid akuta driftsituationer utan förvarning tillfälligt begränsa tillgången till IT-resurser. 8.4, p. 4 (70)

8.5 Befogenheter för LiU:s IT-säkerhetsgrupp

IT-säkerhetsgruppen ansvarar för LiU:s operativa IT-säkerhetsarbete. IT-säkerhetsgruppens uppdrag ska definieras årligen i särskilt uppdrag från universitetsdirektören. Medarbetare i IT-säkerhetsgruppen ska ha undertecknat blanketten för systemadministratörer.

Vid LiU gäller följande riktlinjer för befogenheter för LiU:s IT-säkerhetsgrupp:

1. IT-säkerhetsgruppen har rätt att utvärdera och testa säkerheten i universitetets IT-miljö. 8.5, p. 1 (71)
2. IT-säkerhetsgruppen har rätt att övervaka system och datornät, inklusive ta del av nätverkstrafik och lagrade data, för att säkerställa en godtagbar säkerhetsnivå i LiU:s IT-system och för att förebygga, upptäcka och hantera misstänkta informationssäkerhetsincidenter och brott mot LiU:s regelverk. 8.5, p. 2 (72)
3. IT-säkerhetsgruppen har rätt att vid behov vidta åtgärder för att säkerställa efterlevnad av universitetets regelverk samt för att förebygga och hantera informationssäkerhetsincidenter. Sådana åtgärder kan exempelvis innefatta begränsning av tillgång till datornät eller andra IT-resurser, radera enskilda e-postmeddelanden eller filer, samt omhänderta och undersöka utrustning som ägs av universitetet. 8.5, p. 3 (73)

8.6 Riskägare

Nedan anges riskägare för riktlinjer i detta kapitel.

8.2, p. 1	Informationssäkerhetssamordnaren	8.4, p. 2	Informationssäkerhetssamordnaren
8.3, p. 1	Rektor	8.4, p. 3	Systemägaren
8.3, p. 2	Informationssäkerhetssamordnaren	8.4, p. 4	Systemägaren
8.3, p. 3	Rektor	8.5, p. 1	Rektor
8.3, p. 4	Informationssäkerhetssamordnaren	8.5, p. 2	Rektor
8.3, p. 5	Informationssäkerhetssamordnaren	8.5, p. 3	Rektor
8.4, p. 1	Informationssäkerhetssamordnaren		

9 Ikraftträdande

1. Dessa riktlinjer träder i kraft 30 oktober 2023.

2. Beträffande de riktlinjer som anges nedan tillämpas de första gången från och med den 1 maj 2024:

Kapitel 5

Avsnitt 5.3, p. 1 (inventering av befintliga tillgångar ska vara färdigställd senast den 1 maj 2024).

Kapitel 6

Avsnitt 6.2, p. 1 (systemägare ska ha utsetts senast den 1 maj 2024)

Avsnitt 6.3, p. 6.

Kapitel 7

Avsnitt 7.2 (dokumentation ska vara upprättad senast den 1 maj 2024)

Avsnitt 7.3, 7.7, p. 6 samt 7.7, p. 9.

Ordlista

AD	Active Directory. Katalogtjänst från Microsoft som innehåller bland annat användarkonton.
ADFS	Active Directory Federation Services. Möjliggör single-sign-on (inloggning en gång med en identifiering) till ett flertal IT-tjänster.
Angrepp	Ett försök att förstöra, exponera, förändra, inaktivera, stjäla eller skaffa sig obehörig åtkomst till en tillgång eller använda den på ett obehörigt sätt.
Användare	Individ, system eller tjänst som nyttjar informationstillgångar. Ofta avses en individ som direkt interagerar med ett datoriserat system. Här förutsätts som regel att användaren har behörighet att använda informationstillgångarna.
Behörighet	Tilldelade rättigheter att använda en informationstillgång på ett specificerat sätt.
Betrodd certifikatutgivare	Utgivare av certifikat som IT-säkerhetsgruppen definierat som betrodd, vilket normalt innefattar utgivare betrodda av operativsystem och webbläsare.
Brandvägg	Nätverkskomponent som begränsar och övervakar trafik mellan två nät och hindrar obehörig nätverkstrafik att passera.
Dataskydd	Begrepp som används för att benämna skyddet för personuppgifter i de regelverk och rutiner som tillämpas vid behandling av personuppgifter.
Höga behörigheter	Höga behörigheter innebär fullständiga eller nära fullständiga behörigheter till IT-system.
Icke reversibel	Process som bara går att utföra i en riktning. Typiskt sett uppnås detta i sammanhanget med en kryptografisk hashsumma som givet en klartext genererar en text som till synes är helt slumpmässig. Processen går att upprepa men det är (idealiskt sett) omöjligt att återskapa klartext ifrån hashsumman.

Indirekt identifiering	Identifiering av vilken person en samling uppgifter avser genom att använda flera värden som var och en för sig inte kan identifiera personen (t.ex. adress och ålder i kombination).
Informationssäkerhet	Bevarande av informationens konfidentialitet, riktighet och tillgänglighet. Arbetet med informationssäkerhet omfattar att införa och förvalta administrativa regelverk såsom policys och riktlinjer, tekniskt och fysiskt skydd (cybersäkerhet och skalskydd).
Informationstillgång	Information som insamlats eller upprättats för ett specifikt syfte samt de resurser som används för att hantera informationen, t.ex. programvaror, servrar, IT-system, tjänster och förvaringsutrymmen.
Informationsägare	Den som har mandat att styra över en viss informationstillgång. Informationsägaren har ett antal rättigheter och skyldigheter genom dessa riktlinjer. Utses av prefekt/motsvarande.
Konfidentialitet	Skydd mot obehörig insyn. ISO 27000:2017 definierar konfidentialitet som ”egenskapen att information inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer”.
LDAP	Lightweight Directory Access Protocol. Ett protokoll för kommunikation med katalogservrar, t.ex. med AD.
LiU CA	LiU Certificate Authority. Gruppering vid LiU som samordnar hantering av TLS-certifikat upphandlade av Sunet TCS.
Logisk separation	Placering av IT-utrustning på separata nätverkssegment, t.ex. genom användning av virtuella lokala nätverk (VLAN).
Molntjänst	IT-tjänst som tillhandahålls över internet av en extern leverantör.
Multifaktorautentisering	Se tvåstegsverifiering.
Objektägare	Ansvarig för ett informationsbehandlande system. Se Förvaltningsmodell för informationsbehandlande system vid Linköpings universitet (LiU-2012-00330). Se även informationsägare.

PGP	En metod för kryptering och signering av e-post m.m.
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.
Riktighet	Egenskapen att en information inte obehörigen förändras.
S/MIME	En standard för kryptering och signering av e-post.
SSL	Secure Sockets Layer. Äldre protokoll för att kryptera och signera datatrafik. Ersatt av TLS.
Sekretess	Ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. (3 kap. 1 § OSL)
Sunet	Svensk operatör av datornät för forskning och utveckling.
Sunet TCS	Sunet Trusted Certificate Service. Leverantör av TLS-certifikat till LiU CA.
Systemadministratör	Person som har behörighet i IT-system utöver vad som normalt tilldelas. Exempelvis person med administrativ behörighet till operativsystem eller programvara.
Särskilt skyddsvärd information	Information klassad med **höjd konfidentialitet**, **extrem konfidentialitet**, **höjd riktighet**, eller **höjd tillgänglighet**.
TLS	Transport Layer Security. Ett protokoll för att kryptera och signera datatrafik som ersätter det äldre protokollet SSL.
Tillförlitlig kryptering och signering	Publicerad metod för kryptering och/eller digital signering som används som avsett och som saknar kända säkerhetsbrister.
Tillgänglighet	Åtkomst för behörig person vid rätt tillfälle. ISO 27000:2017 definierar tillgänglighet som ”egenskapen att vara åtkomlig och användbar på begäran från ett behörigt objekt”.
Tvåstegsverifiering	Kallas också **tvåfaktorsautentisering**. Detta är en typ av **multifaktorautentisering (MFA)**. Identifiering med två olika metoder, t.ex. lösenord

	i kombination med engångskod eller PIN-kod i kombination med smartkort.
VLAN	Virtual LAN. Virtuellt datornät för att uppnå separation av nätverksansluten utrustning.
VPN	Virtual private network. Metod som vanligen används för att etablera en skyddad nätverksförbindelse via ett oskyddat nätverk.