# 1 Klassificering av information och IT-utrustning vid LiU

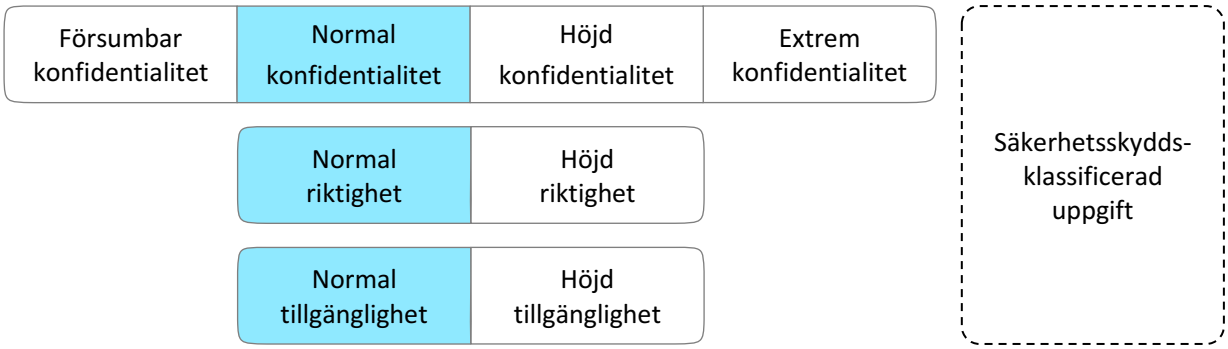
## 1.1 Informationsklassning

Information vid LiU klassificeras enligt tre dimensioner: **konfidentialitet**, **riktighet** och **tillgänglighet**. Som en helt separat klass finns även kategorin **säkerhetsskyddsklassificerad uppgift**.

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 (till exempel hur en viss IT-tjänst får användas).

För dimensionerna riktighet och tillgänglighet finns nivåerna **normal** och **höjd**. För konfidentialitet finns fyra nivåer: **försumbar**, **normal**, **höjd**, och **extrem**.

Det är viktigt att tillämpa klassningsmodellen med omsorg. En för låg klassning innebär att LiU utsätts för oacceptabla risker. En för hög klassning kan däremot leda till onödig administrativ börda och högre kostnader.




*Figur 1: Informationsklassningsmodell vid LiU.*
*Exempel på klassning för en informationstillgång med normal konfidentialitet, riktighet och tillgänglighet.*

### 1.1.1 Säkerhetsskyddsklassificerad uppgift

Säkerhetsskyddsklassificerade uppgifter avser uppgifter som rör säkerhetskänslig verksamhet enligt säkerhetsskyddsförordningen (SFS 2018:658). Uppgift som tidigare bedömts vara ”hemlig uppgift” enligt SFS 1996:633 ska vid LiU behandlas som säkerhetsskyddsklassificerad uppgift.

Säkerhetsskyddsklassificerade uppgifter får under inga omständigheter lagras, bearbetas eller kommuniceras i LiU:s IT-utrustning, system och nätverk, inkluderande alla typer av interna lösningar och externa molntjänster. Varken hårdvara, mjukvara, nätverk eller personal är klassade för detta.

Eventuell förekomst av säkerhetsskyddsklassificerade uppgifter ska heller inte inventeras eller förtecknas enligt 5.1. Istället ska förekomsten meddelas säkerhetsskyddschefen eller den tjänsteman som denne delegerat uppgiften till. Sådant meddelande ska överföras muntligen vid fysiskt möte.

### 1.1.2 Extrem nivå (konfidentialitet)

**Extrem** nivå tillämpas vid förekomst av stora mängder uppgifter som var och en och 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).

Exempel

- Journalsystem (samling av känsliga personuppgifter).
- Hemadress till person i utsatt ställning (risk för liv och hälsa).
- Information om enskilda dissidenter i totalitära regimer (mål för underrättelseverksamhet).

### 1.1.3 Höjd nivå (konfidentialitet, riktighet och tillgänglighet)

För dimensionerna konfidentialitet, riktighet och tillgänglighet ska **höjd** nivå tillämpas om allvarlig skada kan drabba LiU, samarbetspartner eller enskild individ om **konfidentialitet** 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 offentlighets- och sekretesslagen samt för känsliga personuppgifter (se 1.2.1). Se LiU:s vägledning om offentlighet och sekretess för stöd vid bedömning av sekretess och konfidentialitet[2].

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

[2] Finns länkad från https://insidan.liu.se/juridisk-radgivning/offentlighet-sekretess/

Exempel

- Information om personliga förhållanden som framkommer vid besök hos kurator, psykolog, eller studievägledning (höjd konfidentialitet).
- Affärshemligheter i forskningsprojekt (höjd konfidentialitet).
- Lärplattform (höjd tillgänglighet).
- Register över studieresultat (höjd riktighet).

### 1.1.4 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

- Lista med namn eller personnummer på studenter.
- Lisa med anställdas privata bostadsadresser och telefonnummer.
- Handling som omfattas av svag sekretess (sekretess med rakt skaderekvisit).

### 1.1.5 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 1.2.3). 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

- Presentation av LiU som lärosäte.
- Publicerade vetenskapliga artiklar.
- Manuskript under bearbetande (om författaren önskar).

## 1.2 Personuppgifter

En personuppgift är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. För att klassa konfidentialitet i rätt perspektiv är det avgörande att kunna bedöma olika typer av personuppgifter. Skyddsnivån som krävs för personuppgifter styrs till stor del av hur känsliga de är och vilken risk de utgör för den person de rör.

### 1.2.1 Känsliga personuppgifter

**Känsliga personuppgifter** är enligt dataskyddsförordningen[3] uppgifter om:

[3] Europaparlamentets och rådets förordning (EU) 2016/679 (”GDPR” eller ”dataskyddsförordningen”)

- ras eller etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening,
- hälsa,
- en fysisk persons sexualliv eller sexuella läggning samt
- 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 så gott som alltid med minst **höjd konfidentialitet** och större samlingar av icke pseudonymiserade känsliga personuppgifter klassas typiskt med **extrem konfidentialitet**.

Uppgifter om barn förtjänar särskilt skydd, och det kan i många fall vara motiverat att betrakta dem som känsliga personuppgifter, och därmed klassa dem med **höjd konfidentialitet**.

### 1.2.2 Normala personuppgifter

Personuppgift som inte är känslig, inklusive personnummer, refereras fortsättningsvis till som **normala personuppgifter**. Även om personnummer enligt lag anses vara särskild skyddsvärt anses personnummer vara en normal personuppgift.

### 1.2.3 Harmlösa personuppgifter

Begreppet **harmlösa personuppgifter**, som används i vissa riktlinjer och beslut, omfattar normala personuppgifter som beroende på 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 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 utifrån med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt

riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter[4].

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 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.

### 1.2.4 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. Ingår känsliga personuppgifter, till exempel 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 1.3).

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 konfidentialitet klassas enligt de kriterier som skulle berört den ursprungliga datamängden om pseudonymisering inte hade använts som skyddsåtgärd.

### 1.2.5 Anonymiserade uppgifter

Om identifierande uppgifter helt elimineras från en datamängd med personuppgifter så att uppgifterna inte 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.

[4] Dataskyddsförordningen, artikel 24.1.

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.

## 1.3 Flödesschema för informationsklassning

Nedanstående flödesschema 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 så som den definieras i SFS 1996:633
[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)

## 1.4 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 klassningar.

## 1.5 Klassificering av IT-utrustning i skyddsnivåer

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 klassificeras även den IT-utrustning som medarbetare vid LiU använder i skyddsnivåer.

Klassificeringen bygger på färgerna **guld, silver, brons, vit** och **svart**. För normala IT-klienter (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 IT-avdelningen. Högsta skydd aktiverat. |
| **Silver** | Som **guld** men med möjlighet för innehavaren att tillfälligt administrera datorn själv. |
| **Brons** | Möjlighet för innehavaren att inaktivera ytterligare skyddsåtgärder. Användaren kan själv ha administrativa behörigheter till datorn med ordinarie inloggning. |
| **Vit** | Enhet som inventeras, men inte hanteras eller underhålls, av IT-avdelningen. 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 IT-avdelningen, exempelvis privatägd dator. |

# 2 Riktlinjer för anställda och uppdragstagare

I detta kapitel fastställs riktlinjer för anställda, konsulter och andra uppdragstagare vid LiU. Studenter vid LiU omfattas normalt inte av dessa riktlinjer; för dessa gäller Regler för studenters användning av IT-resurser vid Linköpings universitet (LiU-2018-01846).

Riktlinjerna är obligatoriska att känna till och följa. Eventuella avsteg får endast göras efter skriftligt beslut av informationssäkerhetssamordnaren.

## 2.1 Användning av IT-resurser och informationstillgångar

2.1.1 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 på https://styrdokument.liu.se.

2.1.2 Det är inte tillåtet att i användningen förtala, förolämpa, förnedra eller kränka andra.

2.1.3 Användare av LiU:s IT-resurser är skyldiga att följa anvisningar från IT-direktören, IT-säkerhetsgruppen och systemadministratör med ansvar för respektive resurs.

2.1.4 Det är inte tillåtet att utan uttryckligt, skriftligt medgivande från objektägare försöka höja sina behörigheter 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.

2.1.5 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.

2.1.6 LiU:s IT-resurser får inte användas till affärsverksamhet.

2.1.7 När LiU:s IT-utrustning används, transporteras eller förvaras utanför tjänstemiljön ska innehavaren vidta lämpliga åtgärder för att skydda densamma. Observera särskilt Riktlinjer för säkert resande (LiU-2018-00399).

2.1.8 Anställda och motsvarande uppdragstagare[5] 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 information 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[6].

2.1.9 Vid ny personuppgiftsbehandling ska riktlinjer enligt 5.5 samt Riktlinjer för behandling av personuppgifter (LIU-2018-01540) följas.

## 2.2 Användarkonton och lösenord

2.2.1 Behörigheter till IT-resurser är personliga och får inte upplåtas till någon annan annat än under direkt överinseende.

2.2.2 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 IT-avdelningens kundcenter kontaktas.

2.2.3 Det är inte tillåtet att begära att någon annan ska uppge sitt lösenord.

2.2.4 Det är inte tillåtet att använda någon annans inloggningsuppgifter oavsett om denne själv har lämnat ut inloggningsuppgifterna eller inte.

2.2.5 Ett särskilt lösenord ska användas för åtkomst till LiU:s IT-resurser. Det är inte tillåtet att använda detta lösenord för någon extern tjänst.

2.2.6 Vid registrering av e-postadress eller skapande av konto i externa tjänster för universitetets räkning ska e-postadress i universitets e-postsystem anges. Se även 2.5.2.

2.2.7 Lösenord ska väljas så att de är svårgissade[7].

2.2.8 Lösenord ska omgående bytas när det finns misstanke om att de blivit kända av annan än användaren själv.

---

[5] Uppdragstagare avser alla med beslutskonto i LiUs IT-system och uppdrag vid LiU, exempelvis konsulter, gästforskare, adjungerade, emeriti, praktikanter, och arvodister.
[6] 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 (dnr LiU-2017-03903).
[7] Använd gärna en lösenordsfras bestående av minst fem slumpmässigt valda ord. Läs mer på https://insidan.liu.se/it/it-sakerhet/tips-for-ett-sakert-losenord.

2.2.9 Det är tillåtet att använda en lösenordshanterare för lagring av personliga lösenord. Se särskilda rekommendationer från IT-avdelningen.[8]

## 2.3 Grundläggande IT- och informationssäkerhet

2.3.1 Lagring av filer ska normalt ske på LiU-gemensam lagringsserver (fillager eller Onedrive for business). Lagring enbart på lokal hårddisk bör undvikas. För lagring av information klassad med **extrem konfidentialitet** eller **höjd riktighet** se nedan (2.3.2).

2.3.2 Lagring av information klassad med **extrem konfidentialitet** eller **höjd riktighet** ska ske på IT-avdelningens tjänst för säker lagring eller annan lagringstjänst anvisad av informationssäkerhetssamordnaren. Om informationsägaren har utfärdat särskild anvisning för lagringen ska denna i stället följas.

2.3.3 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.

2.3.4 Pappersdokument som slängs ska destrueras med dokumentförstörare av säkerhetsklass 4 eller högre om dokumentet innehåller **särskilt skyddsvärd** information.

2.3.5 När lagringsmedia som innehållit **särskilt skyddsvärd** information inte längre ska användas för sitt ändamål ska detta lämnas till IT-avdelningen för destruktion, eller så ska lagringsmediets innehåll raderas på ett sådant sätt att informationen inte kan återskapas.

2.3.6 Sekretessfilter[9] bör användas på bildskärm vid hantering av information klassad med **höjd konfidentialitet** eller högre i miljöer där många inte har behörighet att ta del av informationen, till exempel på stationer, i kollektivtrafik, i föreläsningssalar, eller på möten.

2.3.7 Användare av datorer ansvarar för att låsa datorn när vederbörande lämnar den utan uppsikt. Undvik att lämna datorer eller andra enheter obevakade där stöldrisken inte är försumbar.

2.3.8 Användare av mobila enheter ansvarar för att skydda enheten med skärmlås (till exempel sexställig PIN-kod, lösenord eller fingeravtryck).

2.3.9 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.

---

[8] https://insidan.liu.se/informationssakerhet/rekommendation-om-losenordshanterare
[9] Sekretessfilter minskar betraktningsvinkeln för bildskärmen, vilket gör det svårare för andra än den som är direkt bakom att se vad som visas.

2.3.10 Ej betrodda tillbehör ska inte anslutas till LiU:s datorer.[10]

2.3.11 Användare som upptäcker säkerhetsbrist i informationssystem eller IT-tjänst som LiU använder eller ansvarar för ska omgående rapportera detta till LiU:s IT-säkerhetsgrupp på e-postadress infosec@liu.se.

## 2.4 Molntjänster

2.4.1 Användning av molntjänst där extern part är huvudman och styr ändamål och medel med behandlingen är tillåten under förutsättning att gällande lagstiftning följs.

2.4.2 För användning av molntjänst där LiU är huvudman gäller att information som är klassad med **försumbar konfidentialitet**, **normal riktighet** och **normal tillgänglighet** får hanteras i molntjänst om informationsägaren beslutar så (enligt avsnitt 5.3). Informationsägaren är ansvarig för att säkerställa efterlevnad av gällande lagstiftning, särskilt kring personuppgiftsbehandling, offentlighet och sekretess samt arkivering. Beslut om att använda en molntjänst ska rapporteras till IT-säkerhetsgruppen.

2.4.3 För annan information än vad som avses i avsnitt 2.4.1 och 2.4.2 beslutar IT-direktören vilka molntjänster som får användas vid LiU. Den aktuella listan över godkända molntjänster finns publicerad på https://insidan.liu.se/it/godkanda-molntjanster. Användning av andra molntjänster får ske endast efter särskilt beslut om detta av IT-direktören. **Särskilt skyddsvärd** information ska inte hanteras i molntjänster om inte informationsägaren gett särskild anvisning som tillåter sådan hantering.

## 2.5 E-post

2.5.1 Inkommande e-post ska läsas regelbundet och alltid hanteras i enlighet med gällande lagstiftning kring offentlighet och sekretess. Observera LiU:s anvisningar[11] rörande dokumenthantering.

2.5.2 All e-postkorrespondens som sker i tjänsten ska hanteras i det e-postsystem som anvisas av IT-direktören och med e-postadress som har formen *förnamn.efternamn*@liu.se eller *funktionsadress*@[*domän*.]liu.se. Privat utrustning får ansluta till e-postsystement endast genom LiU:s webbmail. Se även 2.9.1.

2.5.3 Det är inte tillåtet att automatiskt vidarebefordra e-post till externa e-postleverantörer. Det är heller inte tillåtet att skicka e-post med avsändaradress som slutar på liu.se från externa e-postleverantörer.

[10] Till exempel utrustning som utomstående ber att få ansluta, såsom USB-minnen eller utrustning för skärmavbildning.
[11] https://insidan.liu.se/dokumenthantering

2.5.4 **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 att aktuellt ärende är avslutat.

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.

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.

## 2.6 Massutskick via e-post

Med massutskick menas här e-post som skickas till ett större antal mottagare där flera av mottagarna inte känner avsändaren och som passerar LiU:s e-postsystem. Riktlinjerna gäller även andra e-postutskick om en adress som slutar på liu.se används som avsändare.

E-postlistor som mottagarna själva har gått med i och som de har möjlighet att själva lämna omfattas inte av dessa regler. Detsamma gäller institutionsspecifika listor som får ha andra regler.

LiU:s IT-avdelning kan komma att stoppa utskick som bryter mot dessa regler eller gällande praxis. IT-avdelningen kan också stoppa framtida utskick från källor som tidigare brutit mot dessa regler. Sådant beslut kan omprövas av IT-direktören. Tekniska begränsningar och skräppostfilter kan automatiskt komma att hindra utskick som inte i förväg förankrats med IT-avdelningen.

2.6.1 Massutskick ska göras på ett sådant sätt att mottagarna inte kan se varandras e-postadresser.

2.6.2 Följande typer av massutskick är inte tillåtna:

- Reklam, inklusive festinbjudningar samt platsannonser och annan information från företag.
- Kedjebrev. Med kedjebrev avses brev med uppmaning att skicka brevet vidare.

2.6.3 Massutskick ska ske med stor återhållsamhet. Detta innebär att åtgärder ska vidtas för att säkerställa att informationen verkligen är relevant för mottagarna. Upprepade utskick om samma fråga bör undvikas. Vid osäkerhet om ett utskick är lämpligt kan IT-säkerhetsgruppen ge vägledning om rådande praxis.

Utskick ska ha en tydlig avsändare. Meddelanden ska vara läsbara med verktyg för synnedsättning. Meddelanden bör inte innehålla bilagor; om dokument ändå måste bifogas bör PDF-format användas.

2.6.4 Massutskick med övergripande studieinformation eller annan verksamhetsrelaterad information från LiU till dess studenter och medarbetare är normalt tillåtet.

2.6.5 Enkäter är tillåtna endast i följande fall:

- Enkäten genomförs inom ramen för ett LiU-gemensamt uppdrag eller projekt.
- Enkäten gäller forskningsprojekt som genomförs av forskare vid LiU.

Mottagare av utskick om enkäter ska ha möjlighet att avböja framtida utskick, inklusive eventuella påminnelser, utan att svara på några frågor. Enkäter bör göras i LiU:s enkätverktyg[12].

2.6.6 Kursrelaterade frågor är tillåtna på kurslistor. Kursansvarig kan för sina kurslistor också besluta om att godkänna utskick av kursrelaterade enkäter. Observera att kurspersonal inte automatiskt blir medlemmar på kurslistor.

2.6.7 Massutskick från studentkårerna till sina medlemmar är tillåtna.

2.6.8 Sektion- och kårstyrelse får använda programlistor för information om sin verksamhet med undantag av utskick som bryter mot 2.6.1.

2.6.9 Den som anser att ett e-postmeddelande bryter mot dessa regler kan ställa klagomål till IT-säkerhetsgruppen på e-postadress infosec@liu.se. För att kunna hantera klagomålet bör e-postmeddelandet i sin helhet, inklusive fullständigt brevhuvud (rubrikrader), bifogas.

[12] https://insidan.liu.se/it/survey

## 2.7 Stöld och förlust av IT-utrustning

2.7.1 Stöld eller annan förlust av dator, surfplatta, mobiltelefon eller annan IT-utrustning ska polisanmälas av berörd medarbetare. Förlusten ska även anmälas till IT-avdelningen tillsammans med eventuellt ärendenummer från Polisen. IT-avdelningen kommer i sin tur att meddela universitetets säkerhetschef[13] och i förekommande fall rapportera förlusten som en personuppgiftsincident.

## 2.8 Avyttring av IT-utrustning

2.8.1 Avyttring av datorer, telefoner, surfplattor och andra enheter samt lagringsmedia görs normalt inte av slutanvändare. Om så ändå sker ska riktlinjer i kapitel 5.2 i detta dokument beaktas.

## 2.9 Användning av privat utrustning

2.9.1 **Särskilt skyddsvärd information** får inte hanteras på privat utrustning. Detta inkluderar nyckel för dekryptering av e-post krypterad med exempelvis S/MIME eller PGP.

2.9.2 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 ett uppdaterat skydd mot skadlig programvara (antivirusskydd).

2.9.3 Privat utrustning ansluten till LiU:s datornät kan komma att sårbarhetsscannas av LiU:s IT-säkerhetsgrupp. Utrustning där sårbarheter upptäcks utgör en informationssäkerhetsrisk och kan komma att blockeras. Det är inte tillåtet att försöka kringgå sådan blockering.

## 2.10 Övervakning av IT-resurser och åtgärder vid regelbrott

2.10.1 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.

[13] I enlighet med riktlinjerna för hantering av misstänkta oegentligheter och brott (dnr LiU-2019-03689).

2.10.2 Vid brott mot riktlinjer eller andra användarinstruktioner kan användares tillgång till IT-resurser komma att begränsas. Sådan begränsning kan också ske för att hindra pågående IT-angrepp (exempelvis dataintrång eller skadlig kod).

2.10.3 Brott mot dessa riktlinjer kan komma att överlämnas till prefekt/motsvarande eller hanteras enligt LiU:s riktlinjer för hantering av misstänkta oegentligheter och brott (LiU-2019-03689). Misstänkta lagbrott kan komma att polisanmälas.

2.10.4 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 LiU:s IT-säkerhetsgrupp. Granskningen kan komma att inkludera all data som lagras på utrustningen eller i LiU:s IT-system.