RB 2018-15,5 exp. 2018-06-12 /AA

LINKÖPINGS UNIVERSITET

2018-06-11
DNR LiU-2018-01814
BESLUT
1(2)

Beslut om riktlinjer för informationssäkerhet

Beslut

Linköpings universitet (LiU) beslutar att fastställa bilagda riktlinjer för informationssäkerhet. Detta beslut ersätter ”Informationssäkerhetpolicy” (LiU-2010-01689), ”Ledningssystem för Informationssäkerhet (LIS) vid Linköpings universitet” (LiU-2010-01529) samt "Regler för systemadministratörer vid Linköpings universitet” (LiU-2015-01619). Beslutet ska publiceras i LiU:s regelsamling.

Skäl till beslut

Myndigheten för samhällsskydd och beredskap (MSB) föreskriver i MSBFS 2016:1 att varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet (MSBFS 2016:1 5§). Myndigheten ska upprätta en informationssäkerhetspolicy, andra styrande dokument samt den dokumentation som i övrigt krävs för att kunna bedriva ett ändamålsenligt arbete med myndighetens informationssäkerhet. (MSBFS 2016:1 7§).

Handläggningen av beslutet

Detta beslut har fattats vid rektors beslutsmöte i närvaro av universitetsdirektör Kent Waltersson, chefsjurist Christina Helmér, studeranderepresentant Jacob Larsson och rektors sekreterare Aneth Andersson efter föredragning av IT-direktör Joakim Nejdeby. I ärendets handläggning har deltagit systemingenjör Johannes Hassmund och Enhetschef David Byers. Förslaget har även granskats av institutionerna, fakulteterna och Universitetsförvaltningen inklusive Juristenheten.

Helen Dannetun

Joakim Nejdeby

Kopia till:
Universitetsledningen
Dekaner
Kanslichefer
Prefekter
Adm chefer
UDL
Internrevisionen
Fackliga företrädare
LiU-Nytt
Regelsamlingen

Riktlinjer för informationssäkerhet vid Linköpings universitet

Innehåll

Inledning

I detta dokument fastställs riktlinjer för informationssäkerhet vid Linköpings universitet (LiU). Riktlinjerna är en del av LiU:s ledningssystem för informationssäkerhet. Efter en översyn som pågår under hela 2018 kommer ledningssystemet förutom dessa riktlinjer bestå av en informationssäkerhetspolicy som beskriver universitetsstyrelsens övergripande viljeinriktning för arbete med informationssäkerhet vid LiU samt en dokumentation över arbetsprocesserna inom ledningssystemet.

Riktlinjerna är framarbetade av LiU:s IT-säkerhetsgrupp baserat på verksamhetens behov och förutsättningar, lagkrav, gruppens omvärldsanalys, generella riskanalyser av LiU:s informationstillgångar samt analys av inträffade incidenter. Riktlinjerna ses över med ett intervall om ett till två år.

Ordet riktlinje ska tolkas i en strikt bemärkelse. Såvida inte annat framgår utgör riktlinjerna obligatoriska regler för hantering av LiU:s information. Vissa riktlinjer i kapitlen 5 och 6 kan dock undantas efter särskild analys vars former beskrivs i inledningen till kapitel 5. Avsteg i övrigt kräver särskilt godkännande som regleras i respektive kapitel.

Läsanvisningar

Definitioner

I dessa riktlinjer används orden ska och bör med följande betydelser:

ska	Indikerar ett nödvändigt krav för att uppfylla riktlinjen.
bör	Utgör en stark rekommendation som kompletterar riktlinjen.

Ordlista med huvudsakligen tekniska termer återfinns i slutet av dokumentet.

Relevant för samtliga läsare

Kapitel 1 innehåller beskrivning av LiU:s modell för informationsklassning och klassificering av IT-utrustning. Det är svårt att få en fullgod förståelse för riktlinjerna utan att läsa detta kapitel.

Kapitel 2 innehåller riktlinjer för informationssäkerhet som riktar sig till alla **anställda, konsulter och andra uppdragstagare** vid LiU. Kapitlet är tänkt att kunna läsas fristående från övriga delar. Riktlinjerna är obligatoriska.

Kontoadministratörer och prefekter/motsvarande

Kapitel 3 innehåller riktlinjer för informationssäkerhet som riktar sig till **kontoadministratörer** och **prefekter/motsvarande** vid LiU. Kontoadministratör kallas den person som har behörighet att skapa, stänga och bistå vid återställning av lösenord till användarkonton i LiU:s IT-miljö. Riktlinjerna är obligatoriska.

Systemadministratörer och IT-säkerhetsgruppen

Kapitel 4 innehåller riktlinjer för informationssäkerhet som riktar sig till den som arbetar som **systemadministratör**. Med systemadministratör menas här individ som har högre behörigheter än vanliga användare i ett IT-system och som har undertecknat särskild ansvarsförbindelse för systemadministratörer. Riktlinjerna är obligatoriska för den som har rollen som systemadministratör. I kapitlet fastställs också särskilda befogenheter för systemadministratör som arbetar i **LiU:s IT-säkerhetsgrupp**.

Informationsägare

Kapitel 5 innehåller generella riktlinjer för hantering av LiU:s informationstillgångar. Målgruppen för detta kapitel är främst **informationsägare**, det är dennes ansvar att säkerställa att riktlinjerna efterlevs. Informationsägare är den som har mandat att styra över eller besluta om att avveckla en viss informationstillgång. Exempel på informationsägare kan vara objektägare eller ansvarig för ett forskningsprojekt. Om informationsägaren inte hanterar särskilt skyddsvärd information räcker det med att läsa och säkerställa efterlevnad av **stycke 5.1-5.5**.

Kapitel 6 innehåller riktlinjer för informationssäkerhet för IT-system som hanterar information vid LiU. Informationsägare kan förutsätta att bastjänster[1] från IT-avdelningen uppfyller riktlinjerna. Om informationsägare anskaffar eller nyttjar andra IT-tjänster ska denne säkerställa att riktlinjerna efterlevs. Riktlinjerna i detta kapitel är uteslutande av teknisk karaktär och det faller i normalfallet på en leverantör av IT att implementera åtgärderna.

Det finns vissa möjligheter att göra avsteg från riktlinjerna i kapitel 5 och 6, former för detta regleras i inledningen till kapitel 5.

Objektägare

Utöver kapitel 5 och 6 berörs informationsägare som också är **objektägare** enligt LiU:s förvaltningsmodell för informationsbehandlande system vid Linköpings universitet (LiU-2012-00330) även av riktlinje 4.1.1 i **kapitel 4.**

[1] Till exempel klienter på skyddsnivå guld och silver (se kapitel 1), Office 365 inklusive e-post, Lisam samt IT-avdelningens lagringstjänster.
Se https://insidan.liu.se/informationssakerhet.

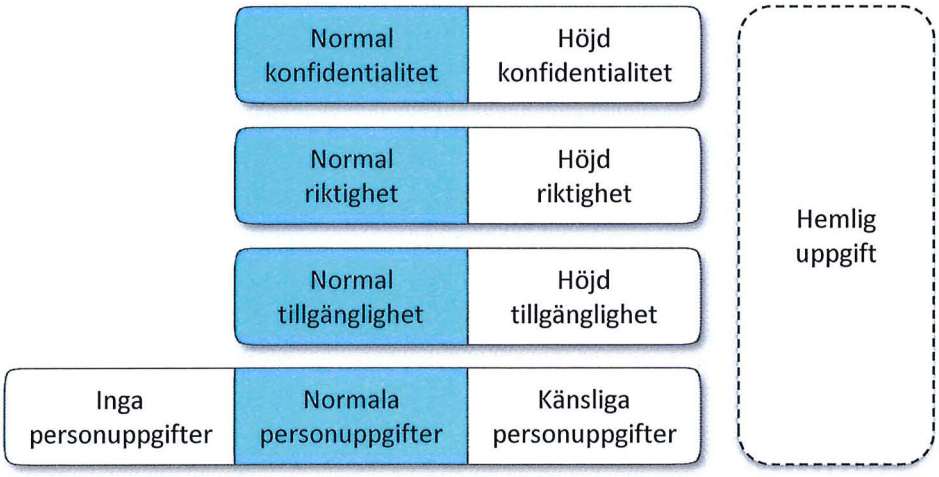
1 Klassificering av information och IT-utrustning vid LiU

1.1 Informationsklassning

Information vid LiU klassificeras enligt fyra dimensioner. Utöver de tre perspektiven **konfidentialitet**, **riktighet** och **tillgänglighet** används här även **personuppgifter** som en egen dimension. Som en helt separat klass finns även kategorin **hemlig uppgift**. Personuppgifter har fått en särställning eftersom en ansvarsfull hantering av personuppgifter är en viktig komponent för samhällets förtroende för LiU som myndighet; vidare är känsliga personuppgifter vanligt förekommande i många delar av LiU:s verksamheter.

Syftet med informationsklassning är att underlätta val av relevanta tekniska och administrativa skyddsåtgärder för LiU:s information. För att uppnå ett effektivt och lätt tillämpat ledningssystem förekommer endast två nivåer i dimensionerna konfidentialitet, integritet och riktighet: **normal** eller **höjd**. För personuppgifter är nivåerna: **ingen personuppgift**, **normala personuppgifter** och **känsliga personuppgifter**.

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 teknikkostnader.



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

1.1.1 Hemlig uppgift

Hemliga uppgifter och hemliga handlingar enligt säkerhetsskyddsförordningen (SFS 1996:633), i den mån de förekommer, 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 hemlig uppgift ska heller inte inventeras eller förtecknas enligt 5.1. I stället ska förekomsten meddelas säkerhetsskyddschefen eller den säkerhetsklassade tjänsteman som denne delegerat uppgiften till. Sådant meddelande ska överföras muntligen vid fysiskt möte.

1.1.2 Höjd nivå (konfidentialitet, riktighet och tillgänglighet)

För dimensionerna konfidentialitet, riktighet och tillgänglighet gäller att **höjd** nivå endast ska tillämpas om **allvarlig skada** kan drabba LiU, samarbetspartner eller enskild individ om **konfidentialitet** bryts, information **förvanskas** (riktighet) eller information **förloras** (tillgänglighet). Allvarlig skada ska tolkas i ett LiU-övergripande perspektiv. En förlust om mindre än 500 000 kr är antagligen inte en allvarlig skada. Minskat förtroende för LiU som organisation till följd av att känsliga personuppgifter exponeras kan däremot vara allvarligt för hela LiU. Vidare ska **höjd konfidentialitet** gälla information som sannolikt omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400).

1.1.3 Normal nivå (konfidentialitet, riktighet och tillgänglighet)

Om nivån inte är **höjd** används alltså nivån **normal** som ändå ska ge ett grundskydd. Notera att **normal konfidentialitet** inte innebär avsaknad av konfidentialitet utan att det räcker med grundskyddet; motsvarande gäller för övriga dimensioner.

1.1.4 Personuppgifter och känsliga personuppgifter

Klassning av personuppgift är i allmänhet lättare att genomföra än att klassa övriga dimensioner. Antingen förekommer inga personuppgifter alls (**inga personuppgifter**), endast personuppgifter som inte är känsliga (**normala personuppgifter**) eller **känsliga personuppgifter**.

En personuppgift är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. **Känsliga personuppgifter** är enligt dataskyddsförordningen uppgifter om:

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

Vidare likställs uppgifter som berör fällande domar i brottsmål samt lagöverträdelser med känsliga personuppgifter.

1.2 Särskilt skyddsvärd information

Begreppet **särskilt skyddsvärd information** används för att snabbare referera till information klassad med någon av nivåerna **höjd konfidentialitet, höjd riktighet, höjd tillgänglighet** eller **känsliga personuppgifter**. Det finns många riktlinjer som är tillämpliga för samtliga dessa klassningar.

1.3 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 http://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 skaffa sig högre 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 onödiga 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 transporteras eller förvaras utanför tjänstemiljön ska innehavaren vidta åtgärder för att skydda densamma. Observera särskilt Riktlinjer för säkert resande (LIU-2018-00399).

2.1.8 Anställda och andra uppdragstagare ska ta del av och följa anvisningar gällande hanteringen av information som vederbörande ges tillgång till genom sitt uppdrag. Information ska i normalfallet endast användas i tjänsten. För eventuell privat användning av information som inte är av uppenbart allmän karaktär, redan har publicerats offentligt, eller faller under ”lärarundantaget” ska man, för att säkerställa en objektiv sekretessprövning, begära ett utlämnande av handling genom registrator eller den som har vården om handlingen.

2.1.9 Vid ny personuppgiftsbehandling ska riktlinjer enligt 5.4 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. 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.

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

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

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

2.2.5 Lösenord ska väljas så att de är svårgissade[2].

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

2.2.7 Det är tillåtet att använda en lösenordshanterare för lagring av personliga lösenord. Se särskilda rekommendationer från IT-avdelningen.[3]

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 **särskilt skyddsvärd** information se nedan (2.3.2).

2.3.2 Lagring av filer som innehåller **särskild skyddsvärd** information ska ske på IT-avdelningens tjänst för säker lagring eller annan lagringstjänst anvisad av informationssäkerhetssamordnaren. Om informationsägare 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 skrivare övervakas under utskrift.

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, alternativt ska lagringsmediets innehåll raderas på ett sådant sätt att informationen inte kan återskapas.

---

[2] Använd gärna en lösenordsfras bestående av minst fem slumpmässigt valda ord.
[3] https://insidan.liu.se/informationssakerhet/rekommendation-om-losenordshanterare

2.3.6 Användare av datorer ansvarar för att låsa datorn när han eller hon lämnar den utan uppsikt.

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

2.3.8 Användare av datorer och andra enheter ska använda LiU:s VPN vid användning av öppna trådlösa nätverk för arbetsuppgifter vid LiU.

2.3.9 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 abuse@liu.se.

2.4 Molntjänster

2.4.1 IT-direktören beslutar vilka molntjänster som får användas vid LiU[4]. Den vid var tid gällande listan 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. Information klassad med **höjd konfidentialitet** eller **känsliga personuppgifter** ska inte hanteras i molntjänster om inte informationsägaren gett särskild anvisning som tillåter sådan hantering.

2.4.2 Andra molntjänster än de som godkänts av IT-direktören ska inte användas för hantering av LiU:s information.

Notera att förbudet gäller även allmänt populära tjänster som exempelvis Googles molntjänster (G Suite inklusive Google Mail och Drive), Apple Icloud (inklusive fillagring och backup), Dropbox, Mailchimp, Evernote, Doodle och Adobe Document Cloud. Undantag kan dock gälla om en extern part är huvudman och säkerställer efterlevnad av lagstiftning.

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[5] 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-postsystemet endast genom LiU:s webbmail. Se även 2.9.3.

---

[4] Stärkt informationssäkerhet på LiU (LiU-2014-00052), punkt 5.
[5] https://insidan.liu.se/dokumenthantering

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.

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:

Känsliga personuppgifter som en individ tillhandahåller om sig själv via okrypterad e-post utan föregående uppmaning från LiU får fortsätta behandlas via okrypterad e-post till dess att ärendet är avslutat eller berörd individ begär att behandlingen ska upphöra.

Uppgift om facktillhörighet får hanteras okrypterad via e-post om personuppgiftsbehandlingen sker för att säkerställa den registrerades rättigheter inom arbetsrätten och både avsändare och mottagare av e-postmeddelandet använder e-postadress som slutar på liu.se.

2.6 Massutskick via e-post

Med massutskick via e-post 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 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-säkerhetsgrupp kan komma att stoppa utskick som bryter mot dessa regler eller gällande praxis. IT-säkerhetsgruppen 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 Följande typer av e-postutskick är inte tillåtna:

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

2.6.2 E-postutskick ska ske med stor urskillning. Detta innebär att åtgärder ska vidtas för 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.

2.6.3 E-postutskick med övergripande studieinformation eller annan verksamhetsrelaterad information från LiU till dess studenter och medarbetare är normalt tillåtet.

2.6.4 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[6].

2.6.5 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.

2.6.6 E-postutskick från studentkårerna till sina medlemmar är tillåtna.

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

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

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 samt ärendenummer på polisanmälan ska också meddelas IT-säkerhetsgruppen på e-postadress abuse@liu.se.

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.

---

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

2.9 Användning av privat utrustning

2.9.1 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).

2.9.2 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.

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

2.10 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.

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 handläggningsordning för hantering av oegentligheter (LiU-2016-00759). 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.

3 Riktlinjer för kontoadministration

Det användarkonto som anställda, konsulter och andra uppdragstagare får tillgång till utgör grunden för åtkomst till IT-resurser vid LiU och är en mycket viktig komponent i skyddet av LiU:s information. För att få initial tillgång till användarkontot krävs en aktiveringsnyckel, vilken utfärdas av särskilt utsedda **kontoadministratörer**. I detta kapitel fastställs riktlinjer för kontoadministration som riktar sig till kontoadministratörer och **prefekter/motsvarande**. Riktlinjerna är obligatoriska. Eventuella avsteg får endast göras efter skriftligt beslut av IT-direktören.

3.1 Prefekt/motsvarande

3.1.1 Prefekt (eller den som denne delegerat uppgiften till) ska tillse att konton som inte längre behövs på grund av avslutad relation med LiU stängs av kontoadministratören. Vid en anställnings upphörande eller vid avslutat uppdrag hos LiU ska prefekt således kontakta kontoadministratör och begära avslutande av konto. Vilka som kan anses berättigade till användarkonto vid LiU regleras i Tillgång till IT- och tekniska resurser (LiU-2018-01792).

3.2 Kontoadministratör

3.2.1 Kontoadministratör ska i samband med att aktiveringsnyckel överlämnas till användare upplysa denne om riktlinjerna för informationssäkerhet enligt kapitel 2 i detta dokument. Kontoadministratör intygar att informationen överlämnats till användaren genom kryssruta i kontoaktiveringsverktyget.

3.2.2 Kontoadministratör ska vid utfärdande av aktiveringsnyckel säkerställa att legitimationskontroll sker samt i systemet för kontoadministration ange hur sådan kontroll genomförts.

3.2.3 Dator som används för utfärdande av aktiveringsnyckel ska omfattas av skyddsnivå **guld** eller **silver**.

3.2.4 Kontoadministratör ansvarar för att utfärdad aktiveringsnyckel överlämnas personligen, skickas med rekommenderat brev eller på annat sätt befordras med likvärdig säkerhetsnivå direkt till användaren. Under inga omständigheter får annan än användaren själv sätta lösenord på användarkontot.

4 Riktlinjer för systemadministratörer

Med systemadministratör menas här individ som har högre behörigheter än vanliga användare i ett IT-system och som har undertecknat särskild ansvarsförbindelse för systemadministratörer (LiU-2018-01854).

I detta kapitel fastställs riktlinjer för informationssäkerhet för systemadministratörer. Vid konflikt med riktlinjer i kapitel 2 har kapitel 4 företräde.

4.1 Objektägares ansvar att utse systemadministratör

4.1.1 Objektägare avgör vem som ska ha rollen systemadministratör för de objekt som denne ansvarar för. Objektägare ska säkerställa att utpekade systemadministratörer bekräftar kännedomen om dessa riktlinjer genom undertecknande av särskild blankett.

4.2 Allmänt

4.2.1 Dedikerade administrationskonton, eller andra konton med förhöjda behörigheter, ska inte användas annat än när arbetsuppgiften kräver det.

4.3 Särskilda skyldigheter

4.3.1 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.

4.3.2 En systemadministratör ska informera universitetets IT-säkerhetsgrupp vid misstanke om säkerhetsbrister eller misstanke om inträffad IT-säkerhetsincident. Informationsskyldigheten gäller upptäckter som görs inom hela universitetets IT-miljö.

4.3.3 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, till exempel lagbrott, ska universitetets IT-säkerhetsgrupp informeras.

4.3.4 En systemadministratör ska ha god kännedom om dessa riktlinjer för informationssäkerhet i sin helhet.

4.4 Särskilda rättigheter

4.4.1 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.

4.4.2 En systemadministratör har rätt att rensa i e-postlådor och lagringsutrymmen som missköts eller är inaktiva. Rensning ska om möjligt föregås av information till berörd användare. Om detta inte är möjligt ska berörd institution eller avdelning informeras.

4.4.3 En systemadministratör har rätt att vid akuta driftsituationer utan förvarning tillfälligt begränsa tillgången till IT-resurser.

4.5 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 ansvarsförbindelsen för systemadministratörer.

4.5.1 IT-säkerhetsgruppen har rätt att utvärdera och testa säkerheten i universitetets IT-miljö.

4.5.2 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 utreda misstänkta informationssäkerhetsincidenter och brott mot LiU:s regelverk.

4.5.3 IT-säkerhetsgruppen har rätt att vid behov vidta åtgärder för att säkerställa efterlevnad av universitetets regelverk samt för att hantera informationssäkerhetsincidenter. Sådana åtgärder kan exempelvis innefatta begränsning av tillgång till datornät eller andra IT-resurser, samt omhänderta och undersöka utrustning som ägs av universitetet.

5 Riktlinjer för informationsägare

I detta kapitel återfinns generella riktlinjer för hantering av LiU:s information. Målgrupp för detta kapitel är framförallt informationsägare, det är dennes ansvar att säkerställa att riktlinjerna efterlevs. Informationsägare är den som har mandat att styra över eller besluta om att avveckla en viss informationstillgång. Exempel på informationsägare kan vara objektägare, ansvarig för ett forskningsprojekt eller examinator av ett exjobb.

En grundprincip i LiU:s ledningssystem för informationssäkerhet är att ansvaret för informationssäkerhet följer den normala delegationsordningen. Det innebär att varje informationsägare har vissa möjligheter att, **efter riskanalys**, välja till och välja bort lämpliga skyddsåtgärder. Riktlinjerna i kapitel 5 och 6 utgör en uppsättning grundläggande skyddsåtgärder.

Vissa skyddsåtgärder baseras på lagkrav eller påverkar informationssäkerheten i flera informationstillgångar. För att säkerställa lagefterlevnad och acceptabelt skydd för LiU i övrigt får avsteg från dessa skyddsåtgärder endast göras efter dokumenterat godkännande av informationssäkerhetssamordnaren. Sådana riktlinjer markeras med stjärna (☆) och grov linje i högermarginalen.

5.1 Förteckning av informationstillgångar

5.1.1 Informationstillgångar ska minst var tredje år inventeras, klassificeras och förtecknas enligt de former som fastställs i LiU:s informationssäkerhetspolicy. ☆

5.1.2 Informationsägare ska löpande uppdatera förteckningen enligt ovan när informationstillgångar tillkommer eller avvecklas i verksamheten.

5.1.3 För samtliga informationstillgångar ska en bevarandeplan upprättas enligt LiU:s strategi för bevarande av handlingar (LiU-2018-01344).

5.2 Anskaffning, upphandling och avyttring av IT-system

Om IT-systemet behandlar personuppgifter notera även 5.4 Särskilda krav vid behandling av personuppgifter.

5.2.1 Vid upphandling och annan anskaffning av nya IT-system ska krav på informationssäkerhet ställas för att säkerställa efterlevnad av tekniska aspekter i dessa riktlinjer. IT-avdelningen underhåller en katalog med baskrav för IT som ska användas vid upphandling och annan kravställning. Genom användning av denna kravkatalog säkerställs att tekniska krav i denna riktlinje uppfylls. Kravkatalogen finns tillgänglig på https://insidan.liu.se/informationssakerhet. ☆

5.2.2 Anskaffning av domännamn ska ske genom IT-avdelningen. LiU ska registreras som innehavare av domännamnet. Undantag kan ske om extern part är huvudman.

5.2.3 Innan avveckling av IT-system sker ska Dokument- och arkivenheten kontaktas för att upprätta en bevarandeplan för informationstillgången eller revidera befintlig bevarandeplan.

5.2.4 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 IT-avdelningen för destruktion.

5.2.5 Det är inte tillåtet att avyttra utrustning utan att rensa eller förstöra lagringsmedia. Vid avyttring av datorer, telefoner, surfplattor och andra enheter samt lagringsmedia ska LiU:s återbrukspolicy (LIU-2015-02023) beaktas.

5.3 Åtkomstkontroll

Exempel på åtkomstkontroll är verifiering av användaridentitet och auktorisation i ett IT-system eller låst förvaring där enbart behöriga ges tillträde.

5.3.1 Tillgång till hantering av en informationstillgång ska ges endast den som behöver tillgången för utförandet av sina arbetsuppgifter eller sitt uppdrag vid LiU.

5.3.2 Vid indikation på att inloggningsuppgifter röjts ska behörighet återkallas och incident rapporteras till LiU:s IT-säkerhetsgrupp. ☆

5.3.3 Behörigheter ska vara individuella. Opersonliga konton till IT-resurser ska undvikas.

5.3.4 Det ska vara möjligt att tillfälligt eller permanent begränsa en enskild individs åtkomst till en informationstillgång. För IT-system kan detta uppnås genom tillämpning av 6.3.4.

5.3.5 Behörigheter till **särskilt skyddsvärd** informationstillgång ska granskas regelbundet, för att upptäcka och korrigera felaktigheter.

5.3.6 Behörigheter ska återtas när behov av behörighet inte längre kvarstår.

5.4 Särskilda krav vid behandling av personuppgifter

Observera även riktlinjer för behandling av personuppgifter (LIU-2018-01540).

5.4.1 Behandling av personuppgifter ska anmälas till universitetets dataskyddsombud enligt LiU:s riktlinjer för behandling av personuppgifter. ☆

5.4.2 Vid behandling av känsliga personuppgifter ska, om möjligt, pseudonymisering tillämpas.

5.4.3 Personuppgiftsbehandling får endast ske om det finns en laglig grund för hanteringen.

5.4.4 Registrerade personer ska få information om den personuppgiftsbehandling LiU utför inklusive dess syfte.

5.4.5 Endast de uppgifter som krävs för att uppfylla behandlingens syfte ska inhämtas och lagras. Endast de som behöver uppgifterna ska ha tillgång till dem. Personuppgifter ska undvikas helt om det är möjligt att uppnå syftet med behandlingen genom användning av anonyma uppgifter utan att det avsevärt försvårar arbetet.

5.4.6 Det ska vara möjligt att rätta felaktiga uppgifter och uppgifterna ska hållas uppdaterade. Kravet gäller inte arkiverade handlingar.

5.4.7 Personuppgifter får endast behandlas så länge det behövs för att uppfylla det ändamål för vilka de samlades in, vilket innebär att det ska vara möjligt att radera personuppgifter. Så snart de avsedda personuppgifterna inte längre behövs för sitt ändamål ska de arkiveras, gallras eller avidentifieras. Vid tveksamhet bör arkivarie vid Dokument- och arkivenheten rådfrågas.

5.4.8 Innan en ny personuppgiftsbehandling som hanterar **känsliga personuppgifter** i stor omfattning inleds ska en konsekvensbedömning genomföras i samråd med LiU:s dataskyddsombud. Sådan konsekvensbedömning ska även genomföras för annan personuppgiftsbehandling om denna bedöms kunna leda till en hög risk för registrerade personers integritet.

5.4.9 Personuppgiftsincidenter ska omgående rapporteras till LiU:s dataskyddsombud enligt LiU:s riktlinjer för behandling av personuppgifter. Incidenten ska också rapporteras till LiU:s IT-säkerhetsgrupp.

5.4.10 Överföring av personuppgifter till land utanför EU/EES är förbjuden om inte landet har en adekvat skyddsnivå eller mottagaren är ansluten till av EU-kommissionen godkänt avtal eller tillämpar standardavtalsklausuler. Vid behov av överföring av personuppgifter till land utanför EU/EES ska dataskyddsombudet kontaktas för rådgivning kring gällande lagstiftning.

5.4.11 Vid behandling av personuppgifter baserad på samtycke ska objektägare säkerställa att det är möjligt att radera personuppgift om den registrerade återkallar sitt samtycke.

5.4.12 När personuppgifter behandlas av tredje part för LiU:s räkning ska personuppgiftsbiträdesavtal upprättas. Detsamma gäller om LiU behandlar personuppgifter för annan organisations räkning. Vid behov av rådgivning ska LiU:s dataskyddsombud kontaktas.

5.5 Incidentrapportering och kontinuitetsplanering

5.5.1 Informationsägare ska säkerställa att avvikelser rörande konfidentialitet, riktighet och tillgänglighet omgående rapporteras till LiU:s IT-säkerhetsgrupp. Personuppgiftsincidenter ska även rapporteras till dataskyddsombudet. ☆

5.5.2 För informationstillgång klassad med **höjd tillgänglighet** som hanteras med hjälp av IT-system ska informationsägaren säkerställa att det finns en plan för fysiskt underhåll av hårdvara anpassad till rådande krav på tillgänglighet.

5.6 Informationssäkerhetsplan

5.6.1 För **särskilt skyddsvärda** informationstillgångar bör informationsägaren fastställa en informationssäkerhetsplan[7]. Planen bör beakta långsiktig kompetensförsörjning (5.7.2) och fysiskt underhåll av hårdvara för att säkerställa krav på tillgänglighet i IT-system (5.5.2). Vidare kan planen vara en naturlig plats att samla användaranvisningar för informationssäkerhet (till exempel sådana som nämns i 5.8.9 och 5.8.10).

5.7 Informationsägares ansvar för medarbetare

5.7.1 Informationsägare ska fastställa anvisningar gällande hanteringen av **särskilt skyddsvärd** informationstillgång. För övriga informationstillgångar bör sådan anvisning fastställas. ☆

5.7.2 Informationsägare ska säkerställa att alla som arbetar med **särskilt skyddsvärd** informationstillgång har god kompetens på system de använder där denna behandlas.

5.8 Fysisk säkerhet

5.8.1 Tillträde till lokaler där en **särskilt skyddsvärd** informationstillgång förvaras eller där system som hanterar sådan förvaras ska vara begränsad till personer som behöver åtkomsten för att utföra sina arbetsuppgifter.

5.8.2 Tillträde till utrymme där **särskilt skyddsvärd** fysisk informationstillgång förvaras ska loggas, till exempel genom passersystem. Detta gäller även tillträde till utrymme där IT-system som hanterar sådan informationstillgång förvaras.

5.8.3 Ändamålsenligt skydd ska används vid fysisk transport av **särskilt skyddsvärd** informationstillgång.[8]

---

[7] En generell mall finns tillgänglig på https://insidan.liu.se/informationssakerhet
[8] Exempel på skydd är rekommenderat brev eller befordran med betrodd kurir i kombination med säkerhetskuvert, plombering eller liknande.

5.8.4 Fysiskt utrymme där **särskilt skyddsvärd** information, eller system som behandlar sådan information, förvaras ska skyddas av larmsystem som uppfyller krav gällande larmklass 2 enligt SSF 130.[9]

5.8.5 Fysiskt utrymme där information förvaras ska ha en ändamålsenlig miljö avseende exempelvis temperaturreglering, luftfuktighet, översvämningsskydd 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.

5.8.6 Fysiskt utrymme där **särskilt skyddsvärd** information, eller system som behandlar sådan information, förvaras ska uppfylla säkerhetsklass SSF 200, skyddsklass 2 avseende fysiskt intrång[10].

5.8.7 **Särskilt skyddsvärda** fysiska informationstillgångar ska inventeras regelbundet. Inventering av en tillgång innebär att en eller flera personer kontrollerar att tillgången finns, är i det skick den ska vara, och förvaras på rätt sätt.

5.8.8 Säkerhetskopiering ska i möjligaste mån genomföras av fysiska informationstillgångar klassade med **höjd riktighet** eller **höjd tillgänglighet**. Säkerhetskopior ska förvaras så att en händelse som påverkar riktighet eller tillgänglighet hos originalen inte påverkar kopiorna (och vice versa).

5.8.9 Vid förvaring av en **särskilt skyddsvärd** informationstillgång utanför tjänstemiljö ska ändamålsenligt skydd finnas. Anvisningar för detta dokumenteras lämpligen i en informationssäkerhetsplan (se 5.6.1).

5.8.10 För information klassad med **höjd konfidentialitet** bör ansvarig fastställa anvisningar för hur och var man får kommunicera om informationstillgången[11]. Detta dokumenteras lämpligen i en informationssäkerhetsplan (se 5.6.1).

---

[9] Övergripande beskrivning av SSF 130 finns beskriven i Vägledning för fysisk informationssäkerhet i it-utrymmen (MSB629)
[10] Övergripande beskrivning av SSF 200 finns beskriven i Vägledning för fysisk informationssäkerhet i it-utrymmen (MSB629)
[11] Exempel på omfattning: vilka platser man får tala om informationen på, om man får diskutera informationen per telefon eller om man får skicka informationen via SMS.

6 Riktlinjer för IT-system

Riktlinjerna i detta avsnitt utgör tekniska krav på drift, utveckling och förvaltning av IT-system och gäller såväl för befintliga system som vid nyanskaffning.

Avsteg från riktlinjerna får endast göras efter särskild riskanalys enligt de premisser som beskrivs i kapitel 5.

6.1 Krav på användares IT-utrustning

6.1.1 Låsning av datorer och mobila enheter ska aktiveras automatiskt vid inaktivitet. Låsning ska ske efter högst tio minuter för stationära datorer och efter högst fem minuter för mobila enheter (inklusive bärbara datorer). ☆

6.1.2 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).

6.1.3 System som hanterar **särskilt skyddsvärd** information ska vid användning kräva klient med skyddsnivå **guld** eller **silver** ansluten till datornät avsett för sådan klient eller ansluten till VPN.

6.2 Grundläggande säkerhet

6.2.1 Programvara och operativsystem på servrar, persondatorer och mobila enheter som hanterar LiU:s information ska löpande hållas uppdaterade med de uppdateringar för säkerhet och tillförlitlighet som leverantörer tillhandahåller. Uppdateringar ska installeras så snart som möjligt och det ska finnas en rutin för omedelbar installation av akuta uppdateringar. ☆

6.2.2 IT-system anslutna till LiU:s datornät ska konfigureras så att automatisk sårbarhetskontroll via nätverket möjliggörs från av IT-säkerhetsgruppen utpekade IP-adresser.

6.2.3 Sårbarheter i IT-system ska åtgärdas skyndsamt då de blir kända eller påtalas.

6.2.4 IT-system ska ha en ändamålsenlig driftsmiljö avseende temperaturreglering, luftfuktighet och elförsörjning. För system som hanterar information klassade med **höjd tillgänglighet** ska driftmiljön vara övervakad för att möjliggöra snabb upptäckt av problem.

6.2.5 Information i IT-system och vid behov programvara för IT-system ska säkerhetskopieras så att denna kan återskapas vid dataförlust. Vid krav på **höjd riktighet** bör inte samma individ kunna ändra både original och säkerhetskopia.

6.3 Användarhantering och inloggning

☆

6.3.1 Inloggning till IT-system ska ske genom användning av LiU:s ADFS med tvåstegsverifiering. Tvåstegsverifiering krävs inte för studenter eller vid inloggning från klient med skyddsnivå **guld** eller **silver** ansluten till datornät avsett för sådan klient.

6.3.2 Inloggning i webbaserade system ska inte ske genom autentisering direkt mot AD eller LDAP. System satta i drift före 2018-06-30 som redan autentiserar direkt mot AD eller LDAP kan under en övergångsperiod fortsätta göra detta. Sådana system ska avvecklas eller anpassas till inloggning med ADFS senast 2020-06-30.

6.3.3 Lösenord ska överföras med tillförlitlig kryptering.

6.3.4 Behörigheter till system ska vara personliga.

6.3.5 Vid användning av lokal användardatabas ska användaridentitet inte likna LiU-ID. Hantering av lösenord ska följa riktlinjer för hantering av användarkonton och lösenord (se 2.2). Lösenord klassas med **höjd konfidentialitet** och **höjd riktighet**.
Lösenord för lokal användardatabas ska lagras kodade på ett icke reversibelt sätt. Om så inte kan ske måste systemet förhindra eller försvåra återanvändning av lösenord från ordinarie användarkonto.
Lösenord ska kunna bytas av användaren själv. Periodiskt återkommande tvingande lösenordsbyten ska undvikas.[12]

6.3.6 Auktorisation av användare ska ske genom användning av grupper i LiU:s AD. Grupptillhörighet ska alltså kunna styra behörigheter i systemet.

6.3.7 För system som inte kan använda tvåstegsverifiering, mobila e-postklienter, IM-klienter och liknande ska särskilda lösenord genereras.

6.4 Loggning och behandlingshistorik

6.4.1 Åtgärder i IT-system som hanterar särskilt skyddsvärd information ska loggas. Loggen i sig klassas med **höjd riktighet**. Minst följande ska loggas:

- Läsning av information klassad med **höjd konfidentialitet** eller **känsliga personuppgifter**.
- Radering av information klassad med **höjd tillgänglighet** eller **höjd riktighet**.
- Förändring av information klassad med **höjd riktighet**.

[12] 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.

6.5 Kryptering och signering

☆

6.5.1 **Särskilt skyddsvärd** information ska överföras krypterad och signerad med tillförlitliga metoder vid elektronisk kommunikation. För e-post se riktlinjer för anställda 2.5 E-post.

6.5.2 Lagring av information klassad med **höjd konfidentialitet** eller **känsliga personuppgifter** ska ske i krypterad form. Krypteringsnycklar för åtkomst av sådan lagring ska klassas med **höjd konfidentialitet**.

6.6 Webbaserade system

Dessa riktlinjer gäller webbaserade system som tillhandahålls av LiU och hanterar LiU:s information.

☆

6.6.1 För webbaserade system ska en lista över vilka webbläsare och plattformar som stöds definieras och dokumenteras. Systemet ska fungera med den senaste och den näst senaste versionen av de webbläsare som stöds. Användare förutsätts uppgradera webbläsare i takt med att nya versioner blir tillgängliga.

6.6.2 System ska inte ställa krav på plugins i webbläsare. Systemet ska fungera med webbläsare enligt 6.6.4 med standardinstallation. Detta innebär att systemet exempelvis inte får kräva webbläsarplugin för Java, Flash, Silverlight, ActiveX eller liknande.

6.6.3 Webbaserade system ska fungera utan särskilda inställningar eller säkerhetspolicys på klienten. Detta innebär att systemet ska fungera med webbläsare som stöds på nyinstallerad dator eller enhet utan vidare justeringar.

6.6.4 Webbaserade system som riktar sig till många användare ska vara åtkomliga under domänadress på formen tjänst.liu.se.[13] System som drivs i samarbete med extern part kan använda annan domänadress efter godkännande från IT-direktören. Omdirigering efter initial åtkomst är tillåten.

6.6.5 Certifikat för webbtjänster ska vara utfärdade av en betrodd utgivare. Certifikat för webbtjänst med domänadress som ägs av LiU (exempelvis alla domänadresser som slutar på .liu.se) ska utfärdas genom LiU CA (via Sunet TCS)[14].

---

[13] Hög grad av användning av interna domännamn ökar förutsättningarna för våra användare att identifiera nätfiske som nästan uteslutande använder externa domäner.
[14] Dessa certifikat beställs kostnadsfritt genom IT-avdelningen

6.6.6 Webbaserade system som riktar sig till många användare ska fungera med nedanstående webbläsare och plattformar:

- Edge (Windows)
- Chrome (Windows, MacOS, Linux, Android)
- Firefox (Windows, MacOS, Linux)
- Safari (MacOS, iOS)

6.6.7 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 användas.

6.6.8 HTTPS för webbaserade system ska konfigureras enligt LiU:s IT-säkerhetsgrupps rekommendationer[15].

6.7 Serversäkerhet i nätverksbaserade tjänster

Nedanstående gäller både webbaserade system och andra system som kommunicerar över nätverket.

6.7.1 Vid krav på **höjd konfidentialitet** eller **höjd riktighet** ska det inte vara möjligt att använda tjänsten med protokoll med stora kända sårbarheter. Exempel på sådana protokoll är NTLM, SSL (version 1–3) och TLS version 1.0–1.1. ☆

6.7.2 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.

6.7.3 IT-system som hanterar **särskilt skyddsvärd** information ska skyddas med nätverksbrandvägg med för ändamålet lämplig konfiguration.

6.7.4 Servrar och annan utrustning ansluten till LiU:s datornät ska vara konfigurerade för att tillåta sårbarhetsscanning från av IT-säkerhetsgruppen utpekade IP-adresser. Detta gäller inte enheter som ägs av annan än LiU, till exempel studenter, anställda privat eller besökare. Dock kan även sådana enheter komma att scannas när de är anslutna till LiU:s datornät.

6.8 IT-system med klient för persondator eller mobil enhet

Dessa krav gäller vid anskaffning och utveckling av IT-system med klientprogramvara.

6.8.1 Klientprogramvara ska tillåta löpande uppdatering (patchning) av operativsystem och andra programvaror (webbläsare, Java, webbläsartillägg och liknande). ☆

[15] https://insidan.liu.se/informationssakerhet

6.8.2 Klientprogramvara ska inte kräva undantag i säkerhetsinställningar i operativsystem. Det innebär till exempel att det inte får krävas gammal programvara, inställningar av betrodda webbplatser, undantag i säkerhetsprogram eller liknande.

6.8.3 Klientprogramvara ska inte kräva att användaren har administratörsbehörighet på den dator där programvaran körs.

6.9 Systemförvaltning

6.9.1 Förändringar på IT-system 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.

6.9.2 För 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.

6.9.3 Förändringar i IT-system som hanterar **särskilt skyddsvärd** information ska prövas i en testmiljö innan de driftsätts i produktionsmiljö.

6.10 Säkerhetskopiering

6.10.1 Vid säkerhetskopiering av information klassad med **höjd konfidentialitet** ska säkerhetskopian lagras krypterad. Krypteringsnycklar klassas med **höjd konfidentialitet**.

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.
Beslutskonto	Användarkonto som kan utfärdas till person som inte har anställning vid LiU
Betrodd certifikatutgivare	Utgivare av certifikat som IT-säkerhetsgruppen definierat som betrodd, vilket normalt innefattar utgivare betrodda av operativsystem och webbläsare.
End-of-life	Tillstånd för program eller hårdvara efter att leverantör slutat underhålla densamma.
Härdning	Process för att konfigurera operativsystem mer motståndskraftigt mot IT-attacker än vad som annars vore fallet.
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.
Informationstillgång	Information eller resurs som används för att hantera information.
Informationsägare	Den som har mandat att styra över eller besluta om att avveckla en viss informationstillgång. Exempel på informationsägare är objektägare och ledare för forskningsprojekt.
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, till exempel med AD. LDAP används också vid LiU för att beskriva en (äldre) katalogserver som LiU använder.

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, till exempel genom användning av virtuella lokala nätverk (VLAN).
MFA	**Multifaktorautentisering.** Autentisering med mer än en faktor. Ordet används ibland för att beskriva tvåstegsverifiering.
Molntjänst	IT-tjänst som tillhandahålls över internet, i allmänhet hos en extern leverantör.
Objektägare	Ansvarig för ett informationsbehandlande system. Se förvaltningsmodell beskriven i Dnr. LiU-2012-00330, se även informationsägare.
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.
PGP	En metod för kryptering och signering av e-post m.m.
Pseudonymisering	Genom pseudonymisering kodas uppgifter i en personuppgiftsbehandling så att det inte utan kodnyckel går att identifiera vilken individ uppgifterna rör.
Riktighet	Egenskapen att en information inte obehörigen förändras.
S/MIME	En standard för kryptering och signering av e-post.
Sekretess	Ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. (SFS 2009:400)
SSL	Secure Sockets Layer. Äldre protokoll för att kryptera och signera datatrafik. Ersatt av TLS.
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**, **höjd riktighet**, **höjd tillgänglighet** eller **känsliga personuppgifter**.
Tillförlitlig kryptering och signering	Publicerad metod som används som avsett och som saknar kända säkerhetsbrister.[16]
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”.
TLS	Transport Layer Security. Ett protokoll för att kryptera och signera datatrafik som ersätter det äldre protokollet SSL.
Tvåstegsverifiering	Kallas också **tvåfaktorsautentisering**. Detta är en typ av **multifaktorautentisering (MFA)** Identifiering med två olika metoder, till exempel 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.

[16] För tekniska detaljer se https://insidan.liu.se/informationssakerhet