RB 2020-15 exp 2020-04-06 KF

LINKÖPINGS UNIVERSITET

2020-04-06
DNR LiU-2019-02942
BESLUT

Beslut om Riktlinjer för informationssäkerhet

Beslut

Linköpings universitet (LiU) beslutar att fastställa bilagda riktlinjer för informationssäkerhet. Beslutet börjar tillämpas direkt efter ikraftträdandet och ersätter "Riktlinjer för informationssäkerhet" (LiU-2018-01814) som fastställdes den 11 juni 2018.
Beslutet ska föras in i LiU:s regelsamling.

Skäl till beslut

Myndigheten för samhällsskydd och beredskap föreskriver i Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1) att varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet (5 § MSBFS 2016:1). 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 (7 § MSBFS 2016:1). Riktlinjerna för informationssäkerhet är en central del av LiU:s ledningssystem och behöver uppdateras regelbundet för att adressera förändrade hot och riskbilder samt ändrade förutsättningar och behov i LiU:s verksamhet. De viktigaste förändringarna från de tidigare riktlinjerna (LiU-2018-01814) är:

- Klassningsmodellen har förbättrats för att möjliggöra förenklingar i riktlinjerna och ett stöd för klassning av konfidentialitet har införts.
- Molntjänster kan användas efter beslut av informationsägaren för information med särskilt låga krav på konfidentialitet och integritet.
- Beslut om undantag från riktlinjerna samt om användning av molntjänster som fattas av informationsägare ska meddelas IT-säkerhetsgruppen.

Samtliga förändringar framgår av särskilt kapitel i riktlinjerna.

Handläggningen av beslutet

Beslut i detta ärende har fattats vid rektors beslutsmöte i närvaro av universitetsdirektören Kent Waltersson, studeranderepresentanten Elin Fägerstam och rektors sekreterare Maria Fält efter föredragning av IT-direktör Joakim Nejdeby.

I ärendets handläggning har deltagit systemarkitekt Johannes Hassmund och enhetschef David Byers. Förslaget har även granskats av institutionerna, fakulteterna och Universitetsförvaltningen inklusive Juristenheten samt varit föremål för samverkan med de fackliga organisationerna vid möte i centrala samverkansgruppen. Redaktionen för regelsamlingen har granskat beslutets form.

Helen Dannetun

Joakim Nejdeby

Sändlista:
Universitetsledningen
Dekanerna
Kanslicheferna
Prefekterna
Överbibliotekarien
Administrativa chefer
UDL
Internrevisionen
Lokala fackliga organisationerna
Studentkårerna
LiU-Nytt
Dokument- och arkivenheten (original)

Riktlinjer för informationssäkerhet

LINKÖPINGS UNIVERSITET
UNIVERSITETSLEDNINGEN

Innehåll

Bakgrund

I detta dokument fastställs riktlinjer för informationssäkerhet vid Linköpings universitet (LiU). Riktlinjerna är en del av LiU:s ledningssystem för informationssäkerhet som också består av en informationssäkerhetspolicy (dnr LiU-2018-02237) som beskriver universitetsstyrelsens övergripande viljeinriktning för arbete med informationssäkerhet vid LiU samt en dokumentation över arbetsprocesserna inom ledningssystemet (dnr LiU-2019-03289).

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.

De viktigaste ändringarna sedan den förra utgåvan av riktlinjerna finns sammanfattade i slutet av detta dokument, tillsammans med en förteckning över samtliga förändringar av betydelse.

Läsanvisningar

Definitioner

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

ska	Indikerar ett nödvändigt krav för att uppfylla riktlinjen. Formuleringar som ”är inte tillåtet” och ”får inte” är också att betrakta som nödvändiga krav.
bör	Utgör en stark rekommendation. Riktlinjen ska följas om det inte finns goda skäl att låta bli.

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**. Informationsägare utses av prefekt/motsvarande och det är informationsägarens ansvar att säkerställa att riktlinjerna efterlevs. Exempel på lämpliga personer att utse som informationsägare kan vara objektägare, ansvarig för ett forskningsprojekt eller examinator av ett exjobb. Om informationsägaren inte hanterar särskilt skyddsvärd information räcker det med att läsa och säkerställa efterlevnad av **stycke 5.1-5.6**.

Kapitel 6 innehåller riktlinjer som rör IT-system som hanterar information vid LiU, inklusive sådana som enskilda medarbetare anskaffar. 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.

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

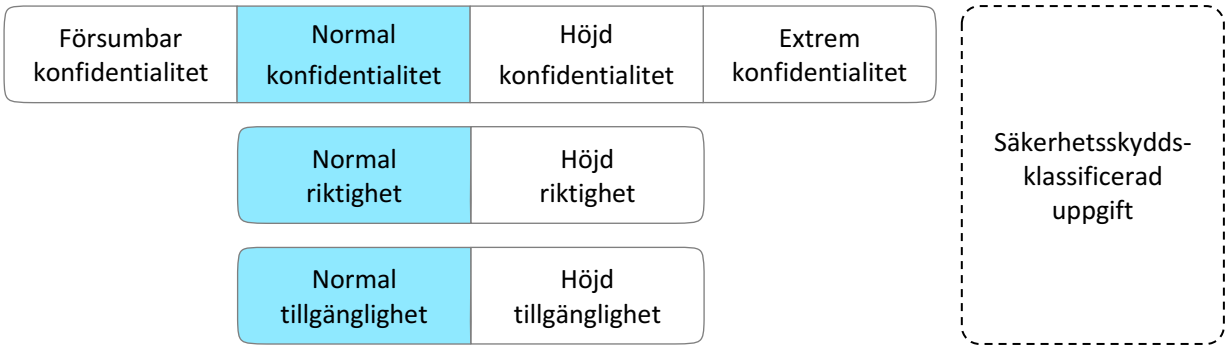
1.1 Informationsklassning

Information vid LiU klassificeras enligt 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 såsom 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.

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. 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**. Riktlinjen träder i kraft tre månader efter att klienter med skyddsnivå guld eller silver är tillgängliga.

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 blankett 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. Vid misstanke om oegentligheter ska dessa dessutom hanteras i enlighet med riktlinjerna för hantering av misstänkta oegentligheter och brott (dnr LiU-2019-03689). Informationsskyldigheten gäller upptäckter som görs inom hela universitetets IT-miljö.

4.3.3 En systemadministratör som får kännedom om en misstänkt personuppgiftsincident ska rapportera enligt gällande rutin[14].

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

[14] https://insidan.liu.se/dataskyddsforordningen/personuppgiftsincident

4.3.5 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 Åtkomst till studenters lagrade data (till exempel på fillager, OneDrive eller i e-post) får endast ske som led i rent teknisk bearbetning eller efter medgivande från berörd individ. Om systemadministratör som led i teknisk bearbetning uppmärksammar allvarlig överträdelse av LiU:s regelverk eller lagbrott, ska detta rapporteras enligt 4.3.

4.4.3 En systemadministratör har rätt att i de system vederbörande ansvarar för 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.

4.4.4 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 blanketten 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 förebygga och 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[15].

Informationsägare utses av prefekt/motsvarande. Det är informationsägarens ansvar att säkerställa att riktlinjerna efterlevs. Exempel på lämpliga personer att utse som informationsägare kan vara objektägare, ansvarig för ett forskningsprojekt eller examinator av ett exjobb.

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. Beslut om undantag från riktlinjerna ska diarieföras och ska skickas för kännedom till IT-säkerhetsgruppen.

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 i detta dokument med stjärna (☆) och grov linje i högermarginalen.

5.1 Förteckning av informationstillgångar

5.1.1 Informationstillgångar[16] ska minst var tredje år inventeras, klassificeras och förtecknas enligt de former som fastställs i LiU:s ledningssystem för informationssäkerhet. Riktlinjen träder i kraft när process och vägledning för inventering har fastställts. ☆

5.1.2 Prefekt eller motsvarande ska löpande uppdatera förteckningen enligt ovan när informationstillgångar tillkommer eller avvecklas i verksamheten. Prefekten eller motsvarande kan utse en kontaktperson för informationssäkerhet som genomför denna uppgift. Riktlinjen träder i kraft när process och vägledning för inventering har fastställts.

5.1.3 För samtliga informationstillgångar som innehåller allmänna handlingar och som inte är avsedd för personligt bruk ska, enligt LiU:s strategi för bevarande av handlingar (dnr LiU-2018-01344), en bevarandeplan upprättas.

[15] Vägledning för inventering av informationstillgångar och för att utse informationsägare kommer att publiceras som del av LiU:s ledningssystem för informationssäkerhet. Vissa av dessa riktlinjer träder inte i kraft förrän denna vägledning är tillgänglig.
[16] Information som insamlats eller upprättats för ett specifikt syfte samt de resurser som används för att hantera informationen, t.ex. programvaror, tjänster, servrar, IT-system och förvaringsutrymmen (definition anpassad från dnr LiU-2018-01344).

5.2 Anskaffning, upphandling och avyttring av IT-system

Om IT-systemet behandlar personuppgifter notera även 5.5 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 (se LiU:s strategi för bevarande av handlingar, dnr LiU-2018-01344).

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 Molntjänster

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

5.3.2 Information där LiU är huvudman får normalt endast hanteras i molntjänst efter beslut av IT-direktören. För information klassad med **försumbar konfidentialitet, normal riktighet** och **normal tillgänglighet** får dock informationsägare själv besluta om vilka molntjänster som får användas. Informationsägaren ska före sådant beslut säkerställa att gällande lagstiftning efterlevs, särskilt avseende personuppgifter[17], offentlighet och sekretess samt arkivering. Beslut om att godkänna molntjänst ska sändas till IT-säkerhetsgruppen.

5.4 Åtkomstkontroll

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

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

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

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

5.4.4 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 6.3.5.

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

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

5.5 Särskilda krav vid behandling av personuppgifter

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

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

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

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

[17] Se även LiU:s riktlinjer för personuppgiftsbehandling (dnr LiU-2018-01540). Notera särskilt dokumentationskrav enligt stycke 4.3 rörande ansvarsskyldighet.

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

5.5.5 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.

5.5.6 Uppgifter ska vara korrekta och hållas uppdaterade, och det ska vara möjligt att rätta felaktiga uppgifter. Kravet är inte tillämpbart på arkiverade handlingar.

5.5.7 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.

5.5.8 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.

5.5.9 Personuppgiftsincidenter ska omgående rapporteras enligt gällande rutin[18]. Incidenten ska också rapporteras till LiU:s IT-säkerhetsgrupp.

5.5.10 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 av EU-kommissionen godkänd uppförandekod eller annan certifiering.

5.5.11 När samtycke används som laglig grund för personuppgiftsbehandlingen ska objektägaren säkerställa att det är möjligt att radera personuppgift om den registrerade återkallar sitt samtycke.

5.5.12 När personuppgifter behandlas av tredje part för LiU:s räkning och enligt LiU:s instruktioner ska personuppgiftsbiträdesavtal upprättas. Detsamma gäller om LiU behandlar personuppgifter för annan organisations räkning och enligt dess instruktioner. Vid behov av rådgivning ska institutionens eller avdelningens kontaktperson för dataskyddsfrågor kontaktas.

[18] Se https://insidan.liu.se/dataskyddsforordningen/personuppgiftsincident

5.6 Incidentrapportering och kontinuitetsplanering

5.6.1 Informationsägare ska säkerställa att avvikelser rörande konfidentialitet, riktighet och tillgänglighet omgående rapporteras till LiU:s IT-säkerhetsgrupp. Personuppgiftsincidenter ska även rapporteras enligt gällande rutiner.[19] ☆

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

5.7 Informationssäkerhetsplan

5.7.1 För **särskilt skyddsvärda** informationstillgångar bör informationsägaren fastställa en informationssäkerhetsplan[20]. Planen bör beakta långsiktig kompetensförsörjning (5.8.2) och fysiskt underhåll av hårdvara för att säkerställa krav på tillgänglighet i IT-system och andra fysiska tillgångar (5.6.2). Vidare kan planen vara en naturlig plats att samla användaranvisningar för informationssäkerhet (till exempel sådana som nämns i 5.9.11 och 5.9.12).

5.8 Informationsägares ansvar för medarbetare

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

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

5.8.3 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.[21]

[19] Se https://insidan.liu.se/dataskyddsforordningen/personuppgiftsincident
[20] En generell mall finns tillgänglig på https://insidan.liu.se/informationssakerhet
[21] Se https://insidan.liu.se/juridisk-radgivning/offentlighet-sekretess, särskilt vägledningen om offentlighet och sekretess, för ytterligare information.

5.9 Fysisk säkerhet

5.9.1 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.

5.9.2 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.

5.9.3 Personer utan eget tillträde till lokal där **särskilt skyddsvärd** informationstillgång förvaras eller där system som hanterar sådan förvaras och som behöver tillfällig åtkomst, till exempel för att utföra en serviceåtgärd, ska eskorteras av en person som har tillträde till lokalen.

5.9.4 Ändamålsenligt skydd ska används vid fysisk transport av **särskilt skyddsvärd** informationstillgång.[22]

5.9.5 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.[23]

5.9.6 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.

5.9.7 Fysiskt utrymme där **särskilt skyddsvärd** information, eller system som behandlar sådan information, förvaras ska uppfylla säkerhetsklass SSF 200, skyddsklass 2 avseende fysiskt intrång[24].

5.9.8 Värdeskåp kan användas för att hantera undantag från 5.9.5 då tillräckligt larm saknas, uppfylla kraven på brandskydd i 5.9.6 samt kraven på intrångsskydd i 5.9.7. Värdeskåpets klass ska väljas efter värdet på den tillgång som skyddas.

---

[22] Exempel på skydd är rekommenderat brev eller befordran med betrodd kurir i kombination med säkerhetskuvert, plombering eller liknande.
[23] 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.
[24] 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.

5.9.9 **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.

5.9.10 Fysiska informationstillgångar klassade med **höjd riktighet** eller **höjd tillgänglighet** ska i möjligaste mån säkerhetskopieras. Säkerhetskopior ska förvaras så att en händelse som påverkar riktighet eller tillgänglighet hos originalen inte påverkar kopiorna (och vice versa).

5.9.11 Vid förvaring av en **särskilt skyddsvärd** informationstillgång utanför tjänstemiljö ska ändamålsenligt skydd finnas. Anvisningar för detta dokumenteras lämpligen i en informationssäkerhetsplan (se 5.7.1).

5.9.12 För information klassad med **höjd konfidentialitet** eller högre bör informationsägaren fastställa anvisningar för hur och var man får kommunicera om informationstillgången[25]. Detta dokumenteras lämpligen i en informationssäkerhetsplan (se 5.7.1).

[25] 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 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 IT-direktören. ☆

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. Riktlinjen träder i kraft tre månader efter att klienter med skyddsnivå guld eller silver är tillgängliga.

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, översvämningsskydd, brandskydd 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.

6.2.6 IT-system ska användas enbart till sina avsedda syften. Det innebär till exempel att servrar eller datorer avsedda för programutveckling inte ska användas för ordbehandling, att läsa e-post eller surfa på webben. Antalet installerade program ska hållas till ett minimum.

6.2.7 Fjärradministration av IT-system ska göras genom säkra lösningar, till exempel säker inloggningsserver eller priviligierad arbetsstation för administratör. IT-avdelningen ska tillhandahålla lämpliga lösningar för detta.

6.2.8 Användning av datornät ska vara spårbart 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 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. Riktlinjen träder i kraft i samband med införande av tvåstegsverifiering för anställda. ☆

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 2021-06-30.

6.3.3 När lösenord används för inloggning ska dessa ha tillräcklig komplexitet. IT-avdelningen fastställer krav på godtagbar komplexitet[26].

6.3.4 Lösenord ska överföras med tillförlitlig kryptering.

6.3.5 Behörigheter till system ska vara personliga.

6.3.6 Vid användning av lokal användardatabas ska LiU-ID inte ingå i användaridentitet. Hantering av lösenord ska följa riktlinjer för hantering av användarkonton och lösenord (se 2.2). Lösenord klassas med **höjd konfidentialitet** och **höjd riktighet**.

[26] https://insidan.liu.se/it/it-sakerhet/krav-pa-losenordskomplexitet

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.[27]

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

6.3.8 För e-postklienter som inte kan använda tvåstegsverifiering ska särskilda lösenord genereras. Riktlinjen träder i kraft i samband med att tvåstegsverifiering införs för anställda.

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 händelser ska loggas:

- 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**.
- Inloggningar och inloggningsförsök.
- Utloggningar.
- Förändringar av användare och behörigheter.

6.4.2 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[28] och ha angiven eller känd tidszon.

6.4.3 Loggar ska i normalfallet bevaras i mellan sex och arton månader om inte annat framgår av dokumenthanteringsplan.

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 2.5. ☆

[27] 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.
[28] Till exempel genom att använda NTP för tidssynkronisering.

6.5.2 Lagring av information klassad med **höjd** eller **extrem konfidentialitet** ska ske i krypterad form. Krypteringsnycklar för åtkomst av sådan lagring ska klassas med samma nivå som informationen.

6.6 Webbaserade system

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

☆

6.6.1 Webbaserade system 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 6.6.1 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.[29] 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 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)[30].

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.

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

6.6.8 HTTPS för webbaserade system ska konfigureras enligt LiU:s IT-säkerhetsgrupps rekommendationer[31].

6.7 Serversäkerhet i nätverksbaserade tjänster

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

☆

6.7.1 Det ska 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).

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 Systemutveckling

Detta avsnitt riktar sig till den som utvecklar IT-system vid LiU.

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

6.9.1 Vid systemutveckling, inklusive utveckling av programvara, ska säkerhetsaspekter beaktas på ett systematiskt sätt.

6.9.2 Vid upphandling eller utveckling av IT-system ska förmågan att ta fram registerutdrag enligt dataskyddsförordningen och annan tillämplig reglering säkerställas.

6.9.3 Vid upphandling eller utveckling av IT-system ska förmågan att korrigera och att radera personuppgifter säkerställas.

6.10 Systemförvaltning

6.10.1 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.

6.10.2 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.

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

6.11 Säkerhetskopiering

6.11.1 Vid säkerhetskopiering av information klassad med **höjd konfidentialitet** eller högre ska säkerhetskopian lagras krypterad. Krypteringsnycklar klassas samma nivå som informationen.

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.
Betrodd certifikatutgivare	Utgivare av certifikat som IT-säkerhetsgruppen definierat som betrodd, vilket normalt innefattar utgivare betrodda av operativsystem och webbläsare.

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 (till exempel adress och ålder i kombination).
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, till exempel med AD. LDAP används också här 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).
Molntjänst	IT-tjänst som tillhandahålls över internet av 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.
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**, **extrem konfidentialitet**, **höjd riktighet**, eller **höjd tillgänglighet**.
Tillförlitlig kryptering och signering	Publicerad metod som används som avsett och som saknar kända säkerhetsbrister.[32]
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”.

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

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.

Lagar, föreskrifter, förordningar, och riktlinjer

Här pekas ett antal lagar, förordningar, och riktlinjer ut som har inverkan på informationssäkerhet och som ska beaktas. **Listan är inte uttömmande** utan fokuserar på reglering med brett tillämpningsområde och reglering som ofta är föremål för frågor eller missförstånd.

Lokala riktlinjer och vägledningar

Dokumenthanteringsplan (LiU-2019-01914) redovisar vilka handlingstyper som förekommer vid myndigheten och hur dessa ska hanteras. Innehåller bland annat anvisningar rörande bevarande och gallring.

Riktlinjer för personuppgiftsbehandling vid Linköpings universitet (LiU-2018-01540). Beskriver hur personuppgifter ska behandlas vid LiU.

Utvalda lagar och föreskrifter

Tryckfrihetsförordningen (SFS 1949:105). Definierar handlingar, allmänna handlingar, offentlighetsprincipen, och lägger grunden till offentlighets- och sekretesslagens reglering av sekretess för allmänna handlingar.

Offentlighets- och sekretesslag (SFS 2009:400). Reglerar offentlighet och sekretess, exempelvis skäl för att inte lämna ut vissa typer av allmänna handlingar.

Arkivlagen (SFS 1990:782) samt Riksarkivets föreskrifter. Reglerar arkiv, dokumenthantering, bevarande, gallring, och rensning och påverkar hur handlingar får hanteras vid LiU.

Dataskyddsförordningen (Europaparlamentets och rådets förordning (EU) 2016/679) och lag med kompletterande bestämmelser till EU:s dataskyddsförordning (SFS 2018:218). Reglerar behandling av personuppgifter och har långtgående inverkan på riktlinjerna för informationssäkerhet.

Patientdatalag (SFS 2008:355). Reglerar vårdgivares behandling av personuppgifter i hälso- och sjukvården. Kompletteras av Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40). Riktlinjerna för informationssäkerhet tar ingen hänsyn till dessa regleringar. **Notera att dessa är tillämpliga enbart för vårdgivare; de är inte tillämpliga i ren forskning.**

Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1). Ställer vissa krav på myndighetens arbete med informationssäkerhet, och är utgångspunkten för dessa riktlinjer.

Förändringar gentemot tidigare version

Detta avsnitt beskriver förändringarna som har införts i riktlinjerna sedan den förra versionen (dnr 2018-01814), beslutad 2018-06-11.

Viktiga förändringar

Förbättring av klassningsmodellen

Klassningsmodellen har förenklats genom att perspektivet personuppgifter tagits bort. Riktlinjer som tidigare styrdes av perspektivet personuppgifter styrs nu av konfidentialitet. Klassningsmodellen har också gjorts mer uttrycksfull i perspektivet konfidentialitet genom två nya nivåer: **försumbar** och **extrem konfidentialitet**. Därigenom har det blivit möjligt att bättre differentiera kraven som ställs, och bland annat förenkla hanteringen av information med särskilt lågt skyddsvärde.

Försumbar konfidentialitet omfattar information som har särskilt lågt skyddsvärde, endast innehåller harmlösa personuppgifter, och inte omfattas av sekretess.

Extrem konfidentialitet tillämpas för bland annat stora mängder uppgifter som var och en skulle klassas med höjd konfidentialitet, uppgifter som omfattas av absolut sekretess, och uppgifter vars röjande skulle ha synnerligen allvarliga konsekvenser.

Kapitel ett i riktlinjerna innehåller en mer fullständig beskrivning av de nya nivåerna och en förklaring av begreppet harmlösa personuppgifter.

Stöd för informationsklassning

Riktlinjerna innehåller ett flödesschema som underlättar klassning av konfidentialitet.

Ökad frihet i användningen av molntjänster

Införandet av nivån **försumbar konfidentialitet** har gjort det möjligt att väsentligt förenkla riktlinjerna kring molntjänster. Information som klassas med **försumbar konfidentialitet, normal riktighet och normal tillgänglighet** får efter beslut av respektive informationsägare behandlas i molntjänster, förutsatt att gällande lagstiftning följs. Godkännande av IT-direktören krävs inte, men beslut ska diarieföras och sändas i kopia till IT-säkerhetsgruppen.

Informationsplikt för undantag och användning av molntjänster

Vid beslut om undantag från riktlinjerna eller godkännande av molntjänster ska IT-säkerhetsgruppen informeras. Kännedom om vilka undantag som görs och vilka tjänster som används gör det möjligt att bättre anpassa framtida riktlinjer till verksamhetens behov och att genomföra mer rättvisande riskanalyser.

Samtliga förändringar

Nedanstående förteckning innefattar inte rent enklare förtydliganden, omnumrerade riktlinjer, eller rent redaktionella förändringar.

Definitioner: förtydligat definitionerna av ”ska” och ”bör”.

Läsanvisningarna: ny definition av informationsägare, förtydligande att kapitel 6 även gäller för IT-system som enskilda medarbetare anskaffar.

Avsnitt 1.1: nya nivåer för klassning av konfidentialitet (”försumbar” och ”extrem”), dimensionen ”personuppgifter” borttagen. Hemlig uppgift ersatt med säkerhetsskyddsklassificerad uppgift för att reflektera ny säkerhetsskyddsförordning.

Avsnitt 1.1.1: förändrad för att reflektera ny säkerhetsskyddsförordning.

Avsnitt 1.1.2: ny beskrivning av nivån ”extrem konfidentialitet”.

Avsnitt 1.1.3: förtydligande av nivån ”höjd konfidentialitet”; förtydligande av nivån ”höjd tillgänglighet”; exempel på tillgångar som skulle kunna klassas med höjd nivå.

Avsnitt 1.1.4: förtydliganden till följd av införandet av ”försumbar konfidentialitet” samt förtydligande genom exempel.

Avsnitt 1.1.5: ny beskrivning av nivån ”försumbar konfidentialitet”.

Avsnitt 1.2: nytt avsnitt om personuppgifter, hur de relaterar till konfidentialitet, samt vägledning kring pseudonymisering och anonymisering.

Avsnitt 1.3: nytt flödesschema för klassning.

Riktlinje 2.1.8: ny formulering av riktlinje och fotnot på begäran av rättsavdelningen.

Riktlinje 2.2.1: klargörande att personliga behörigheter får upplåtas till andra under direkt överinseende.

Riktlinje 2.2.6: ny riktlinje rörande registrering av e-postadresser i externa tjänster.

Riktlinjer 2.3.1, 2.3.2: förenklade till följd av införandet av extrem konfidentialitet.

Riktlinje 2.3.5: ändring från ”ska” till ”bör” i första meningen.

Riktlinje 2.3.6: ny riktlinje rörande sekretessfilter.

Riktlinje 2.3.7: förtydligande att datorer eller andra enheter inte bör lämnas obevakade där stöldrisken inte är försumbar.

Riktlinje 2.3.8: komplexa mönster betraktas inte längre som adekvat skärmlås.

Riktlinje 2.3.9: ny riktlinje rörande kontroll av riktighet i information. Riktlinjen är framförallt avsedd att ge stöd till medarbetare för att ifrågasätta till exempel vid misstänkta ”VD-bedrägerier”.

Riktlinje 2.3.10: ny riktlinje rörande ej betrodda tillbehör.

Riktlinje 2.4.1: ny riktlinje rörande molntjänster där extern part är huvudman.

Riktlinje 2.4.2: ny riktlinje rörande molntjänster och uppgifter klassade med försumbar konfidentialitet.

Riktlinje 2.5.4: förtydligande om när känsliga personuppgifter får hanteras i okrypterad e-post.

Avsnitt 2.6: klargörande angående rätten att stoppa utskick, förtydligande att riktlinjerna endast avser massutskick

Riktlinje 2.6.1: ny riktlinje rörande massutskick.

Riktlinjer 2.6.9: ändring av e-postadress till IT-säkerhetsgruppen.

Riktlinje 2.7.1: omformulerad för att överensstämma med andra riktlinjer vid LiU.

Riktlinje 3.1.1: strykning av att prefekten ska kontakta kontoadministratör när ett konto ska avslutas.

Riktlinje 3.2.3: klargörande rörande när riktlinjen träder i kraft.

Kapitel 4, inledningen: ändring från ”ansvarsförbindelse” till ”blankett”.

Riktlinje 4.3.2: misstänkta oegentligheter ska rapporteras enligt gällande regelverk.

Riktlinje 4.3.3: ny riktlinje om att systemadministratörer ska rapportera misstänka personuppgiftsincidenter.

Riktlinje 4.4.2: ny riktlinje som förtydligar under vilka omständigheter LiU får ta del av studenters lagrade data.

Riktlinje 4.4.3: förtydligande att systemadministratörers särskilda rättigheter är begränsade till system som vederbörande ansvarar för.

Avsnitt 4.5, inledningen: ändring från ”ansvarsförbindelse” till ”blankett”.

Riktlinje 4.5.3: förtydligande att IT-säkerhetsgruppen har rätt att vidta åtgärder för att förebygga informationssäkerhetsincidenter.

Kapitel 5, inledningen: nya definitioner av informationsägare och informationstillgång, undantag om beslut från riktlinjerna ska dokumenteras. Klargörande kring när vissa riktlinjer träder i kraft.

Riktlinje 5.1.1: klargörande kring när riktlinjen träder i kraft.

Riktlinje 5.1.2: ny definition av informationsägare. Klargörande kring när riktlinjen träder i kraft.

Riktlinje 5.1.3: omformulerad.

Riktlinje 5.2.3: referens till annat regelverk tillagt.

Riktlinjer 5.3.1 och 5.3.2: nya riktlinje rörande användning av molntjänster..

Riktlinje 5.5.6: förtydligande av riktlinjen.

Riktlinje 5.5.9: förtydligande om hur personuppgiftsincidenter ska rapporteras.

Riktlinje 5.5.10: förtydligande kring överföring av personuppgifter till land utanför EU/EES.

Riktlinje 5.5.12: förtydligande kring när personuppgiftsbiträdesavtal krävs.

Riktlinje 5.6.1: förtydligande kring hur personuppgiftsincidenter ska rapporteras.

Riktlinje 5.6.2: utökad till att gälla andra fysiska tillgångar än IT-system.

Riktlinje 5.7.1: förtydligande angående att informationssäkerhetsplanen ska omfatta alla fysiska tillgångar, inte enbart IT-system.

Riktlinje 5.8.3: ny riktlinje rörande sekretessavtal för externa uppgradstagare, på begäran av rättsavdelningen.

Riktlinje 5.9.3: ny riktlinje rörande tillfälligt tillträde till lokaler.

Riktlinje 5.9.4 och 5.9.5: klargörande rörande huruvida LiU:s lokaler normalt uppfyller kraven.

Riktlinje 5.9.8: ny riktlinje rörande användning av värdeskåp för att uppfylla krav på inbrottsskydd och brandskydd.

Riktlinje 5.9.10: omformulerad.

Riktlinje 5.9.12: anpassning till ny klassningsmodell, förtydligande.

Riktlinje 6.1.1: förtydligande kring vad ”mobila enheter” är, omformulering, ny text rörande undantag.

Riktlinje 6.1.3: klargörande rörande när riktlinjen träder i kraft.

Riktlinje 6.2.4: listan över exempel utökad med översvämningsskydd och brandskydd.

Riktlinje 6.2.6: ny riktlinje rörande användning av IT-system.

Riktlinje 6.2.7: ny riktlinje rörande fjärradministration av IT-system.

Riktlinje 6.2.8: ny riktlinje rörande spårbarhet vid användning av datornät.

Riktlinje 6.3.1: klargörande rörande när riktlinjen träder i kraft.

Riktlinje 6.3.2: tidpunkten då system ska vara anpassade till ADFS har flyttats.

Riktlinje 6.3.3: ny riktlinje rörande lösenordskomplexitet.

Riktlinje 6.3.6: var tidigare sammanskriven med 6.3.5, har gjorts mindre restriktiv.

Riktlinje 6.3.8: tydliggjort att riktlinjen avser e-postklienter, klargörande rörande när riktlinjen träder i kraft.

Riktlinje 6.4.1: tillägg av inloggningar, inloggningsförsök, utloggningar, och förändringar av användare och behörigheter i listan över händelser som ska loggas; förtydligande att riktlinjen enbart berör vilka händelser som ska loggas.

Riktlinje 6.4.2: ny riktlinje rörande information i logghändelser.

Riktlinje 6.4.3: ny riktlinje rörande bevarande av loggar.

Riktlinje 6.5.2: anpassning till den nya klassningsmodellen.

Riktlinje 6.6.2: korrigerad hänvisning.

Riktlinje 6.7.1: riktlinjen tillämpas nu på alla tillgångar, inte enbart de med höjd riktighet eller konfidentialitet.

Avsnitt 6.9: nytt avsnitt med nya riktlinjer rörande systemutveckling.

Riktlinje 6.11.1: anpassning till den nya klassningsmodellen.

Ordlista: borttagning av ord som inte används längre, ny definition av indirekt identifiering, ny definition av informationsägare, ny definition av informationstillgång, anpassning till ny klassningsmodell.

Lagar, föreskrifter, förordningar, och riktlinjer: nytt avsnitt.