

Informationssäkerhetspolicy

Inledning

Universitetsledningen fastställde 2010-11-22 Ledningssystem för informationssäkerhet för Linköpings universitet. Detta dokument tar sin utgångspunkt i detta beslut.

Definitioner

Inom LIS används flera begrepp som är viktiga att förstå, se Ledningssystem för Informationssäkerhet (LIS) vid Linköpings universitet, för en mer omfattande företeckning av dessa.

Mål

Arbetet med informationssäkerhetsarbetet på LiU syftar till att säkerställa att universitetets informationstillgångar har optimal nivå av konfidentialitet, riktighet och tillgänglighet för verksamhetens behov. För att åstadkomma detta räcker det inte med enskilda tekniska åtgärder. Informationssäkerhetsarbetet utgår från ledningsnivån och omfattar alla anställda och studenter.

Omfattning och avgränsningar

Regler och riktlinjerna i detta dokument omfattar samtliga LiUs informationstillgångar, om inte annat anges i respektive kontrollåtgärd.

Organisation och ansvar

Rektor har det övergripande ansvaret för informationssäkerheten inom universitetet medan respektive objektägare har ansvaret för säkerheten i egna informationsbehandlandesystem.

För att hantera det dagliga informationssäkerhetsarbetet utses en **informationssäkerhetssamordnare**. Denne har det löpande ansvaret för såväl förebyggande arbete som implementering och uppföljning. Informationssäkerhetssamordnaren ansvarar för att årligen se över och vid behov föreslå förändringar av LiUs policy för informationssäkerhet. Som stöd för denna verksamhet används det LiU-övergripande rådet för IT och infrastruktur.

Informationssäkerhetssamordnaren har också befogenhet att besluta, eller delegera beslut, om åtgärder såsom avstängning från LiUs datornät för informationstillgångar som utgör ett hot mot informationssäkerheten.

Övervakning, loggning och utredning av intrång med mera uppdras till en IT-säkerhetsgrupp (**Incident Response Team, IRT**). Informationssäkerhetssamordnaren är beställare och följer arbetet i nära kontakt med utförarna.

IRT svarar för de kontakter med polis och övriga rättsvårdande myndigheter som föranleds av informationssäkerhetsarbetet. Universitets juristfunktion är här en stödjande funktion.

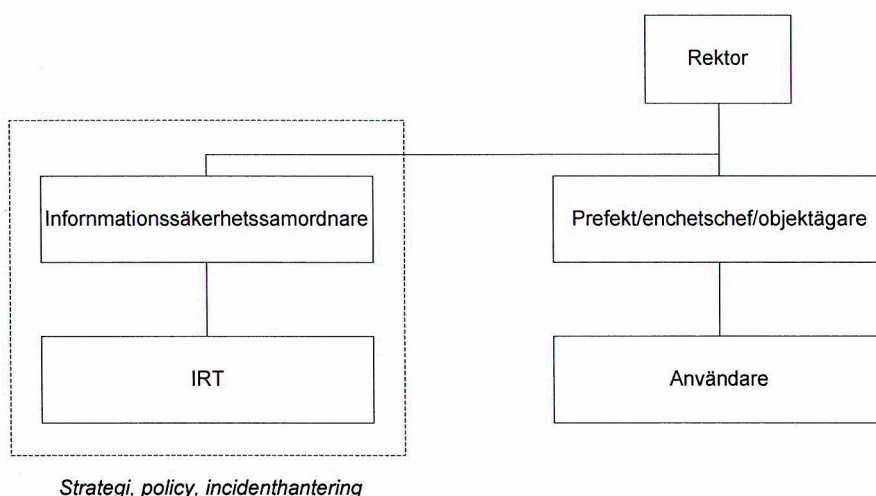
Inom varje institution/enhet är **prefekten**, enhetschefen eller motsvarande ansvarig för informationssäkerheten. Vid varje institution och annan enhet skall finnas en kontaktperson som medverkar i informations- och erfarenhetsutbyte i dessa frågor (se kontrollåtgärder för organisation av informationssäkerheten).

Prefekter och enhetschefer ansvarar för att personalen får nödvändiga kunskaper för att information och informationsbehandlande system skall kunna utnyttjas på ett säkert och effektivt sätt.

Prefekter och enhetschefer har möjlighet att delegera informationssäkerhetsarbetet genom att utse en objektägarrepresentant för varje informationstillgång (se Förvaltningsmodell för informationsbehandlande system vid Linköpings universitet, Dnr LiU-2010-01692).

Varje **objektägare** ansvarar för informationssäkerheten i det egna förvaltningsobjektet. Säkerhetsnivå och skyddsåtgärder skall fastställas utgående från bedömning av hotbilden och av konsekvenserna av störningar. Skyddsåtgärder skall väljas så att nyttan är rimlig i förhållande till kostnaderna för skyddet. Rutiner för förvaltning inklusive informationssäkerhetsarbete skall dokumenteras och uppdateras kontinuerligt.

Alla användare skall vara medvetna om informationssäkerhetsfrågornas betydelse och ha de kunskaper de behöver för att använda universitetets informationstillgångar på ett säkert sätt. Användare skall underteckna en särskild ansvarsförbindelse där de förbinder sig att följa universitetets regelverk för IT-användning.



Regler och riktlinjer

LiU-gemensamma kontrollåtgärder obligatoriska för samtliga informationstillgångar har utarbetats enligt bilagor.

Utöver de gemensamma kontrollåtgärderna skall objektägare i enlighet med ledningssystem för informationssäkerhet utfärda ytterligare kontrollåtgärder för respektive informationstillgång. Kontrollåtgärder kan baseras på ISO 27002:2005, alternativt kan egna åtgärder utarbetas. Valda åtgärder skall framgå av riskbehandlingsplan.

Objektförvaltningsmodell

För objekt som uppnår en sammanvägd informationsklass på betydande eller högre gäller att de ska förvaltas i enlighet med beslut Dnr LiU-2010-01692 . Detta ersätter inte behandling inom LIS utan Objektförvaltningsmodellen kompletterar LIS.

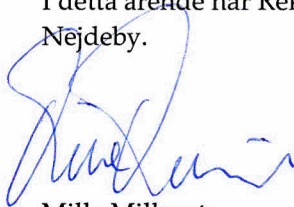
Rapportering och uppföljning

Informationssäkerhet är ett gemensamt ansvar och var och en har därför skyldighet att utan dröjsmål rapportera iakttagna säkerhetsbrister och incidenter (i enlighet med utfärdade regler för IT-användning). Nya hot och risker identifieras ständigt varför det är nödvändigt att fortlöpande aktivt arbeta för säkerheten. Informationssäkerhetssamordnaren har ansvar för att informationssäkerhetsarbetet inom institutioner och andra enheter följs upp och att erfarenhetsutbyte sker.

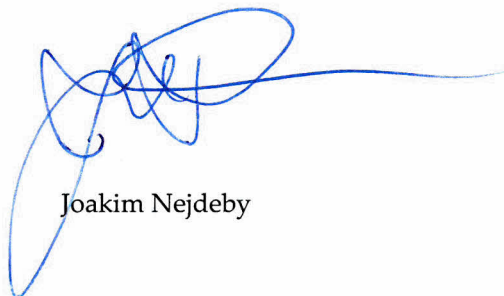
Informationssäkerhetsincidenter, så som t.ex. intrång, skall utan dröjsmål, rapporteras till IRT, som också skall bistå vid utredning och eventuella åtgärder. Vid gemensamma akuta informationssäkerhetsproblem skall alla institutioner och andra enheter medverka till skyndsam lösning.

Detta beslut ersätter det tidigare beslutet LiU Dnr LiU-2009-00857 och publiceras i LiUs regelverk.

I detta ärende har Rektor Mille Millnert beslutat efter föredragning av IT-direktör Joakim Nejdeby.



Mille Millnert



Joakim Nejdeby

Kopia till

Universitetsledningen
Fakulteterna
Institutionerna
Universitetsbiblioteket
Universitetsförvaltningen
LiU-IT

Bilaga 1.

Kontrollåtgärder för användares lösenordshantering

Ansvarig

Varje **användare** är ansvarig för att följa dessa regler och riktlinjer.

Inledning

En mycket viktig del i IT-säkerheten är att alla användare har bra lösenord som byts regelbundet. Vid förlust av ett lösenord kan tillförlitligheten och konfidentialiteten hos informationen i ett LiU övergripande system allvarligt äventyras.

Kontrollåtgärder

Dessa kontrollåtgärder gäller generellt för alla IT-system. Det finns system med särskilt höga säkerhetskrav som kan ha ytterligare krav som bestäms av respektive objektägare.

Olika lösenord

- Du bör inte använda samma lösenord till allting.
- Använd aldrig samma lösenord på universitetets system som du använder till webbtjänster på Internet. Använd aldrig samma lösenord på viktiga system med höga säkerhetskrav och mindre viktiga system.
- Det är även olämpligt att återanvända gamla lösenord. Hitta hellre på ett helt nytt för nya syften.

Bra lösenord

- Välj ett långt lösenord (minst 8 tecken, gärna längre).
- Använd en blandning av stora och små bokstäver, siffror och andra tecken (som " ! % & ").
- I system som tillåter ordentligt långa lösenord kan det vara ett bra alternativ att använda en hel fras (passphrase) bestående av många ord istället för ett kort lösenord. Frasen måste vara lika svårgissad som ett vanligt lösenord.
- Ytterligare ett alternativ är att hitta på en hel fras som ovan och sedan ta initialbokstäverna i varje ord, samt krydda med lite siffror och/eller specialtecken.
- Använd enbart a-z och A-Z bland bokstäverna, eftersom vissa system har problem med "svenska tecken" (åäöÅÄÖ) med mera.

Dåliga lösenord

- Undvik teckenkombinationer som ligger i lättgissade mönster på tangentbordet (till exempel "qwerty", "asdfgh", "1234567890") eller är ordnade på annat enkelt sätt ("abcdefghijklmnopqrstuvwxyz").
- Undvik ord eller namn. Dessa finns nämligen med i de ordlistor som används av de som försöker gissa lösenord.
- Undvik lösenord som kan gissas om man vet något om dig (till exempel användarnamn, eget namn, namn på anhöriga, namn på husdjur, registreringsnummer, telefonnummer, personnummer).

- Lägg inte bara till en siffra först eller sist i ett i övrigt lättgissat lösenord.
- Byt inte bara ut tecken mot "liknande" (till exempel "gr33n" istället för "green") i ett i övrigt lättgissat lösenord.

Byta lösenord

- Lösenord skall bytas direkt om det finns misstanke om att någon obehörig fått tillgång till det. Detta gäller också om din dator där du använt lösenordet blivit stulen. Diskutera också det som hänt med den IT-säkerhetsansvarige på din institution eller enhet.
- Lösenord bör bytas ibland för att minska risken att lösenord som stulits eller gissats kan fortsätta att användas, även om inga konkreta misstankar finns. I det flesta system som inte har särskilda krav är det lämpligt att byta en gång per år.

Avslöja lösenord

- Ingen person skall fråga dig efter ditt lösenord (via telefon, e-post eller på annat sätt). Detta gäller även systempersonal på universitetet. Om detta inträffar ändå: vägra att uppge ditt lösenord och rapportera genast händelsen till den IT-säkerhetsansvarige på din institution eller enhet.
- Skicka aldrig lösenord osäkert via e-post, chat eller liknande tjänster. Det finns risk att det hamnar hos fel mottagare eller att någon snappar upp det på vägen.

Bilaga 2.

Kontrollåtgärder för VPN-användning

Ansvarig

Varje användare är ansvarig för att följa dessa regler och riktlinjer.

Inledning

Tillträde till universitets IT-resurser genom uppkoppling via VPN (Virtuellt Privat Nätverk) innebär att den enskilde användaren själv måste ansvara för att säkerheten upprätthålls.

Kontrollåtgärder

Följande gäller för all VPN-användning:

- VPN-kontot är personligt och får inte upplåtas till annan person.
- Datorn måste uppfylla kraven i "Kontrollåtgärder för antivirus och annan skadlig programvara".
- Datorn skall hållas uppdaterad vad avser säkerhetsuppdateringar och liknande.
- Den VPN-programvara som universitetet tillhandahåller eller anvisar skall användas för uppkopplingen.
- VPN-anslutningen bör kopplas ned när den inte behövs.
- Datorn måste hållas säker även under de perioder då den inte är uppkopplad via VPN.
- Objektägare kan besluta att ytterligare villkor ska gälla för tillträde till särskilt känsliga system.

Bilaga 3.

Kontrollåtgärder för säkerhet i enskilda datorsystem

Ansvarig

Varje **objektägare** är ansvarig för att följande åtgärder verkställs. Saknas utsedd objektägare så är **prefekt** ansvarig.

Inledning

Varje dator som är ansluten till Linköpings universitets nätverk har betydelse för IT-säkerheten i stort. Felaktigt installerade datorer och datorer som inte uppdaterats med säkerhetsuppdateringar från programvaruleverantörer utgör ett hot mot resten av nätverket. Detta gäller serversystem men också enskilda persondatorer, vilket innebär att kraven ökar på en aktiv förvaltning av samtliga datorsystem.

Även annan utrustning, såsom skrivare, scanners, videokonferenssystem, avancerade mobiltelefoner med mera, som ansluts till nätverket kan påverka säkerheten. Det som sägs nedan om datorer gäller i tillämpliga delar även sådan utrustning.

De som sköter datorer och annan utrustning måste därför ha kompetens för detta och måste kontinuerligt hålla sig informerade om hotbilder och åtgärder mot dessa.

Kontrollåtgärder

- Vid inköp av datorer och programvara skall hänsyn alltid tas till IT-säkerhetsaspekter i god tid.
- Datorer på universitetets nätverk samt programvaran på dessa skall installeras på ett sådant sätt att onödiga risker inte uppstår.
- Datorerna skall kontinuerligt uppdateras med de säkerhetsuppdateringar som leverantörer av operativsystem, tillämpningar med mera gör tillgängliga.
- Programvaror och tjänster som inte används skall stängas av. Detta är särskilt viktigt för server-datorer.
- Medföljande brandväggsprogramvara på datorerna bör användas för att minska riskerna för otillbörlig åtkomst.
- Utrustning och programvara som inte hålls uppdaterad och säker skall kopplas bort från universitets nätverk.

Bilaga 4.

Kontrollåtgärder för identifiering av användare

Ansvarig

Varje **objektägare** är ansvarig för att följande åtgärder verkställs. Saknas utsedd objektägare så är **prefekt** ansvarig.

Inledning

För att upprätthålla IT-säkerheten har universitetet ett behov av att kunna identifiera vem som använder datorer och nät. Det finns också ett behov av att kunna spåra enskilda datorer i samband med intrång, virusangrepp och liknande.

I "Regler för tillåten användning av SUNET" finns dessutom följande bestämmelse:

"En organisation som använder SUNET via publika terminaler skall tillse att det finns ett system för identifiering av användarna av de publika terminalerna."

Kontrollåtgärder

- I samband med att konto för inloggning utdelas skall i normalfallet legitimation avkrävas. Även i de fall systempersonal återställer borttappat lösenord skall legitimation avkrävas.
- Nätanslutna datorer skall ha inloggningssystem som kräver inloggning med personligt konto.

Bilaga 5.

Kontrollåtgärder för behörighetshantering

Dessa regler och riktlinjer utgör Linköpings universitets anpassning av följande kontrollåtgärder enligt ISO 27002:2005: 11.2.1, 11.2.2, 11.2.4

Ansvarig

Varje **objektägare** är ansvarig för att följande åtgärder verkställs. Saknas utsedd objektägare så är **prefekt** ansvarig.

Inledning

Inom Linköpings universitet förekommer en stor mängd informationstillgångar. Skyddsbehovet för den information som hanteras avgör vilka rutiner för behörighetshantering som skall gälla.

Kontrollåtgärder

För **alla** typer av behörigheter gäller att:

- Behörigheter skall upphöra om anställning, studier eller annat uppdrag vid Linköpings universitet upphör. Behörighet kan förlängas efter särskilt beslut.
- Behörigheter bör återkallas med automatik. Om automatiskt återkallande av behörighet inte är möjlig så skall objektägare tillse att det finns rutiner för gallring av behörighet i samband med att uppdrag upphör.
- Behörigheter skall baseras på en unik användaridentitet. Studenter ges särskild användaridentitet vilket innebär att individ som är både student och anställd kan ha två användaridentiteter.

För informationssystem som innehåller **personuppgifter** eller är klassad enligt **konfidentialitet allvarlig eller betydande**, eller, **riktighet allvarlig eller betydande** gäller att:

- Verksamma vid universitetet bör endast ha tillgång till de uppgifter som var och en behöver för sin anställning, forskning eller studier. Detta gäller även om informationen i sig är offentlig.
- En formell och dokumenterad rutin skall gälla för tilldelande och återtagande av behörigheter
- Revision av aktiva behörigheter skall ske minst var 12:e månad.
- Behörighet skall upphöra då det uppdrag som ursprungligen motiverat behörigheten upphör.
- Den som tilldelas en behörighet skall särskilt informeras om rutiner för hantering av behörigheten och information som tillgängliggörs genom behörigheten.

För informationssystem klassade enligt **konfidentialitet allvarlig**, eller, **riktighet allvarlig** gäller att:

- Tvåfaktorausentisering skall användas vid inloggning av systemförvaltare och systemadministratörer.

Bilaga 6.

Kontrollåtgärder för loggning och behandlingshistorik

Dessa regler och riktlinjer utgör Linköpings universitets anpassning av följande kontrollåtgärder enligt ISO 27002:2005: 10.10.1, 10.10.2, 10.10.3, 10.10.6, 15.1.4

Ansvarig

Varje **objektägare** är ansvarig för att följande åtgärder verkställs. Saknas utsedd objektägare så är **prefekt** ansvarig.

Kontrollåtgärder

Där annat inte framgår gäller respektive åtgärd för samtliga informationsbehandlande system.

Systemloggar

Relevant loggning av systemhändelser i operativsystem och systemnära programvara utgör en viktig förutsättning för upptäckt och utredning av informationssäkerhetsincidenter. Eftersom intrång på ett system kan utgöra språngbräda för attack mot andra system gäller följande:

- Alla nätverksanslutna servertjänster skall utnyttja vedertagen funktionalitet för loggning som tillhandahålls av respektive operativsystem och programvara.

Behandlingshistorik

Med behandlingshistorik menas här loggning av användaraktiviteter i ett informationssystem.

- För system som hanterar information klassad enligt **konfidentialitet allvarlig eller betydande** skall behandlingshistorik registreras när uppgift tas fram ur systemet. Minst följande skall loggas:
 - Användaridentitet
 - Tidsstämpel
 - Nätverksadress
 - Vilken uppgift som har lästs ut
- För system som hanterar information klassad enligt **Integritet allvarlig eller betydande** skall behandlingshistorik registreras när en uppgift ändras eller matas in i systemet. Minst följande skall loggas:
 - Användaridentitet
 - Tidsstämpel
 - Nätverksadress
 - Vilken inmatning eller uppdatering som har gjorts

Övervakning av loggar

- Loggar bör övervakas regelbundet med manuell inspektion och/eller automatiska metoder.
- System som förvaltas enligt universitets objektförvaltningsmodell skall dokumentera rutiner för övervakning och granskning av loggar. Sådana rutiner skall hanteras konfidentiellt.

Skydd av loggar

- För att skydda loggfiler mot obehöriga ändringar skall dessa skrivas till ett särskilt system (loggserver) separerat från det som loggas. Normal användning av loggserver skall ej medge behörighet att modifiera redan skrivna loggar. Loggning till loggserver utesluter inte lokal loggning inom det egna systemet.

För särskilt skyddsvärda system gäller dessutom följande för loggar skyddade enligt ovanstående punkt:

- För system klassificerade enligt nivåer **konfidentialitet allvarlig eller betydande, riktighet allvarlig eller betydande** gäller följande:
Samma individ som administrerar server eller förvaltar system skall ej ha behörighet att modifiera redan skrivna loggar, ej heller ha möjlighet att genomföra gallring av skrivna loggar.
- För system klassificerade enligt nivåer **konfidentialitet allvarlig eller betydande** gäller:
Behörighet att läsa loggar för systemet bör endast ges den som administrerar systemets server eller förvaltar systemets applikation samt driftansvariga för loggserver.

Klocksynchronisering

För att loggar skall vara korrekta är det viktigt att datorklockor är rätt ställda. Korrekta tidsangivelser i loggfiler underlättar analys av loggar samt stärker tilltron till desamma då loggen används som bevis.

- Systemklockor skall vara synkroniserade. Synkronisering bör ske genom användning av ett nätverkstidsprotokoll.

Personlig integritet och loggdata

Loggfiler kan innehålla integritetskänsliga personuppgifter. Rutiner för gallring av loggar skall därför finnas för alla system.

- Hur länge loggfiler behöver sparas måste avgöras från fall till fall. Om det inte finns synnerliga skäl för att spara loggarna kortare eller längre tid så bör loggfiler sparas minst 12 och max 24 månader.

Bilaga 7.

Kontrollåtgärder för kryptering av datatrafik

Ansvarig

Varje **objektägare** är ansvarig för att följande åtgärder verkställs. Saknas utsedd objektägare så är **prefekt** ansvarig.

Inledning

Varje objektägare ansvarar för säkerheten i egna system. Säkerhetsnivå och skyddsåtgärder skall fastställas utgående från bedömning av hotbilden och av konsekvenserna av störningar. Skyddsåtgärder skall väljas så att nyttan är rimlig i förhållande till kostnaderna för skyddet.

Trafik i datornätverk kan avlyssnas med mycket enkla medel, t.ex. finns allmänt tillgänglig programvara som explicit söker efter logginnamn/lösenord, vilket medför att okrypterade lösenord över datornätverk i princip kan likställas med att systemet i fråga är helt oskyddat. Observera att e-post normalt överförs okrypterat.

Det finns flera tekniska möjligheter för att kryptera datatrafik och IT-säkerhetsamordnaren erbjuder råd vid behov.

Kontrollåtgärder

- Inloggningsinformation (lösenord och liknande) skall alltid överföras krypterat.
- Skyddsvärda data bör alltid överföras krypterat. Vad som är skyddsvärt måste bedömas av den enskilde objektägaren. Några exempel är:
 - Sekretessbelagda data
 - Personuppgifter
 - Ännu ej given tentamen
 - Data i samband med företagssamarbete

Bilaga 8.

Kontrollåtgärder för säkerhetskopiering

Ansvarig

Varje **objektägare** är ansvarig för att följande åtgärder verkställs. Saknas utsedd objektägare så är **prefekt** ansvarig.

Inledning

En mycket stor del av universitetets information finns lagrad på olika typer av datamedia. Förlust eller skada på informationen genom tekniska problem, stöld av utrustning eller andra oönskade händelser kan medföra stora skador för universitetet, både ekonomiskt, arbetsmässigt och för LiUs varumärke.

Kontrollåtgärder

- Säkerhetskopiering skall ske av väsentlig information, såväl på servrar som arbetsstationer
- Säkerhetskopiorna skall förvaras väl skyddade från stöld, skada och obehörig åtkomst.
- Det skall finnas kopior "off-line" (ej åtkomliga och modifierbara utan fysisk åtkomst till media) av viktig information.
- Skriftliga rutiner för säkerhetskopiering skall finnas inom samtliga institutioner och andra enheter

För användare rekommenderas att man använder fillagertjänst med inbyggd säkerhetskopiering för att uppfylla ovanstående krav.

Bilaga 9.

Kontrollåtgärd för antivirus

Ansvarig

Varje **objektägare** är ansvarig för att följande åtgärder verkställs. Saknas utsedd objektägare så är **prefekt** ansvarig.

I det fall en hemdator används för att använda informationssystem vid universitetet är **respektive användare** ansvarig för att tillse att datorn har relevant skydd enligt detta regelverk.

Inledning

Virus och elak kod (datorprogram som installeras utan samtycke i skadligt syfte) medför risker som måste hanteras.

Kontrollåtgärder

- Antivirus skall finnas installerat i alla nätanslutna virushotade datormiljöer (klientdatorer anses normalt alltid som virushotade).
- Antivirus skall uppdateras automatiskt och ofta (minst dagligen om nätanslutning finns).

För att hantera risken med skadlig programvara gäller följande:

- Datorer som misstänks vara infekterade med elak kod skall kopplas bort från nätverket och kontrolleras med ett uppdaterat antivirusprogram.
- Om en dator visar sig vara infekterad med elak kod skall detta omgående rapporteras till Incident Response Team (IRT).

Bilaga 10.

Kontrollåtgärder för radering av hårddiskar och andra datamedia

Ansvarig

Varje **objektägare** är ansvarig för att följande åtgärder verkställs. Saknas utsedd objektägare så är **prefekt** ansvarig.

Inledning

Det finns många skäl att se till att hårddiskar och andra datamedia inte lämnas vidare utan att innehållet på dem raderats eller på annat sätt gjorts oläsligt.

På hårddiskar från datorer är det troligt att det finns lösenord, inställningsfiler med mera, som inte får spridas till obehöriga, därför att det kan äventyra IT-säkerheten. En uppenbar anledning är också att det kan finnas känsliga verksamhetsuppgifter lagrade, som inte får bli offentliga. Det är också möjligt att det på hårddiskar finns program installerade, vars licensvillkor inte tillåter att de används utanför universitetets verksamhet.

Kontrollåtgärder

- Hårddiskar skall raderas (med programvara som skriver över innehållet ett flertal gånger med olika datamönster) innan de överlätes till utomstående eller kasseras.
- Om så inte kan ske skall de förstöras fysiskt på ett sätt som omöjliggör återläsning av informationen.
- Ovanstående kan utföras av personal på universitetet eller genom skriftligt avtal med företag som tar hand om utrustningen för skrotning.
- Samma regler gäller för andra datamedia (USB-minnen, CD/DVD-skivor, band, disketter med mera) om det kan antas finnas känslig information på dem.

Innehåller datamediet allmänna handlingar kan det vara fråga om gallring (förstörelse) i lagens mening. Gallring kräver att det finns beslut om att uppgifterna kan tas bort.

Bilaga 11

Kontrollåtgärder för nätverkssäkerhet

Ansvarig

IT-direktören är ansvarig för att följande åtgärder verkställs.

Inledning

LiUs datornätverk utgör en av de mest basala infrastrukturkomponenterna och utgör därför en betydande informationstillgång.

Universitetet är anslutet till SUNET (Swedish University Network) och är därmed skyldigt att följa SUNET:s regler (<http://www.sunet.se/>).

Kontrollåtgärder

- Trådlöst nätverk och publika nätverksuttag skall ha system som verifierar användaridentitet innan åtkomst ges till nätverket.
- Nätverk skall övervakas så att datorer kan spåras till det uttag de är eller varit inkopplade i.
- LiU:s datornät skall övervakas med målsättning att upptäcka informationssäkerhetsincidenter. Rutiner för detta skall underhållas inom uppdraget för IRT och hållas konfidentiella.

Bilaga 12

Kontrollåtgärder för e-postservrar

Ansvarig

Varje **objektägare** är ansvarig för att följande åtgärder verkställs. Saknas utsedd objektägare så är **prefekt** ansvarig.

Inledning

E-post är ett viktigt arbetsredskap på universitetet. För att detta ska fungera måste eposten skyddas från virus (och annan elak kod) och spam.

Kontrollåtgärder

- E-postservrar som används av användare med virushotad datormiljö skall ha antivirusfiltrering av e-posten.
- E-postservrar som är åtkomliga utifrån Internet skall ha fungerande reläskydd som ser till att de inte kan missbrukas för spamskickande.
- E-postservrar som är åtkomliga utifrån Internet skall använda aktuella spamskyddstekniker för att begränsa inkommande spam.
- E-postservrar skall för varje meddelande som förmedlas logga följande (notera särskilt kontrollåtgärder för gallring av loggar):
 - Avsändande e-postadress
 - Mottagande e-postadress
 - Nätverksadresser för servrar nyttjade för överföringen
 - Tidsstämpel
 - Message-ID

Informationssäkerhetssamordnaren (eller de som uppgiften delegerats till) har rätt att bestämma vilka e-postservrar som får vara åtkomliga utifrån Internet.

Bilaga 13

Kontrollåtgärder för fysiskt skydd av tekniska lokaler

Dessa regler och riktlinjer utgör Linköpings universitets anpassning av följande kontrollåtgärder enligt ISO 27002:2005: 9.1.1, 9.1.2.

Ansvarig

Varje **objektägare** är ansvarig för att följande åtgärder verkställs. Saknas utsedd objektägare så är **prefekt** ansvarig.

Med "teknisk lokal" menas i denna text lokaler som inhyser infrastruktur för informationsbehandlande system. Exempel på sådana lokaler är datorhallar, korskopplingsrum och arkiv. Följande riktlinjer gäller för lokaler som inhyser informationsbehandlande system klassificerade som varandes av informationsklass **betydande eller högre** ur något av de tre perspektiven **konfidentialitet, riktighet och tillgänglighet**.

Skalskydd

- Lokalen bör lägst uppfylla säkerhetsklass SSF 200:3 nivå 2 med avseende på fysiskt intrång.
- Inbrottslarm skall finnas och bör uppfylla krav för gällande larmklass enligt SSF 130
- Informationsbehandlingsresurser som hanteras av organisationen bör fysiskt åtskiljas från sådana som hanteras av tredje part. (ISO 27002:2005, 9.1.1 g)

Tillträdeskontroll

Lokaler skall skyddas genom tillträdeskontroller för att säkerställa att endast behörig personal ges tillträde.

- Tillträde skall styras, t.ex. genom användning av LiU-kort tillsammans med PIN-kod. Allt tillträde skall loggas och logg skall förvaras säkert.
- Behörighet för eget tillträde ges endast person som behöver detta för att fullgöra ett uppdrag åt Linköpings universitet. Behörighet skall upphöra när uppdraget upphör eller inte längre förutsätter egen behörighet
- Beviljande av behörigheter för tillträde skall dokumenteras skriftligen.
- Behörigheter för tillträde skall revideras minst var 12:e månad.
- Vid tillträde för besökare skall denna eskorteras av behörig personal.
- Vid tillträde för servicepersonal skall denna eskorteras av behörig personal. Om servicepersonal lämnas ensam i lokalen skall detta endast ske efter särskilt godkännande av ansvarig för lokalen. Sådant godkännande skall dokumenteras.

Brandskydd

- Brandlarm skall finnas och bör uppfylla krav enligt SBF 110.

Bilaga 14

Kontrollåtgärder för hantering av informationssäkerhetsincidenter

Dessa regler och riktlinjer utgör Linköpings universitets anpassning av följande kontrollåtgärder enligt ISO 27002:2005: 13.1.1, 13.1.2, 13.2.2, 13.2.3

Ansvarig

Dessa kontrollåtgärder pekar ut ansvar för **användare, informationssäkerhetsansvariga** vid institution/enhet och IRT.

Inledning och definitioner

Med **informationssäkerhetsincident** menas här en enskild eller en serie oönskade eller oväntade händelser vilka med stor sannolikhet kan äventyra verksamhet och hota informationssäkerheten.

En informationssäkerhetsincident kan antingen vara orsak av en **avsiktlig attack** eller en **oavsiktlig händelse**. Med avsiktlig attack menas en händelse som individ eller organisation avsiktligt iscensatt, exempelvis intrång, sabotage eller stöld. Analogt är en oavsiktlig händelse som något som sker utan uppsåt, exempelvis till följd av olyckshändelse, slarv eller naturfenomen.

Snabb respons på informationssäkerhetsincidenter är avgörande för att minimera skada för verksamheten samt undvika

Kontrollåtgärder

Rapportering av informationssäkerhetsincidenter

- Informationssäkerhetsincidenter där avsiktlig attack ej går att utesluta skall alltid rapporteras till IRT.
- Incidenter som orsakats av oavsiktliga händelser skall rapporteras till IRT om dessa påverkat informationstillgång med sammanvägd klassificering **betydande eller högre**.
- IRT skall underhålla mallar och rutiner för rapportering av informationssäkerhetsincidenter

Att lära av informationssäkerhetsincidenter

Inträffade incidenter utgör en komponent i arbete med riskanalyser och utgör ett underlag till granskning av LIS. Informationsspridning av inträffade incidenter kan allmänt sett vara en väg att sprida kunskap om informationssäkerhet samt ge underlag för förbättrade rutiner.

- IRT skall halvårsvis sammanställa rapporter över inträffade incidenter. Incidenter som av säkerhetsskäl är olämpliga att publicera skall utelämnas i dessa rapporter.

Rapportering och test av säkerhetsbrister

- Varje anställd eller annan uppdragstagare skall rapportera misstänkta säkerhetsbrister i informationssystem eller tjänster. Rapportering sker till informationssäkerhetsansvarig inom respektive institution/ enhet eller till IRT.
- Vid mottagande om rapport av misstänkt säkerhetsbrist skall informationssäkerhetsansvarig vid institution eller annan enhet informera IRT och vice versa.
- Det är inte tillåtet för anställd eller annan uppdragstagare att testa säkerhetsbrister i informationsbehandlande system utan föregående medgivande från objektägare.
- IRT har rätt att utan förvarning eller medgivande testa säkerhetsbrister samt genomföra penetrationstester om det kan göras sannolikt att sådant test i sig inte hotar riktighet eller tillgänglighet i information. Utan skriftligt medgivande får sådant test endast ske mot system som är under Linköpings universitets kontroll.
- IRT skall rutinemässigt genomföra tester av säkerhetsbrister. Dokumenterade rutiner för detta skall finnas och hållas konfidentiella.
- Av IRT upptäckta, eller till IRT inrapporterade, säkerhetsbrister skall omgående rapporteras till informationssäkerhetsansvarig på respektive institution/enhet. Allvarigare brister rapporteras också till informationssäkerhetssamordnaren.

Utredning av informationssäkerhetsincidenter

I det akuta skede då en informationssäkerhetsincident utreds står det ofta inte klart om händelsen kommer att leda till polisanmälan eller rättslig prövning. Tills detta har uteslutits skall material hanteras på ett sådant sätt att bevisvärde av hanterat material inte riskeras.

Detta innebär att:

- Dagbok skall föras av den som utreder incidenten.
- Material som kan komma att användas som bevis i rättslig prövning skall lagras och behandlas så att god spårbarhet tydliggörs. Detta innebär att:
 - Eventuell forensisk utredning görs på kopia av materialet (till exempel klon av hårddisk)
 - Originaldokument och datamedia skall förvaras under former som säkerställer att manipulation ej skett samt att tillgänglighet till materialet inte riskeras. Särskilda säkerhetspåsar för det förra ändamålet kan rekvideras genom IRT.
 - Material bör sparas i 18 månader.

Bilaga 15

Kontrollåtgärder för personalresurser och säkerhet

Ansvarig

Varje **prefekt eller motsvarande** är ansvarig för att följande åtgärder verkställs.

Inledning

Det är viktigt att säkerställa att medarbetare och uppdragstagare förstår sitt ansvar och är lämpliga för de roller de avses ha och för att minska risken för stöld, bedrägeri eller missbruk av resurser.

Var och en ansvarar för säkerhet i samband med sin egen datoranvändning. LiU-gemensamma regler klargör hur universitetets allmänna IT-resurser får utnyttjas (återfinns i både svensk och engelsk version på <http://regelverk.liu.se/innehft/> under fliken Lokala regelsamlingen/IT/Regler för IT användning vid LiU).

Kontrollåtgärder

Roller och ansvar

- Alla medarbetare och uppdragstagare skall underteckna regler för anställdas användning av dator-, nät- och systemresurser vid Linköpings universitet
- Alla systemförvaltare, systemadministratörer och uppdragstagare med denna typ av arbetsuppgifter skall underteckna "Användning av dator-, nät- och systemresurser vid Linköpings universitet – ansvar, rättigheter och skyldigheter för systemadministratörer"

Åtgärder vid brott mot informationssäkerhetspolicy

- Informationssäkerhetsansvarig skall utan dröjsmål rapportera upptäckta brott mot informationssäkerhetspolicy till prefekt/enhetschef och IRT.
- IRT skall rapportera upptäckta brott mot informationssäkerhetspolicy till informationssäkerhetsansvarig vid berörd institution/enhet.
- IRT skall rapportera informationssäkerhetsincidenter till informationssäkerhetssamordnaren som vid allvarliga fall skall informera universitetsledningen (se kontrollåtgärder för hantering av informationssäkerhetsincidenter). Vad som utgör allvarligt bedöms från fall till fall.

Åtgärder vid anställnings upphörande

- Då anställning upphör skall normalt alla tidigare uthämtade informationstillgångar (t.ex. programvara, dokument, datautrustning, kreditkort, LiU-kort) återlämnas.
- Om prefekt beslutar att en medarbetare som slutar får behålla utrustning skall denna rensas på information enligt kontrollåtgärder för radering av hårddiskar och andra datamedia.