Exp 10/12-02 /y

LINKÖPINGS UNIVERSITET
Vicerektor för IT-frågor

BESLUT
2002-12-03

Dnr LiU 1686/02-14

IT-säkerhet vid Linköpings universitet

Inledning

Universitetsstyrelsen beslutade 2002-02-27 fastställa IT-strategi för Linköpings universitet. Där fastslås att modern informations- och kommunikationsteknik skall möjliggöra och främja universitetets övergripande mål. IT-resurser utgör viktiga verktyg inom samtliga verksamheter inom universitetet och det är således helt nödvändigt att såväl studenter, forskare, lärare och övriga anställda kan lita på de resurser som ställs till förfogande.

IT-säkerhet är ett antal åtgärder med syfte att förebygga och minimera konsekvenserna av oönskade händelser. Detta dokument skall klargöra för universitetets personal och studenter vilka mål som finns för IT-säkerheten och hur dessa kan uppnås.

Mål

IT-säkerhetsarbetet skall utgå från att universitetet även fortsättningsvis skall utgöra en öppen miljö där institutioner och enheter har stora möjligheter att utforma sitt egna IT-stöd. Med kännedom om den ständigt förändrade hotbilden mot system och information är det nödvändigt att vidta IT-säkerhetsåtgärder som i vissa fall kan komma att inskränka öppenheten.

IT-säkerhetsarbetet skall ha som mål att anställda och studenter skall kunna använda IT-resurser utan oönskade störningar och med hög grad av

- tillgänglighet
- tillförlitlighet
- sekretess

Organisation

Universitetsledningen har det övergripande ansvaret för IT-säkerheten inom universitetet medan respektive systemägare själv har ansvaret för säkerheten i egna system. Ledningsnivån utgörs i dessa frågor av vicerektor för informationsteknikens tillämpning (IT-vicerektor). En särskilt utsedd IT-säkerhetschef inom rektorskansliet har det löpande ansvaret för såväl förebyggande arbete som implementering och uppföljning. Denne har också befogenhet att besluta om åtgärder såsom avstängning från nätet av IT-resurser som utgör ett hot mot säkerhet i datornät och datasystem. Universitetets juristfunktion svarar för de kontakter med polis och övriga rättsvårdande myndigheter som föranleds av IT-säkerhetsarbetet.

Universitetets IT-enhet (UNIT) har i uppdrag att utgöra kompetenscentrum i IT-frågor innefattande även säkerhetsfrågor. Verksamheten inom UNIT skall drivas med säkerheten i fokus och med aktivt deltagande i förebyggande IT-säkerhetsarbete. Det är också önskvärt att universitetets institutioner och enheter kan få råd och stöd i det egna IT-säkerhetsarbetet.

Övervakning, loggning och utredning av intrång mm uppdras (i separat dokument) till ”Incident Response Team” inom UNIT (IRT). IT-säkerhetschefen är beställare och följer arbetet i nära kontakt med utförarna.

Inom varje institution/arbetsenhet är prefekten/enhetschefen ansvarig för IT-säkerheten. Säkerhetsarbete kan utföras av anställda inom institutionen alternativt upphandlas. Vid varje institution/enhet skall finnas en kontaktperson i IT-säkerhetsfrågor som kan medverka i information och erfarenhetsutbyte i dessa frågor.

Intrång och andra incidenter skall rapporteras till IRT, som också kan bistå vid utredning och eventuella åtgärder. På samma sätt förväntas tillgänglig teknisk expertis inom institutioner och enheter medverka till att lösa gemensamma akuta säkerhetsproblem.

Som stöd för IT-säkerhetsfunktionens verksamhet finns Centrala säkerhetsgruppen (CSG) med IT-vicerektor som ordförande. Gruppen skall svara för information, policyskapande mm för all IT-säkerhetsverksamhet inom universitetet.

Ansvar
a) Systemägare
Varje systemägare ansvarar för säkerheten i egna system. Säkerhetsnivå och skyddsåtgärder skall fastställas utgående från bedömning av hotbilden och av konsekvenserna av störningar. Skyddsåtgärder ska väljas så att nyttan är rimlig i förhållande till kostnaderna för skyddet. Rutiner för förvaltning och datasäkerhetsarbete bör dokumenteras och kontinuerligt aktualiseras.
b) Prefekter och enhetschefer
Prefekter och enhetschefer ansvarar för att personalen inom enheten får nödvändiga kunskaper för att IT-hjälpmedel skall kunna utnyttjas på ett säkert och effektivt sätt.
c) Alla användare
Alla anställda skall vara medvetna om IT-säkerhetsfrågornas betydelse så att de kan ta ansvar för att den personliga IT-användningen kan ske med bibehållande av god säkerhet.
Alla användare skall ha tillgång till informationsmaterial så att de kan ta eget ansvar för IT-säkerheten vid den personliga IT-användningen.

Regler och riktlinjer
Universitetet är anslutet till SUNET (Swedish University Network) och är därmed skyldigt att följa SUNET:s regler (http://www.sunet.se) . Därutöver har följande lokala regler utarbetats för användningen av LiU:s IT-resurser:

a) användning
Var och en ansvarar för säkerhet i samband med egen datoranvändning. Lokala regler klargör hur LiU:s allmänna IT-resurser får utnyttjas (återfinns i http://regelverk.liu.se/innehft/ under fliken Lokala regelsamlingen/Information och dokumentation):
Ansvarsförbindelse för användning av dator-, nät- och systemresurser vid Linköpings universitet (regler och ansvarsförbindelse för studenter)
Regler för anställdas användning av dator-, nät- och systemresurser vid Linköpings universitet
Användning av dator-, nät- och systemresurser vid Linköpings universitet – ansvar, rättigheter och skyldigheter för systemadministratörer

Därutöver kan prefekt/systemägare utfärda anvisningar för egna system. Respektive prefekt/systemägare ansvarar för information om förekomsten av sådana anvisningar.

b) drift av nät och servrar
Nät- och serverutrustning som ansluts till universitetets nät kan utgöra en säkerhetsrisk om drift och underhåll åsidosätts. Det är nödvändigt att enheter som driver egna system har kompetens att utarbeta riktlinjer för och verkställa en aktiv förvaltning av dessa. Särskilda föreskrifter finns för:
Säkerhet för enskilda datorsystem
Kryptering av datatrafik
Epostservrar
Identifiering av användare

c) lokala resurser
Varje användare av IT-resurser bör känna trygghet att den egna informationen kan uppfylla krav på tillgänglighet, tillförlitlighet och sekretess. Detta gäller såväl stationär utrustning på arbetsplatsen som eventuell bärbar utrustning. För detta ändamål finns fastställda krav på:
Säkerhet för enskilda datorsystem
Virusskydd
Säkerhetskopiering

d) utbildning och information
IT-resurser blir allt viktigare verktyg inom universitetets verksamhet. Det är nödvändigt att anställda och studenter har tillgång till utbildning och information för åstadkommande av effektiv och säker IT-användning. Universitetet tillhandahåller utbildning för de vanligaste verktygen och det ankommer på prefekter och enhetschefer att motivera anställda att ta del av dessa liksom studenter bör uppmuntras att utnyttja de läromedel som tillhandahålls.

Systemägare kan föreskriva att användare måste ha genomgått viss utbildning.

Regler och viktig information bör finnas lätt tillgänglig via www och information om säkerhetshöjande åtgärder skall utarbetas och publiceras.

Upphandling
Vid upphandling och utveckling av IT-system och IT-tjänster skall säkerhetsaspekter beaktas.

Konsulter och andra externa användare
När konsulter och andra externa användare ges tillgång till universitetets IT-resurser skall universitetet genom avtal försäkra sig om att användningen sker i enlighet med universitetets regler och med upprätthållande av god säkerhet.

Rapportering och uppföljning
IT-säkerhet är ett gemensamt ansvar och var och en har därför skyldighet att rapportera iakttagna risker 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. IT-säkerhetschefen har ansvar för uppföljning av IT-säkerhetsarbetet inom institutioner och enheter och bör årligen besöka ett antal institutioner för uppföljning och erfarenhetsutbyte.

Mille Millnert
Vicerektor för IT-frågor

Gun Djerf
IT-säkerhetschef

Delges:
Institutionerna
Övriga enheter
Rektorskansliet (Djerf, Hessling, C Karlsson, Tegnefur)
De lokala fackliga organisationerna
Centrala säkerhetsgruppen för IT-frågor