LUNDS UNIVERSITET

Rektor

## Riktlinjer för informationssäkerhet vid Lunds universitet

***Bakgrund***
Universitetet genererar och hanterar stora mängder information. Denna information måste hanteras på ett sätt som dels säkerställer att universitetets behov av tillgång tillfredsställs och dels att universitetet kan uppfylla tillämpliga förordningar från t.ex. Myndigheten för samhällsskydd och beredskap, Datainspektionen, Riksarkivet med flera. För att leva upp till detta har riktlinjer för informationssäkerhet inklusive information och mallar uppdaterats.

Detta ärende är förhandlat med personalorganisationerna enligt 11 § MBL 2017-06-20.

***Beslut***
Universitetet beslutar att fr.o.m. 2017-06-22 fastställa bifogade Riktlinjer för informationssäkerhet inklusive följande bilagor:
Bilaga 1: Informationssäkerhetsinstruktion: Användare – Anställda (Infosäk A – anställda)
Bilaga 2: Informationssäkerhetsinstruktion: Användare – Studenter (Infosäk A – studenter)
Bilaga 3: Informationssäkerhetsinstruktion: Förvaltning (Infosäk F) inkl underbilaga Infosäk F – bilaga 1 – Anvisningar för informationsklassificering
Bilaga 4: Informationssäkerhetsinstruktion: Kontinuitet och drift (Infosäk KD)

Samtidigt upphävs Riktlinjer för informationssäkerhet beslutade 2012-02-15 (Dnr BY 2012/37).

Beslut i detta ärende har fattats av undertecknad rektor i närvaro av förvaltningschef Susanne Kristensson efter hörande av representant för Lunds universitets studentkårer och efter föredragning av utvecklingsstrateg John Westerlund. I handläggningen av ärendet har SamIT deltagit.

Torbjörn von Schantz

John Westerlund
(Utveckling)

*Postadress* Box 117, 221 00 Lund *Universitetshuset Telefon 046-222 12 54*, 046-222 00 00 , *E-post* john.westerlund@rektor.lu.se

Kopia
Samtliga fakulteter
Samtliga sektioner
USV/LUKOM/MAX IV
LUS
SamIT

2017-06-22 Dnr STYR 2017/947

LUNDS UNIVERSITET

Rektor

# Riktlinjer för informationssäkerhet vid Lunds universitet

Informationssäkerhetsriktlinjerna[1] vänder sig till universitetets medarbetare, såväl anställda som studenter, samt till samarbetspartners med engagemang i universitetet.

Vid universitetet finns stora mängder information, i och om forskning och undervisning samt i de administrativa systemen. Det är viktigt att informationen hanteras på ett säkert och effektivt sätt. Avsikten med riktlinjerna är att beskriva universitetets arbete med att skydda samtliga informationstillgångar som ägs eller hanteras vid universitetet mot alla hot, såväl interna som externa och avsiktliga eller oavsiktliga.

***Allmänt om informationssäkerhet***
Målen för informationssäkerheten vid universitetet består av fyra huvudkomponenter:

1. alla medarbetare ska ha tillgång till den information som de behöver för att utföra sina arbetsuppgifter och åtaganden (*tillgänglighet*),
2. informationen ska vid varje tillfälle vara korrekt och informationsresurserna ska säkerställa att informationen inte kan förvanskas genom obehörig eller felaktig hantering (*riktighet*),
3. informationen och informationsresurserna ska alltid vara skyddade mot obehörig åtkomst (*konfidentialitet*), och
4. det ska i efterhand gå att visa vad som har hänt, när det hände och vem som har gjort vad (*spårbarhet*).

Som information avses inte bara alla former av data, bilder m.m. som lagrats i databaser, datorer, datamedia, webb, e-post, som nedtecknats på papper, eller som på annat sätt finns åtkomlig (oberoende av i vilken form eller miljö), utan även det talade ordet via t.ex. telefon, på allmänna platser eller i andra sociala sammanhang. Innehållet i informationssäkerhetsriktlinjerna specificeras i informationssäkerhets-instruktioner för användare[2], förvaltning[3] samt kontinuitet och drift[4].

***Allmänna mål och principer för universitetets informationssäkerhetsarbete***
Ett aktivt informationssäkerhetsarbete bidrar till att nå uppsatta mål, att skapa trygghet för medarbetare och samarbetspartners samt att minska/undvika skador.

[1] Informationssäkerhetsriktlinjerna är en del i universitetets ledningssystem för informationssäkerhet, LIS, och motsvarar det som i Myndigheten för Samhällsskydd och Beredskaps föreskrifter, MSBFS 2016:1, kallas informationssäkerhetspolicy.
[2] Bilaga 1: Informationssäkerhetsinstruktion – Användare (Infosäk A - Anställda),
Bilaga 2: Informationssäkerhetsinstruktion – Användare (Infosäk A - Studenter)
[3] Bilaga 3: Informationssäkerhetsinstruktion – Förvaltning (Infosäk F)
[4] Bilaga 4: Informationssäkerhetsinstruktion – Kontinuitet och Drift (Infosäk KD)

*Postadress* Box 118, 221 00 Lund *Besöksadress* Universitetshuset, Paradisgatan 2 *Telefon +4646-222 12 54*, +4646-222 00 00
*E-post* john.westerlund@rektor.lu.se *Webbadress* http://www.lu.se/

Universitets informationssäkerhetsarbete ska ske med långsiktighet och kostnadseffektivitet och ska ske på ett strukturerat sätt.

Följande principer är styrande för arbetet:

- Informationssäkerhetsfrågorna ska vara en integrerad del av det dagliga arbetet.
- Alla anställda och studenter ska känna till innehållet i, och vara skyldiga att följa, gällande lagar, förordningar, regler, föreskrifter och avtal samt vara medvetna om ansvaret vid hantering av information.
- Informationssäkerheten ska hålla samma nivå oberoende av var och i vilken form informationsbehandling sker.
- All information inom universitetet ska klassificeras så att det går att avgöra vilket skydd informationen behöver och hur den får hanteras.

Årliga mål för arbetet beslutas i och framgår av verksamhetsplaneringen. För de årliga målen anges vad som ska görs under året och hur, tidplan, behov av personella och ekonomiska resurser, när och hur uppföljning, utvärdering och avrapportering ska ske, samt när och hur medarbetarna ska informeras och utbildas.

***Ansvarsfördelning***
I enlighet med arbets- och delegationsordningarna och i andra dokument regleras följande särskilt inom informationssäkerhetsområdet:

- Rektor har det övergripande ansvaret för informationssäkerheten inom universitetet[5].
- Chefer och systemägare ansvarar för att informationssäkerheten inom det egna ansvarsområdet upprätthålls och att medarbetare informeras och utbildas.[6]
- Säkerhetschefen ansvarar för att stödja, utbilda och implementera samt följa upp informationssäkerhetsarbetet inom universitetet.
- Varje anställd och student ansvarar för att följa informationssäkerhetsriktlinjerna med tillhörande instruktioner[7].
- Varje anställd är skyldig att genomgå av universitetet erbjuden utbildning[8] i informationssäkerhet.

**Bilagor:**
Bilaga 1: Informationssäkerhetsinstruktion: Användare – Anställda (Infosäk A – anställda)
Bilaga 2: Informationssäkerhetsinstruktion: Användare – Studenter (Infosäk A – studenter)
Bilaga 3: Informationssäkerhetsstruktur: Förvaltning (Infosäk F) inkl underbilaga Infosäk F Bilaga 1 – Anvisningar för informationsklassificering
Bilaga 4: Informationssäkerhetsinstruktion: Kontinuitet och drift (Infosäk KD)

[5] Universitetets arbetsordning, Dnr STYR 2017/783
[6] Bilaga 3: Informationssäkerhetsinstruktion – Förvaltning (Infosäk F)
[7] Bilaga 1: Informationssäkerhetsinstruktion – Användare (Infosäk A – Anställd) resp Bilaga 2: Informationssäkerhetsinstruktion – Användare (Infosäk A – Student)
[8] www.lu.se/kompetensportalen, Beslut: Dnr BY 2013/134

LUNDS UNIVERSITET

Rektor

# Informationssäkerhetsinstruktion: Användare – Anställda

**1. Dokumentets roll i informationssäkerhetsarbetet**
Detta dokument vänder sig till samtliga anställda vid Lunds universitet och innehåller instruktioner och information rörande informationssäkerhetsarbetet vid genomförandet av utbildning, forskning och stödverksamhet inom universitetet.

**2. Användarens ansvar**
Varje anställd är ansvarig för att följa denna informationssäkerhetsinstruktion och är skyldig att genomgå av universitetet anvisad utbildning.

Information som publiceras, görs tillgänglig eller annars hanteras ska följa SUNET:s regler[1] och inte bryta mot lagar, förordningar, föreskrifter, regler och avtal.

**3. Hantering av information**
Anställd vid Lunds universitet får endast behandla personuppgifter i den omfattning och för de syften som ingår inom ramen för anställningen och den anställdes arbetsuppgifter. Att söka efter, och titta på, uppgifter i IT-system av ren nyfikenhet eller av andra orsaker som inte omfattas av anställningen eller användarinstruktioner är inte tillåtet. Detta gäller även om uppgifterna i sig är allmänna handlingar och kan begäras ut med stöd av offentlighetsprincipen.

**4. Åtkomst till information**
*4.1 Inloggning och lösenord för att skydda informationen*
Lösenord som tilldelas vid universitetet ska omedelbart bytas till ett personligt lösenord. Lösenord får inte lämnas ut eller förvaras på ett sådant sätt att det kan vara åtkomligt för andra.

*4.2 Användarvillkor*
Alla användare kommer att anmodas att godkänna universitetets användarvillkor[2] i samband med att en LUCAT-identitet tilldelas.

[1] https://www.sunet.se/policy-for-tillaten-anvandning/
[2] Användarregler IT, STYR 2016/361

*Postadress* Box 118, 221 00 Lund *Besöksadress* Universitetshuset, Paradisgatan 2 *Telefon +4646-222 12 54*, +4646-222 00 00
*E-post* john.westerlund@rektor.lu.se *Webbadress* http://www.lu.se/

**5. Skydd av arbetsplatsen m.m.**

*5.1 Utrustning*

All installation, konfigurering, drift och utnyttjande av utrustning ansluten till universitetets datanät ska utföras så att hög informations- och datorsäkerhet tillgodoses. Om olika alternativ finns, ska det alternativ väljas som med rimlig arbetsinsats ger den högsta säkerheten.

*5.2 Anslutning till universitetets nätverk*

Endast universitetets utrustning eller utrustning som godkänts av behörig tekniskt ansvarig får kopplas in i universitetets fysiska nätverk. Det är inte tillåtet att utan särskilt tillstånd använda universitetets datanät för annan verksamhet än universitetets eller att upplåta eller vidareförsälja dator- eller nätkapacitet till andra personer eller organisationer.

*5.3 Programvaror*

Endast behöriga personer får installera programvaror på universitetets datorer. Installation ska i normalfallet ske efter godkännande av närmaste chef. Endast programvaror där det finns en giltig licens eller program som får spridas licensfritt får finnas installerade på universitetets dator. Det är inte tillåtet att ändra i eller att kopiera av universitetet licensierade programvaror eller att tillgängliggöra sådana utanför verksamheten.

Programvaror som installerats på privat utrustning med hänvisning till s.k. ”Home Usage Agreements” ska omgående avinstalleras när det aktuella anställningsförhållandet upphör.

*5.4 Service på utrustning*

Innan utrustning lämnas till en extern part för service ska information som kan vara konfidentiell i möjligaste mån tas bort.

*5.5 Kassering av utrustning*

Utrustning som ska kasseras ska lämnas till den som är tekniskt ansvarig för en miljö- och säkerhetsmässigt godkänd hantering.

*5.6 Mobiltelefoner, läsplattor etc.*

Mobiltelefoner eller annan likartad utrustning som tillhör universitetet, eller är konfigurerad att automatiskt ansluta till universitetets tjänster, t ex e-postserver, ska konfigureras så att skärmlås (motsv.) automatiskt aktiveras om enheten inte används inom maximalt fem minuter. Det är inte tillåtet att på utrustning som ägs av universitetet att kringgå operativsystemets inbyggda säkerhetsfunktioner.

*5.7 Lagring av information*

Lagring av information i så kallade molntjänster får ske om följande tre kriterier uppfyllts:

1. En dokumenterad laglighetsbedömning utifrån personuppgiftslagen är genomförd och användningen av molntjänsten bedöms ske i enlighet med personuppgiftslagen. Detta innebär bl a att ett personuppgiftsbiträdesavtal ska ha upprättats med molnleverantören. Vidare ska ställning ha tagits till;
   - om det finns risk att personuppgifter kan komma att behandlas för ändamål som strider mot de ursprungliga,

- om molnleverantören kan komma att överlämna personuppgifterna till ett land utanför EU/EES och i så fall vilket lagligt stöd i Personuppgiftslagen som finns för överföringen,
- vilka säkerhetsåtgärder som behöver vidtas för att skydda de behandlade personuppgifterna.

2. En risk- och sårbarhetsanalys är genomförd och analysen påvisar inga risker som motiverar att verksamheten bör avstå från användande av molntjänsten.
3. Prefekt (motsv.) ansvarar för att laglighetsbedömningen och risk- och sårbarhetsanalys har genomförts innan molntjänsten beställs och tas i bruk.

Varje användare måste säkerställa att dokument, datafiler, etc. säkerhetskopieras till en plats där universitetet har tillgång till informationen.

Det är tillåtet att lagra enstaka privata bilder, filer eller texter på universitetets utrustning men användaransvaret under punkten 2 ovan måste beaktas.

*5.8 Privat användning*
Universitetets utrustning får användas för privata syften, men bara i sådan omfattning att det inte inkräktar på arbetet eller medför onödiga kostnader för universitetet.

**6. Internet**
Besök på hemsidor med innehåll som kan uppfattas som kränkande, oetiskt eller på annat sätt framstå som stötande ska i förväg godkännas av prefekt och meddelas till universitetets informationssäkerhetssamordnare[3].

*6.1 Generell användning*
Vid användning av internet gäller följande:

- Användandet får inte riskera att skada omvärldens förtroende för universitetet.
- Tillgängligheten till universitetets e-tjänster m.m. för medarbetare, såväl anställda som studenter och samarbetspartners får inte påverkas negativt.
- Användandet får inte strida mot universitetets grundläggande värderingar.

*6.2 Universitetets rätt att stänga av access till universitetets nätverk*
Universitetet har rätt att av säkerhetsskäl utan föregående varning tillfälligt stänga hela eller delar av nätet och dess tjänster om det behövs för att skydda universitetets verksamhet. Beslut att stänga ner fattas av universitetets säkerhetschef eller i enlighet med vad som föreskrivs i LU-IRT[4] .

*6.3 Privat användning*
Internetanslutningen får användas för privata syften, men bara i sådan omfattning att det inte inkräktar på arbetet, påverkar tillgängligheten till universitetets e-tjänster m.m. eller medför onödiga kostnader för universitetet.

[3] Universitetets säkerhetschef
[4] http://www.ldc.lu.se/tjanster/it-sakerhet

## 7. E-post

*7.1 Hantering av e-post*

Vid användning av e-post gäller följande:

- Uppgifter som omfattas av tystnadsplikt eller sekretess får inte skickas via okrypterad kommunikation (som vanlig e-post). När sådana uppgifter kommuniceras elektroniskt, via t.ex. e-post, ska uppgifterna vara krypterade på ett sådant sätt att endast avsedda mottagare kan ta del av uppgifterna.
- Det är inte tillåtet att ta emot och skicka universitetsrelaterade ärenden från och till en egen privat e-postadress.
- Det är inte tillåtet att automatiskt vidarebefordra mail till en extern e-postadress.
- Privat e-post får endast i begränsad omfattning tas emot och skickas från universitetets e-postadress.
- Privata e-postmeddelanden ska gallras snarast eller lagras i en särskild mapp märkt ”privat”.

## 8. Kontroll av datoranvändande

*8.1 Loggning*

All e-post och internettrafik i universitetets nätverk loggas och universitetet har som arbetsgivare rätt att gå igenom dessa loggar och under vissa omständigheter ta del av innehåll i e-post för att kunna kontrollera att regler i lagstiftning eller myndigheters riktlinjer följs och för att kunna utföra de uppgifter som åligger universitetet, samt för att identifiera, hantera eller motverka informationssäkerhetshot. Detsamma gäller filer och annat material som finns lagrat i datorer och som transporteras i nätverk.

I informationssystem loggas information som är relevant för tjänstens drift t.ex. användarnamn, tidpunkter, datoradresser etc. För nättrafik loggas användarnamn, datoradress, destinationsadress, typ av tjänst, besökta hemsidor och tidpunkt.

Loggfiler gallras efter senast tre månader. Om en utredning påbörjats kommer uppgifter att bevaras så länge utredningen kräver det.

*8.2 Kontroll*

Universitetet som arbetsgivare kontrollerar inte regelmässigt innehållet i anställdas datorer, e-postmeddelanden eller internettrafik, för att så långt möjligt respektera den personliga integriteten. Universitetet kan dock komma att kontrollera uppgifter som finns i en dator, e-postmeddelanden och internettrafik om det är nödvändigt för att

- uppfylla myndighetens skyldigheter såsom allmänna handlingars offentlighet,
- vid fara för informationssäkerheten,
- att utreda eller förhindra brott och oegentligheter i enlighet med universitetets riktlinjer[5],
- på uppdrag från polis eller andra rättsvårdande myndigheter,
- vid fara för någons liv eller hälsa.

5 Riktlinjer för hantering av misstänkta oegentligheter, dnr STYR 2014/410

Om missbruk utreds av annan än universitetet kan data lämnas ut till rättsvårdande myndigheter.

Beslut om kontroll fattas av lägst prefekt (motsv.). Beslut om kontroll ska omedelbart meddelas till universitetets säkerhetschef.

**9. Konsekvenser**

Följs inte denna informationssäkerhetsinstruktion kan det innebära att arbetsrättsliga eller andra åtgärder kommer att vidtas[6]. I fall där en statlig arbetsgivare finner att en anställd är skäligen misstänkt för vissa brott som kan föranleda annan påföljd än böter, är arbetsgivaren dessutom enligt 22 § lagen (1994:260) om offentlig anställning skyldig att anmäla det misstänkta brottet till åtal. Även andra fall kan komma att anmälas till polis för utredning.

6 Arbetsrättsliga åtgärder kan vara disciplinpåföljd såsom varning eller löneavdrag, uppsägning eller vid graverande fall avstängning eller avsked.

LUNDS UNIVERSITET

Rektor

# Informationssäkerhetsinstruktion: Användare – Studenter

**1. Dokumentets roll i informationssäkerhetsarbetet**
Detta dokument vänder sig till samtliga studenter vid Lunds universitet och innehåller instruktioner och information rörande informationssäkerhetsarbetet vid genomförandet av utbildning och forskning vid universitetet.

**2. Användarens ansvar**
Varje student är ansvarig för att följa denna informationssäkerhetsinstruktion.

Information som publiceras, görs tillgänglig eller annars hanteras ska följa SUNET:s regler[1] och inte bryta mot lagar, förordningar, föreskrifter, regler och avtal.

**3. Hantering av information**
Personuppgifter som behandlas inom ramen för studier vid Lunds universitet är universitetet personuppgiftsansvarigt för. Personuppgifter får endast behandlas i den omfattning och för de syften som ingår inom ramen för studierna. Detta gäller även om uppgifterna i sig är allmänna handlingar och kan begäras ut med stöd av offentlighetsprincipen.

**4. Åtkomst till information**
*4.1 Inloggning och lösenord för att skydda informationen*
Lösenord som tilldelas vid universitetet ska omedelbart bytas till ett personligt lösenord. Lösenord får inte lämnas ut eller förvaras på ett sådant sätt att det kan vara åtkomligt för andra.

*4.2 Användarvillkor*

Alla användare kommer att anmodas att godkänna universitetets användarvillkor[2] i samband med att en StiL-identitet tilldelas.

**5. Skydd av studentarbetsplatser m.m.**
*5.1 Anslutning till universitetets nätverk*
Endast universitetets utrustning eller utrustning som godkänts av behörig tekniskt ansvarig får kopplas in i universitetets fysiska nätverk. Det är inte tillåtet att utan särskilt tillstånd använda universitetets datanät för annan verksamhet än universitetets eller att upplåta eller vidareförsälja dator- eller nätkapacitet till andra

[1] https://www.sunet.se/policy-for-tillaten-anvandning/
[2] Användarregler IT, STYR 2016/361

*Postadress* Box 118, 221 00 Lund *Besöksadress* Universitetshuset, Paradisgatan 2 *Telefon +4646-222 12 54*, +4646-222 00 00
*E-post* john.westerlund@rektor.lu.se *Webbadress* http://www.lu.se/

personer eller organisationer.

*5.2 Programvaror*
Endast behöriga personer får installera programvaror på universitetets datorer. Endast programvaror där det finns en giltig licens eller program som får spridas licensfritt får finnas installerade på universitetets dator. Det är inte tillåtet att ändra i eller att kopiera universitetets programvaror eller att tillgängliggöra sådana utanför verksamheten.

Programvaror som installerats på privat utrustning med hänvisning till s.k. ”Student Usage Agreements” ska omgående avinstalleras när det aktuella studieförhållandet upphör.

*5.3 Mobiltelefoner, läsplattor etc.*
Mobiltelefoner eller annan likartad utrustning som är konfigurerad för att automatiskt ansluta till universitetets tjänster, t ex e-postserver, ska konfigureras så att skärmlås (motsv.) automatiskt aktiveras om enheten inte används inom maximalt fem minuter.

*5.4 Privat användning*
Universitetets utrustning får användas för privata syften, men bara i sådan omfattning att det inte inkräktar på universitetets verksamhet eller medför onödiga kostnader för universitetet.

**6. Internet**
*6.1 Generell användning*
Vid användning av universitetets internetanslutning gäller följande:

- Användandet får inte riskera att skada omvärldens förtroende för universitetet.
- Tillgängligheten till universitetets e-tjänster m.m. för medarbetare, såväl anställda som studenter och samarbetspartners får inte påverkas negativt.
- Användandet får inte strida mot universitetets grundläggande värderingar.

*6.2 Universitetets rätt att stänga av access till universitetets nätverk*
Universitetet har rätt att av säkerhetsskäl utan föregående varning tillfälligt stänga hela eller delar av nätet och dess tjänster om det behövs för att skydda universitetets verksamhet. Beslut att stänga ner fattas av universitetets säkerhetschef eller i enlighet med vad som föreskrivs i LU-IRT[3] .

*6.3 Privat användning*
Internetanslutningen får användas för privata syften, men bara i sådan omfattning att det inte påverkar tillgängligheten till universitetets e-tjänster m.m. eller medför onödiga kostnader för universitetet.

**7. E-post**
*7.1 Hantering av e-post*
Vid användning av e-post gäller följande:

[3] http://www.ldc.lu.se/tjanster/it-sakerhet

- Uppgifter som omfattas av tystnadsplikt eller sekretess får inte skickas via okrypterad kommunikation (som vanlig e-post). När sådana uppgifter kommuniceras elektroniskt, via t.ex. e-post, ska uppgifterna vara krypterade på ett sådant sätt att endast avsedda mottagare kan ta del av uppgifterna.

**8. Kontroll av datoranvändande**

*8.1 Loggning*

All e-post och internettrafik i universitetets nätverk loggas och universitetet har som nätägare rätt att gå igenom dessa loggar och under vissa omständigheter ta del av innehåll i e-post för att kunna kontrollera att regler i lagstiftning eller myndigheters riktlinjer följs och för att identifiera, hantera eller motverka informationssäkerhetshot. Detsamma gäller filer och annat material som finns lagrat i datorer och som transporteras i nätverk.

I informationssystem loggas information som är relevant för tjänstens drift t.ex. användarnamn, tidpunkter, datoradresser etc. För nättrafik loggas användarnamn, datoradress, destinationsadress, typ av tjänst, besökta hemsidor och tidpunkt.

Loggfiler gallras efter senast tre månader. Om en utredning påbörjats kommer uppgifter att bevaras så länge utredningen kräver det.

*8.2 Kontroll*

Universitetet kontrollerar inte regelmässigt innehållet i studenters e-postmeddelanden eller Internettrafik för att så långt möjligt respektera den personliga integriteten. Universitetet kan dock komma att kontrollera uppgifter som finns i e-postmeddelanden och Internettrafik om det är nödvändigt för att till exempel:

- uppfylla myndighetens skyldigheter såsom allmänna handlingars offentlighet,
- vid fara för informationssäkerheten,
- för att utreda eller förhindra brott,
- på uppdrag från polis eller andra rättsvårdande myndigheter.

Om missbruk utreds av annan än universitetet kan data lämnas ut till rättsvårdande myndigheter.

Beslut om kontroll fattas av lägst prefekt (motsv.). Beslut om kontroll ska omedelbart meddelas till universitetets säkerhetschef.

LUNDS UNIVERSITET

Rektor

# Informationssäkerhetsinstruktion: Förvaltning

**1. Dokumentets roll i informationssäkerhetsarbetet**
Detta dokument vänder sig till systemägare och ledningsfunktioner och reglerar de grundläggande informationssäkerhetskraven för de som äger eller förvaltar informationssystem inom Lunds universitet.

**2. Organisation och ansvar**
*2.1 Ledning*
Rektor fattar de övergripande besluten för hur informationssäkerhetsarbetet ska bedrivas.

*2.2 IT-Samordningsgrupp, SamIT*[1]
Gruppen ska, på uppdrag av universitetsledningen, hantera och utreda generella frågor avseende anskaffning, drift, förvaltning och avveckling av informationshanteringsresurser. Inom ramen för detta ingår frågor som avser informationssäkerhet.

*2.3 Informationssäkerhetssamordnare*
Informationssäkerhetssamordnaren[2] stödjer arbetet med att uppnå informations-säkerhetspolicyns mål. Informationssäkerhetssamordnaren stödjer systemägarnas arbete med att genomföra enskilda systemsäkerhetsanalyser. Informationssäkerhetssamordnaren kan vid behov initiera systemsäkerhetsanalyser.

*2.4 Systemägare*
Systemägaren fattar inom ramen för utdelade delegationer beslut om de egna informationssystemens införande, drift, förvaltning och avveckling. Systemägaren ansvarar för att förvaltningsplanering inklusive systemsäkerhetsanalyser genomförs i enlighet med universitetets systemförvaltningsmodell[3] och att informationssäkerhetsklassificering genomförs i enlighet med Bilaga 1 till detta dokument – Anvisningar för informationsklassificering.

Systemägaren ansvarar för att det finns behörighetsnivåer, användarhandledning, manualer etc. för aktuellt system. Systemägaren ansvarar också för att användare informeras om sina rättigheter och skyldigheter vid nyttjandet av respektive informationssystem och däribland, om så krävs, erbjuda utbildningar för att uppnå tillräckliga sådana kunskaper. Systemägaren ansvarar för att

[1] http://www.lu.se/samit
[2] Universitetets säkerhetschef är utsedd som informationssäkerhetssamordnare
[3] LU Systemförvaltningsmodell, http://www3.lu.se/luwiki/index.php/Systemförvaltning. Modellen är avstämd mot Myndigheten för samhällsskydd och beredskaps modell BITS Plus.

*Postadress* Box 118, 221 00 Lund *Besöksadress* Universitetshuset, Paradisgatan 2 *Telefon +46 46 222 12 54*, +46 46 222 00 00
*E-post* john.westerlund@rektor.lu.se *Webbadress* http://www.lu.se/

systemförvaltningsplaner med bilagor rapporteras till IT-samordningsgruppen, SamIT.

*2.5 Systemförvaltare*

Systemförvaltaren innehar den verksamhetsmässiga kompetensen och utses av systemägaren. Systemförvaltaren arbetar med den dagliga driften och förvaltningen av aktuellt informationssystem.

*2.6 IT-systemägare*

IT-systemägaren ansvarar för att informationssystemens tekniska delar fungerar. IT-systemägaren ansvarar för att Infosäk KD[4] upprättas.

*2.7 IT-systemförvaltare*

IT-systemförvaltaren innehar den tekniska kompetensen, och arbetar tillsammans med systemförvaltaren för att den dagliga driften upprätthålls i enlighet med förvaltningsplanen.

**3. Regler och rutiner**

*3.1 Ansvar för tillgångar*

Varje fysisk informationsbehandlingstillgång (dvs. servrar, datorer, mobiltelefoner, läsplattor etc.) ska vara förtecknad samt ha ett unikt nummer. Av förteckningen ska framgå var tillgångarna är placerade samt vem som ansvarar för tillgången. Omflyttning och överlåtelse av tillgång får inte ske utan samråd med den ansvarige.

*3.2 Kompetenskrav vid användning av universitetets informationssystem*

Prefekt/motsvarande ansvarar för att nya användare ges en introduktion till universitetets informationssäkerhetsarbete före tilldelning av behörighet i respektive system.

*3.3 Säkrade utrymmen*

Känslig information från informationssystem ska lagras på resurser i datorhallar som är försedda med kontrollsystem för in- och utpassering. Loggning av tillträde ska ske. Utrymmen med konsolutrustning ska vara låsta när de är obemannade. Utrymmen med kopplingspunkter ska vara låsta. Beslut om tillträde tas av respektive IT-systemägare.

Känslig information som inte hanteras i informationssystem ska förvaras i säkerhetsskåp som är brandklassade för minst 120 minuter.

*3.4 Kontroll av utomstående tjänsteleverantörer*

Beställare av utomstående leverantörers tjänster ska följa upp och granska att leverantören lever upp till lägst universitetets säkerhetskrav.

*3.5 Hantering av datamedia*

Datamedia med känslig information som inte längre ska användas i universitetets verksamhet ska överlämnas till IT-systemägaren som ansvarar för miljö- och säkerhetsmässigt korrekt destruktion.

---

[4] LU Systemförvaltningsmodell, Bilaga 3 – Infosäk KD ITSÄ

*3.6 Flytt av fysisk informationslagringstillgång*

Om media som innehåller känslig information måste transporteras fysiskt ska säkerhetschefen kontaktas inför beslut om tillvägagångssätt.

*3.7 Övervakning*

För informationssystems loggar ska systemägaren besluta:

- För vilka syften en logg får analyseras
- Hur ofta de ska analyseras
- Vem som ansvarar för analyser av dem
- Hur länge de ska sparas om avvikelse skall ske från standard 90[5] dagar.
- Hur de ska förvaras.

*3.8 Styrning av användarens åtkomst – behörighetshantering*

För att säkerställa att endast behöriga användare förekommer i informationssystemen ska styrning av åtkomst till informationssystem i möjligaste mån ske via universitetets identitets- och behörighetssystem[6]. Systemägaren beslutar om åtkomsten och eventuella avsteg från nämnda behörighetssystem.

Universitetet tillämpar två nivåer inom behörighetshantering; dels traditionell behörighetshantering som avgör vilka användare som har åtkomst, dels användandet av tillitsnivåer[7] som signalerar hur väl användaren har identifierats.

*3.9 Styrning av åtkomst till datanät*

All installation, konfigurering, drift och utnyttjande av utrustning ansluten till Lunet[8] skall utföras så att hög informations- och IT-säkerhet tillgodoses samt i enlighet med uppställda krav i varje enskilt fall. Det är inte tillåtet att tillhandahålla tjänster som medger anonym användning av datanäten.

*3.10 Styrning av åtkomst till operativsystem*

IT-systemägaren beslutar i vilken utsträckning användning av operativsystem, administrationsverktyg eller andra systemhjälpmedel som kan förbigå system- och tillämpningsspärrar får användas.

*3.11 Mobil datoranvändning och distansarbete*

Systemägaren beslutar om ett informationssystems information ska få hanteras på distans med stationär eller mobil utrustning.

*3.12 Säkerhetskrav på informationssystem*

Inför nyanskaffning och införande av ett universitetsövergripande informationssystem ska verksamhetsansvarig chef i samråd med SamIT utforma en

---

[5] Rekommenderad lagringstid enl. datainspektionen
[6] LUCAT
[7] Universitetet tillämpar det tillitsramverk som är etablerat inom högre utbildning i Sverige. *Bekräftade användare* ska användas i informationssystem med extra högt skyddsvärde. *Bekräftade användare* är de användare som uppfyller SWAMID Assurance Level 2. Tilllitsramverket med nivåerna SWAMID Asssurance Level 1 resp SWAMID Assurance Level 2 är baserat på det internationella tillitsramverket Kantara Initiative
[8] Universitetets fasta och trådlösa datanätverk, http://www.ldc.lu.se/tjanster/natverk

plan[9] för införandet, vilken också ska kunna ligga till grund för upphandlingen av sådana system.

### *3.13 Säkerhet i utvecklings- och underhållsprocesser*

Förslag om önskemål på förändringar i systemet lämnas till systemförvaltaren. Arbetet ska bedrivas enligt universitets systemförvaltningsmodell[10] respektive projektmodell[11].

### *3.14 Hantering av informationssäkerhetsincidenter och förbättringar*

Systemägaren och IT-systemägaren ska via universitetets incidentsrapporteringssystem[12] rapportera:

- intrång och avancerade försök till intrång
- incidenter som orsakar eller skulle kunna orsaka betydande avbrott och störningar
- konsekvenser och förslag till åtgärder efter intrång eller funktionsfel.

Misstänkt brott mot lagstiftning eller internt regelverk ska rapporteras enligt universitetets *riktlinjer för hantering av misstänkta oegentligheter*[13].

[9] Innehållande behovsbeskrivning, säkerhetsanalys, driftsättningskrav mm
[10] http://www3.lu.se/luwiki/index.php/Systemförvaltning
[11] http://www3.lu.se/luwiki/index.php/Projektkontoret
[12] http://www.lu.se/alarm
[13] http://www.medarbetarwebben.lu.se/organisation-och-styrning/regler-och-beslut/regelverket/regler-juridik-och-dokumenthantering

LUNDS UNIVERSITET

Rektor

## Infosäk F bilaga 1 – Anvisningar för informationsklassificering

***Klassificering av information med avseende på behov av säkerhet***
Syftet med att klassificera informationen utifrån säkerhetsaspekterna nedan är att bedöma kraven på hur universitetets information och berörda informationssystem ska hanteras.

Klassificeringsmodellen baseras på de, enligt SS-ISO/IEC 27001, tre vedertagna informationssäkerhetsaspekterna: *konfidentialitet*, *riktighet* och *tillgänglighet*. Därutöver finns möjligheten att lägga till aspekter (t. ex spårbarhet, avbrottsskydd, autencitet, icke-förnekbarhet, etc.) där speciella krav på informationssäkerhet föreligger.

| SÄKERHETSASPEKT | SKYDDSMÅL |
|---|---|
| **KONFIDENTIALITET** | Informationen ska inte göras tillgänglig eller avslöjas för obehöriga personer, system eller processer |
| **RIKTIGHET** | Informationen ska inte förändras eller förstöras, varken obehörigen, av misstag eller på grund av funktionsstörningar. |
| **TILLGÄNGLIGHET** | Informationen ska vara åtkomlig och användbar på förväntat sätt och inom önskad tid |

***Användningsområden***
Konkreta användningsområden där en informationsklassificering enligt dess anvisningar bör ligga till grund för val av säkerhetsnivå och därav följande säkerhetsåtgärder är:

- Kravställning/kravspecificering inför systemutveckling eller upphandling av system
- Fastställande av säkerhetsdesign av ett informationssystem
- Genomförande av risk- och hotbildsanalyser av ett systemförvaltningsobjekt eller enskilt informationssystem
- Genomförande av informationssäkerhetsanalyser (egenkontroller) i ett förvaltningsobjekt eller enskilt informationssystem
- Fastställande av hanteringsregler av information, t.ex. med avseende på krav på kryptering av e-post, regler för och eventuell märkning av intern och extern post, kommunikation via mobiltelefon etc.

*Postadress* Box 118, 221 00 Lund *Besöksadress* Universitetshuset, Paradisgatan 2 *Telefon +4646-222 12 54*, +4646-222 00 00
*E-post* john.westerlund@rektor.lu.se *Webbadress* http://www.lu.se/

***Säkerhetsnivåer***
Klassificeringen görs med utgångspunkt från omfattningen av de konsekvenser som kan uppkomma vid brister i skyddet. Behovet av säkerhet (skyddsbehovet) för information beskrivs med någon av nivåerna: **basnivå**, **hög nivå** eller **särskilda krav**.

Publik information som till exempel information nedladdad från internet, allmänt tillgänglig text eller bild etc. behöver inte klassificeras alls. Man kan uttrycka det som att det finns ytterligare en nivå, ”Oklassificerad”, utan något specificerat behov av säkerhet.

Behov av säkerhetsnivå beskrivs separat för var och en av de tre säkerhetsaspekterna med stöd av *Mall för informationsklassificering* nedan.

# Mall för informationsklassificering

## 1 Beskrivning av säkerhetsklasserna

### 1.1 Konfidentialitet

Behovet av skydd mot att informationen görs tillgänglig eller avslöjas för obehöriga personer, system eller processer.

**Basnivå**
***Allmän beskrivning***
Information som behöver skydd mot oavsiktlig eller obehörig åtkomst. Information som avsiktligt görs tillgänglig för allmänheten.

***Exempel på information***
Merparten information vid universitetet (arbetsmaterial, men även allmänna handlingar) ingår i basnivån

***Exempel på skydd***
Informationen ska vara skyddad mot oavsiktlig eller obehörig åtkomst genom inloggning, eller genom inlåsning eller på annat sätt skyddad förvaring. Offentlig information ska vara tillgänglig på ett kontrollerat sätt.

***Möjliga konsekvenser av brister***
Brister i skyddet kan medföra obehag eller begränsad ekonomisk förlust för enskilda personer, eller begränsad skada för universitetet eller tredje part.

**Hög nivå**
***Allmän beskrivning***
Information som behöver ett starkt skydd mot oavsiktlig eller obehörig åtkomst, inklusive information som omfattas av sekretess.

***Exempel på information***
Sekretesskyddad information, starkt integritetskänslig information (till exempel information om sjukdom)

***Exempel på skydd***
Informationen ska vara skyddad genom kvalificerad kryptering, inlåsning i väl skyddat skåp eller på annat motsvarande sätt.

***Möjliga konsekvenser av brister***
Brister i skyddet kan orsaka omfattande obehag eller ekonomisk förlust för enskilda personer, eller omfattande skada för universitetet eller tredje part.

**Särskilda krav** (kan avse en eller flera aspekter av sekretesskydd)
***Allmän beskrivning***
Information som behöver ett särskilt starkt skydd mot oavsiktlig eller obehörig åtkomst, inklusive skydd mot kvalificerade angrepp avsedda att komma åt informationen.

***Exempel på information***
Skyddade identiteter eller adresser. Särskilt känslig forskningsinformation (företagshemligheter e.d.). Information som omfattas av försvarssekretess.

***Exempel på skydd***
Mycket kvalificerat skydd mot obehörig eller oavsiktlig åtkomst. Skydd mot kvalificerade angrepp avsedda att komma åt informationen ska finnas.

***Möjliga konsekvenser av brister***
Brister i skyddet kan medföra skada på liv eller hälsa för enskilda personer, eller orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer, eller mycket allvarligt skada för universitetet eller tredje part.

## *2.2 Riktighet*

Behovet av skydd mot att informationen förändras eller förstöras – obehörigen, av misstag eller på grund av funktionsstörningar.

**Basnivå**
***Allmän beskrivning***
Information som behöver ett grundläggande skydd mot att förändras eller förstöras.

***Exempel på information***
Merparten information vid universitetet (arbetsmaterial och allmänna handlingar) ingår i basnivån.

***Exempel på skydd***
Informationen ska vara skyddad – genom säkerhetskopiering, noggrann testning av program, skyddad förvaring, signatur på dokument e.d. – mot oavsiktlig eller obehörig förändring eller förstöring.

***Möjliga konsekvenser av brister***
Brister i skyddet kan medföra obehag eller begränsad ekonomisk förlust för enskilda personer, eller begränsad skada för universitetet eller tredje part.

**Hög nivå**
***Allmän beskrivning***
Information som behöver ett starkt skydd mot att förändras eller förstöras.

***Exempel på information***
Beslut och annan information som har ”rättsverkan” eller som har stor betydelse för universitetet eller enskilda. Bokföringsmaterial, information i bokförings- och redovisningssystem, listor med tentamensresultat. Forskningsdata med stor vetenskaplig eller ekonomisk betydelse.

***Exempel på skydd***
Informationen ska vara väl skyddad
– genom loggning av förändringar, digitala signaturer, manuella signaturer, noggranna hanteringsrutiner e.d. – mot oavsiktlig eller obehörig förändring eller förstöring.

***Möjliga konsekvenser av brister***
Brister i skyddet kan orsaka omfattande obehag eller ekonomisk förlust för enskilda personer, eller omfattande skada för universitetet eller tredje part.

**Särskilda krav** (kan avse en eller flera aspekter av skydd av riktighet)
***Allmän beskrivning***
Information som behöver ett särskilt starkt skydd mot att förändras eller förstöras.

***Exempel på information***
Original till avhandlingar. Ladok-databasens tabeller över personer och deras studieresultat. Avtalsoriginal.

***Exempel på skydd***
Mycket kvalificerat skydd mot oavsiktlig och obehörig förändring, till exempel genom användning av certifikatbaserade digitala signaturer och kontrollsummor. Särskilt utformade rutiner för säkerhetskopiering och loggning av förändringar.

***Möjliga konsekvenser av brister***
Brister i skyddet kan medföra skada på liv eller hälsa för enskilda personer, eller orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer, eller mycket allvarligt skada för universitetet eller tredje part.

## 2.3 Tillgänglighet

Behovet av skydd som möjliggör att informationen är åtkomlig och användbar på förväntat sätt och inom önskad tid.

**Basnivå**
***Allmän beskrivning***
Information som normalt ska vara tillgänglig dygnet runt (eller vid särskilt beslutade tider), men där enstaka avbrott upp till en halv arbetsdag endast medför begränsad skada.

***Exempel på information***
Merparten information vid universitetet (arbetsmaterial och allmänna handlingar av i första hand internt intresse) ryms inom basnivån.

***Exempel på skydd***
Informationen ska helst vara tillgänglig hela dygnet. Avbrott i tillgängligheten under kontorstid ska normalt vara i högst 4 timmar. Informationens tillgänglighet ska möjliggöras genom stabila och väl testade IT-system, och fungerande stödrutiner.

***Möjliga konsekvenser av brister***
Brister i tillgängligheten kan medföra obehag eller begränsad ekonomisk förlust för enskilda personer, eller begränsad skada för universitetet eller tredje part.

**Hög nivå**
***Allmän beskrivning***
Information som ska vara tillgänglig dygnet runt (eller vid särskilt beslutade tider) utan avbrott. Enstaka kortare avbrott medför endast begränsad skada.

***Exempel på information***
Universitetets externa webbsidor. Information som studenter behöver för att fullgöra studier eller tentamina (t.ex. information om tider och lokaler). Gemensamma mailsystem. Information på filservrar. Allmänna handlingar av stort intresse för allmänheten.

***Exempel på skydd***
Informationen ska vara tillgänglig under hela dygnet. Avbrott i tillgängligheten ska normal vara i högst 0,5 timmar. Planerade avbrott ska vara aviserade i god tid.

***Möjliga konsekvenser av brister***
Brister i tillgängligheten kan orsaka omfattande obehag eller ekonomisk förlust för enskilda personer, eller omfattande skada för universitetet eller tredje part.

**Särskilda krav** (kan avse en eller flera aspekter av skydd av riktighet)
***Allmän beskrivning***
Information som måste vara tillgänglig dygnet runt (eller vid särskilt beslutade tider) utan avbrott, och där även kortare avbrott kan orsaka stor skada.

***Exempel på information***
Katalog- och inloggningstjänster (informationen i dessa). DNS, DHCP och andra tjänster av mycket stor betydelse för utnyttjandet av samtliga IT-tjänster vid universitetet.

***Exempel på skydd***
Redundanta system och andra åtgärder för att möjliggöra i princip obruten åtkomst trots mycket allvarliga störningar (redundanta system i olika lokaler etc.).

***Möjliga konsekvenser av brister***
Brister i tillgängligheten kan medföra skada på liv eller hälsa för enskilda personer, eller orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer, eller mycket allvarligt skada för universitetet eller tredje part.

| | |
|---|---|
| Informationsresurs (*förvaltningsobjekt informationssystem, projekt etc*.) | |
| Datum | |
| Deltagare | |

**Konfidentialitet**
Skyddsmål: Informationen ska inte göras tillgänglig eller avslöjas för obehöriga personer, system eller processer.

| **Nivå** | **Finns** | **Exempel på information tillhörig denna nivå** |
|---|---|---|
| Basnivå | | |
| Hög nivå | | |
| Särskilda krav | | |
| Ange de särskilda kraven: | | |

**Riktighet**
Skyddsmål: Informationen ska inte förändras eller förstöras, varken obehörigen, av misstag eller på grund av funktionsstörningar.

| **Nivå** | **Finns** | **Exempel på information tillhörig denna nivå** |
|---|---|---|
| Basnivå | | |
| Hög nivå | | |
| Särskilda krav | | |
| Ange de särskilda kraven: | | |

**Tillgänglighet**
Skyddsmål: Informationen ska vara åtkomlig och användbar på förväntat sätt och inom önskad tid.

| **Nivå** | **Finns** | **Exempel på information tillhörig denna nivå** |
|---|---|---|
| Basnivå | | |
| Hög nivå | | |
| Särskilda krav | | |
| Ange de särskilda kraven: | | |

**Sammanfattning**

| **Säkerhetsaspekt** | **Basnivå** | **Hög nivå** | **Särskilda krav** |
|---|---|---|---|
| Konfidentialitet (sekretess) | | | |
| Riktighet (integritet) | | | |
| Tillgänglighet | | | |

**Kommentarer till bedömningarna**

| # | **Kommentar** |
|---|---|
| | |

LUNDS UNIVERSITET

Rektor

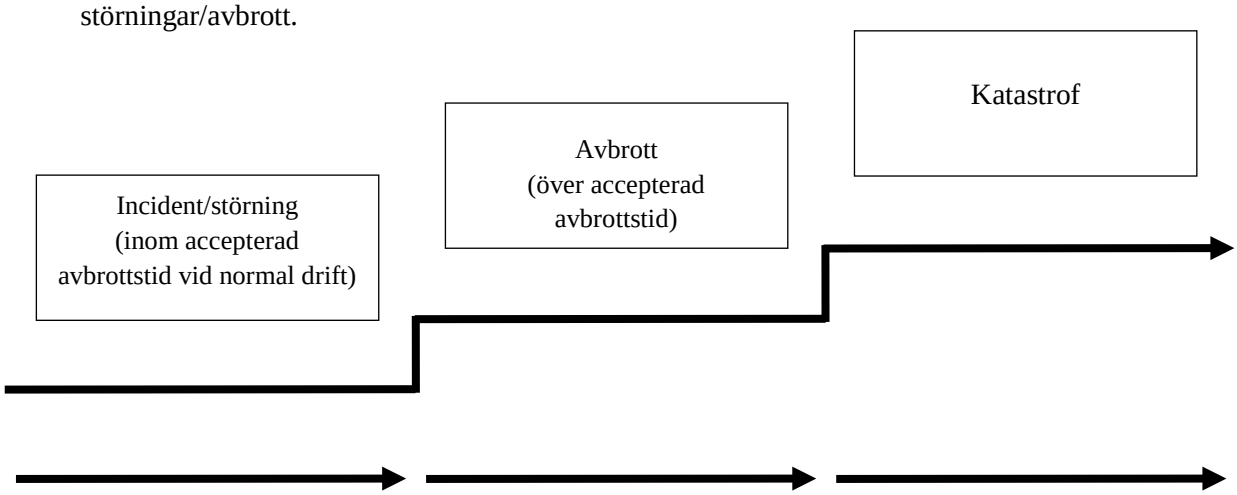
## Informationssäkerhetsinstruktion: Kontinuitet och drift

### 1. Dokumentets roll i informationssäkerhetsarbetet

Detta dokument vänder sig till de IT-organisationer eller andra funktioner som ansvarar för IT-drift av informationssystem vid Lunds universitet.

### 2. Organisation och ansvar för säkerhetsarbetet

Nedanstående modell beskriver hur avbrott hanteras under olika faser av störningar/avbrott.




| Hanteras av: | Hanteras av: | Hanteras av: |
|---|---|---|
| • *<vem>* | • *<vem/vilka>* | • *<vem/vilka>* |
| **Incident/Störning** | **Avbrott** | **Katastrof** |
| En oönskad händelse som kan hanteras inom accepterad avbrottstid med interna eller externa resurser | En oönskad händelse som inte kan hanteras inom accepterad avbrottstid med interna resurser | En mycket allvarlig händelse bortom all kontroll och som kraftigt påverkar verksamheten |

*Postadress* Box 118, 221 00 Lund *Besöksadress* Universitetshuset, Paradisgatan 2 *Telefon +4646-222 12 54*, +4646-222 00 00
*E-post* john.westerlund@rektor.lu.se *Webbadress* http://www.lu.se/

Ledningsorganisationen vid olika faser skiftar. Generellt innebär detta att organisationen växer efter hand som händelsen eskalerar.

***Support***

*Beskriv hur supportorganisationen är bemannad och vilka arbetsuppgifter den har. Tex:*

*Supporten är bemannad dagtid under vardagar och utgör första steget i IT-service organisationen. Support ska:*

- *Ta emot anmälan om alla typer av händelser*
- *Upprätta dagbok med utrymme för tidpunkt för anmälan, vem anmälde, och om möjligt hur händelsen uppstod eller upptäcktes (under införande)*
- *Klassificera händelserna. (Incident, avbrott eller katastrof?)*
- *Klara incidenter och störningar*
- *Planera inför avbrottsfas och katastroffas genom att sammankalla berörda*

Hos Support ska minst finnas:

- Förteckning över resurspersoner
- Förteckning över aktuella avtal med kontaktpersoner

Hos Support ska också checklistor för de allvarligaste hoten som:

- Checklista angrepp skadlig kod
- Checklista återläsning och återställande
- M fl

## 3. Verksamhetens interna nätverk

Plats för nätverksbild

## 4. Kraven på nätverkets resurser

*Beskriv de enheter i det interna nätverket som ska skyddas i nedanstående tabell.*

*De krav som tabellen visar för respektive enhet baseras på den*

- *samlade hotanalysen för de applikationer i organisationen som ingår i det interna nätverket*
- *information som lagras eller transporteras*

*Organisationens gemensamma Informationssäkerhetsinstruktion för kontinuitet- och drift baseras på tabellen.*

B=Basnivå, HN=Hög nivå & MHN=Mycket hög nivå.

*(Exempel på resurser. Lägg till så många rader som du behöver..)*

| **Resurs** | **Placering** | **Informationssystem** | **Kravnivå Tillgänglighet** |
|---|---|---|---|
| *Applikationsservrar* | *VLAN* | | *B* |
| *Backupserver* | *VLAN* | *Backupserver med extern lagring* | *HN* |
| *Databasservrar* | *VLAN* | | *HN* |

## 5. Genomförda åtgärder

*(Exempel på åtgärder)*

| **Resurs** | **Genomförda åtgärder / Reservförfarande** |
|---|---|
| Klienter | • *Senaste säkerhetsrelaterade uppdateringarna är installerade både vad det gäller operativsystemet och applikationerna*<br>• *Antivirusprogram är installerat och uppdateras kontinuerligt* |
| Servrar | • *Senaste säkerhetsrelaterade uppdateringarna är installerade både vad det gäller operativsystemet och applikationerna*<br>• *Antivirusprogram är installerat och uppdateras kontinuerligt* |
| Datorhall | • *Utrustning för fukt- och temperaturlarm finns.*<br>• *UPS finns.*<br>• *Automatisk brandlarmsutrustning*<br>• *Handbrandsläckare finns* |

# 6. Daglig drift

## *6.1. Resurser*

### 6.1.1. Lokaler och utrustning

*Beskriv den fysiska miljön där dels utrustning finns, och dels utrustning används. Tex:*

*Serverhallen:*
*Serverhallen utgör basen för serverparkens fysiska placering. Lokalen har ändamålsenlig utrustning, såsom, klimatanläggning, UPS:er, upphöjt antistatiskt golv, mm.*

*Undervisningssalar:*
*Verksamheten har ett antal undervisningssalar som i regel består av en tunn klient samt projektor varpå läraren kan koppla upp sig till den miljö som han/hon önskar, så att han/hon kan utföra sin undervisning.*

### 6.1.2. Programvaror/register – Applikationer

*Beskriv den fysiska miljön där dels utrustning finns, och dels utrustning används. Tex:*

*Programansvariga:*
*Verksamheten nyttjar LDCs programförmedling för de flesta programvaror. I de fall programvaran ej finns tillgänglig, görs inköp/hyrs de hos respektive leverantör.*

*Lunds universitet har Campusavtal med bl.a Microsoft, Adobe samt Alfasoft (Endnote) vilket ger alla anställda rätt att använda dessa produkter i sitt arbete.*

*Vi har även MSDNAA som är ett avtal som man tecknar med Microsoft vilket ger Studenterna tillgång att fritt ladda ner ett antal av Microsofts programvaror som man använder i sin utbildning.*

### 6.1.3. Märkning och benämningar

*Beskriv om, och i så fall hur, utrustning märks. Samt hur märkningen dokumenteras Tex:*

*All IT-utrustning som lämnas ut till användare märks med datornamn efter Institutionens namn samt löpnr.*
*Vi har vår dokumentation i Live@Lund (Sharepointmiljö).*
*Delar av detta finns även i Nettools.*
*Servrar samt annan Nätverksutrustning som skall vara som tjänst för verksamhetens användare är också uppmärkta efter namnstandarden.*

### 6.1.4. Klassning av resurser

*Beskriv hur informationsklassning av innehållet i servrar praktiskt genomförs*

6.1.5. Arbetsplatser
*Beskriv hur arbetsplatsdatorer hanteras. Tex:*

*Klienterna på arbetsplatserna består av standardiserad hårdvara ur ”långtidsserier”. Hårdvaran består av stationära/bärbara persondatorer samt tunna klienter.*

*Mjukvaruinstallation gör mha standardimages (via ”Ghost”) innehållande aktuellt OS och arbetsplatsprogramvara, t.ex. MS Office, Adobe Acrobat, Endnote samt program efter behov.*

6.1.6. Omflyttning och överlåtelse av IT-utrustning
*Beskriv hur omflyttning och överlåtelse All IT-utrustning som överlåtes till annan användare går till inklusive metoder för destruktion av utrangerade lagringsmedia.*

### *6.2. Fysiskt skydd*

6.2.1. Klimatutrustning
Kontaktuppgifter:

6.2.2. Brandskydd
Kontaktuppgifter:

6.2.3. Tillträdeskontroll
*Beskriv metoder och regler för fysiskt tillträde till serverhallar och andra utrymmen där det finns dator- eller nätverksutrustning. Tex:*

*Fysiskt tillträde – Serverhallen*
- *Serverhallen är ett ”eget företag” i passagesystemet med begränsade rättigheter.*
- *Vid borttappat kort: www.lu.se/lukortet*

*Fysiskt tillträde – allmänna utrymmen*
- *Tillträde till allmänna utrymmen hanteras enligt normala regler.*
- *Vid borttappat kort: www.lu.se/lukortet*

### *6.3. Kommunikation*

6.3.1. LAN
*Beskriv LAN konfiguration. Tex:*

*Verksamhetens nätverk är uppdelade i VLAN efter funktion. Servrar, skrivare, klienter, m.fl. är indelade i olika nät. Dessa nät är åtskilda med brandvägg. Kommunikationen sker med IP v4. All kommunikationsutrustning finns i låsta*

*utrymmen och ingår i CFL. Managering av näten görs av ITS-gruppen samt resurser från LDC.*

6.3.2. Fjärraccess/VPN

*Används fjärraccess? Hur? Till vad?*

*För managering av servrar utnyttjas fjärraccess (RDC). Vid klientanslutning utanför våra klientnät utnyttjas LDC:s VPN-tjänst.*

6.3.3. Brandvägg

*Används brandväggar? Vilka? Hur?*

*Vi använder oss av LDC:s tjänst för brandväggar, med loggning aktiverad på misslyckad trafik. Övervakning av brandväggen ingår i tjänsten.*
*Kontroll av loggar utförs av oss vid misstankar om problem.*

6.4. Roller och ansvar – IT

*Beskriv vilka roller som finns, och vem som bemannar rollerna.*

### *6.5. Åtkomsträttigheter – användare*

6.5.1. Konton

*På vilka grunder delas konton ut?*
*Hur skapas dom?*
*Hur dokumenteras det?*
*Hur underhålls (plockas bort..) dom?*

### *6.6. Loggning och spårbarhet*

6.6.1. Övervakning

*Vad övervakas? Med hjälp av vilka application/er? Tex:*

- *Våra servrar övervakas med MS SCOM*
- *Vi har övervakning av OperativSystem, DNS, AD, DFS, SQL , mail, Sharepoint, webb*
- *Övervakning av hårdvara via ILO*
- *Viss prestandaövervakning med SCOM*

#### *6.6.2. Logghantering*

*Beskriv hur ni säkerställer att relevanta loggar bevaras. Tex:*

*Backupprogramvaran tar backup av loggar.*

6.6.3. Logganalys

*Beskriv hur och när loggar analyseras. Tex:*

*Analyserar loggar när system mår dåligt eller SCOM reagerat på något*

### *6.7. Säkerhetskopiering*

6.7.1. Intervall och omfattning

*Beskriv hur säkerhetskopiering går till, vad som kopieras och hur länge säkerhetskopior sparas. Tex:*

*Dokumentation över systemägarnas beslut avseende:*

- *Alla servrar inkl klienternas hemmakataloger & profiler ingår i backuptagning*
- *Backup sker på daglig basis, veckovis samt en gång per månad*
- *De olika backupmetoderna har varierande tidsperiod gällande skydd mot överskrivning*
- *Backupsystemet är fysiskt skilt från övriga servrar*
- *Backupmediat består av dedupliceringsteknik*
- *Verifiering av tagen backup görs alltid*

## 7. Störningar/avbrott

### *7.1. Avbrottsplan*

*Beskriv hur ni agerar vid avbrott. Tex:*

*Om ett strömavbrott inträffar så har vi batteridrift i c:a 50 minuter. Detta är till för att kunna stänga ner alla servrar.*

### *7.2. Reservdrift och reservrutiner*

*Beskriv reservrutiner. Tex:*

*Vid strömbortfall så kommer hela serverhallen att gå över på UPS. Samtidigt kommer det att skickas information till SCOM som i sin tur skickar ut mail till supporten. Det är förinställt att ingenting kommer att hända de första 15 minuterna. Efter 15 minuter kommer systemen att börja stängas ner. Detta sker med hjälp av <metod>.*

*System som stängs av efter 15 minuter:*

- *<lista system>*

*System som stängs av efter 45 minuter:*

- *<lista system<*

### *7.3. Reservkraft*

*Finns reservkraft? Kapacitet? Vilka funktioner/system täcks av reservkraft? Vem sköter service/underhåll?*

### *7.4. Återstartsrutiner*

Hur ser återstartsrutiner ut? I vilken ordning skall system startas? Vilka kontroller skall genomföras I samband med återstart? Vem skall göra dem? Hur skall det dokumenteras? Vem skall notifieras?

## 8. Incidenthantering

### *8.1. Uppdatering av antivirusprogram*

*Beskriv hur ni säkerställer att alla relevanta maskiner har uppdaterat antivirusskydd. Tex:*

*Alla stationära datorer och server uppdateras via antivirusserver så snart det finns nya uppdateringar. Antivirusservern uppdateras från Symantec när nya uppdateringar finns tillgängliga.*

### *8.2. Förebyggande åtgärder*

*Beskriv vilka förebyggande åtgärder ni tillämpar för att säkra kontinuerlig drift. Tex:*

- *Antivirusprogram*
- *Brandvägg*
- *Tillhandahåller backuper*
- *Profilhantering: Lokala kataloger så som ”My Documents” styrs till server.*

### *8.3. Dokumentation av inträffade incidenter*

*Beskriv hur incidenter, eller befarade incidenter, hanteras, dokumenteras och rapporteras. Tex:*

*Någon kontaktar oss eller vi själv upptäcker att något inte står rätt till på en server.*

- *Två personer sätter sig med detta och antecknar allt man gör och ser.*
- *Ta reda på så mycket som möjligt innan servern stängs av*
- *Några exempel:*
  - *Vad är klockan och datumen på servern skiljer det mot verklig tid?*
  - *Ip-adresser, Hostname*
  - *Annat som kan vara avvikande.*

- *Kör en image(Diskcopy) live i servern innan den stängs ner för att kunna titta mer ingående på data senare.*
- *Nu kan man stänga av servern och börja att titta i image'en istället.*
- *Kontrollera antivirusskyddet när det senast uppdaterades samt Windows update.*
- *Kontrollera användarkonto m.m.*
- *Rapportering till LU IRT och/eller www.lu.se/alarm*

## 9. Dokumentation

*Beskriv hur dokumentation hålls aktuell och tillgänglig för berörd personal.*