



## IT-säkerhetsplan vid Umeå universitet

Med it-säkerhet avses säkerheten i användningen av universitetets it-resurser.

### **Mål**

IT-säkerheten vid Umeå universitet ska:

- säkerställa att universitetet kan använda kommunikationsnät och it-system utan onödiga störningar och med avsedd funktion och hög tillgänglighet.
- förhindra att störningar i kommunikationsnät och it-system orsakar allvarliga konsekvenser för universitetets anställda, studerande och allmänheten.
- säkerställa att information som överförs, lagras eller behandlas i kommunikationsnät och it-system ska skyddas mot oavsiktlig, obehörig eller otillåten förändring, förstöring, åtkomst eller kopiering.
- säkerställa att kommunikationsnät och it-system skyddas mot intrång, otillåten användning, stöld eller skadegörelse.

### **Ansvar**

Se Informationssäkerhetspolicy för Umeå universitet.

### **Stöd, samordning och kontroll**

Universitetet ska ha centralt finansierade resurser för stöd, samordning och kontroll av it-säkerheten.

IT-chefen ansvarar för:

- övergripande samordning av allt it-säkerhetsarbete vid universitetet.
- utformning och revision av regler och anvisningar.
- beredning av it-säkerhetsärenden för styrelse och rektor.
- samordning av it-säkerheten för de centrala it-resurserna.

### **Regler och riktlinjer**

Det ska finnas fastställda regler och riktlinjer för datasäkerheten i kommunikationsnät och it-system som är särskilt viktiga för universitetet, och för sådana skyddsåtgärder som är av särskild betydelse för it-säkerheten vid universitetet.

### **Skyddsåtgärder**

I allt säkerhetsarbete ska skyddet av liv, hälsa och personlig integritet värderas högst.



Säkerhetsnivåer och skyddsåtgärder för it-säkerheten vid universitetet ska utformas så, att målen för it-säkerheten uppnås till rimliga kostnader, och utan att den dagliga verksamheten försvaras mer än nödvändigt.

Utformning av säkerhetsnivåer och skyddsåtgärder ska grunda sig på aktuell eller förväntad hotbild, och på konsekvenserna av störningar för universitetet eller för anställda, studerande och allmänheten. Hänsyn ska tas till såväl direkta som indirekta konsekvenser.

Bedömningar av hotbild och konsekvenser av störningar ska göras systematiskt och med vedertagna metoder.

IT-säkerheten vid universitetet ska, för nät och system anslutna till SUNET, uppfylla SUNETs regler.

Skyddsåtgärder för IT-säkerheten ska baseras på etablerade standarder.

### **Information och utbildning**

Kunskaperna och säkerhetsmedvetandet hos it-personalen och användarna är avgörande för it-säkerheten. Personalen och användarna måste få den information och utbildning som behövs för att de ska kunna upprätthålla avsedd it-säkerhet.

IT-chefen ansvarar för att grundläggande informations- och utbildningsmaterial om it-säkerhet tas fram och hålls aktuellt.

Verksamhetsansvariga ansvarar för att anställda och studenter inom den egna enheten får information och utbildning om it-säkerhet.

Systemägarna ansvarar för att informations- och utbildningsmaterial tas fram samt att information till och utbildning av användarna initieras.

### **Användare**

Varje användare ska, innan den får tillgång till universitetets it-resurser intyga att de tagit del av universitetets *Regler för användning av Umeå universitetets it-resurser*.

Reglerna ska omfatta:

- villkor för användning av it-resurserna.
- användarnas ansvar och skyldigheter.
- gällande regler för användning av it-resurser.

### **Systemadministratör**

Med systemadministratör avses en person som har högre behörighet än vanliga användare i it-system och kommunikationsnät. Systemadministratören har normalt ett drift- eller säkerhetsansvar, eller medverkar i drift eller förvaltning av it-system och nät.

Systemadministratören utses och tilldelas sina rättigheter och skyldigheter genom ett skriftligt beslut



av verksamhetsansvarig. I beslutet ska anges vilka system eller motsvarande som rättigheterna avser.

Samtliga personer som är verksamma som systemadministratörer vid universitetet ska ha undertecknat en särskild ansvarsförbindelse. Ansvarsförbindelsen ska innehålla:

- hänvisning till informationen i regler för användare.
- information om systemadministratörens ansvar och skyldigheter.
- information om gällande regler för drift och förvaltning av nät och it-system.
- information om regler och rutiner för åtgärder vid incidenter.

### **Drift**

Den som ansvarar för drift av kommunikationsnät eller it-system ska normalt också tilldelas ansvar för it-säkerheten i driften samt tillse att kompetent personal finns tillgänglig i den omfattning som krävs för att avsedd it-säkerhet ska kunna upprätthållas.

### **Avbrottsplanering**

Ansvariga för it-säkerheten för:

- centrala it-resurser,
- it-system av stor betydelse för utbildning eller forskning,
- it-system av stor ekonomisk betydelse för universitetet,
- it-system av betydelse för säkerheten i övrigt vid universitetet,

ska genomföra avbrottsplanering för systemen eller resurserna.

### **Upphandling och utveckling**

Vid upphandling och utveckling av it-system och it-tjänster ska säkerhetskraven alltid beaktas. Krav på it-säkerhet ska ingå i kravspecifikationen och avtalet.

### **Outsourcing**

Då en annan part utför uppdrag åt universitetet där it-tjänster eller it-system utgör en viktig del, ska universitetet i avtalet försäkra sig om att parten upprätthåller en it-säkerhet som motsvarar universitetets krav.