

IT-policy Student

### **Användning av Högskolans IT-infrastruktur**

Till högskolans nätverk ges högskolans studenter rätt att använda befintlig datautrustning och infrastruktur för att utföra studier.

Utrustning får inte användas för andra ändamål utan godkännande av IT-chefen.

### **Internetanvändning**

Användning av Internet av studenter på högskolan är tillåten.

Missbruk av Högskolans tjänster är inte tillåten.

Exempel på olämplig användning av Internet är:

- Chatt program eller tjänster som inte är godkända av högskolan.
- Alla former av avsiktlig surfning, användning eller nerladdning av pornografiskt material är oacceptabelt och i fall där detta gäller barnpornografiskt material är detta brottsligt enligt lag. Upptäcks det av IT-avdelningens personal rapporteras det till närmaste enhetschef.
- Spel om pengar samt andra former av spelaktiviteter.
- Aktiviteter för personlig vinning t ex aktiv handel med aktier eller fonder.
- Underhållning. Att lyssna på musik över Internet är inte tillåtet då det belastar Högskolans utgång till Internet.
- Det är inte tillåtet att på Högskolans datorer spela datorspel som erbjuds via Internet eller spelas på Internet.
- Visning eller publicering av information som tillhör högskolan utan särskilt tillstånd.
- Uppladdning och nedladdning av kommersiell mjukvara eller data utan särskilt tillstånd. Det är inte tillåtet att ladda ner musik (t ex MP3-filer), videosekvenser eller liknande för privat bruk.
- Försök att sabotera Högskolans Internetanslutning eller försök att reducera tillgängligheten till Internet.

### **Installation av program**

All installation av programvaror på ESH's datorer skall utföras av IT-avdelningens personal eller under deras vägledning. Detta för att säkerställa driften och ge en maximal kommunikation mellan de olika programmen i datorn.

Om IT-avdelningens personal upptäcker att det finns installerade program som inte har med arbetet att göra, kan dessa avinstalleras. Detta för att minimera risken för virus och öka driftsäkerheten.

### **Lagring av information**

Det tas ingen säkerhetskopia på information som lagras på den lokala dator det vill säga C:\ och ev D:\. Detta gäller även det som lagras på "Skrivbordet" och "Mina dokument".

IT-avdelningen tar inget ansvar för information som lagras på den lokala datorn vid eventuell service.

### **Datorhantering**

Student ansvarar för att låsa eller logga ut från dator då denne lämnar datorn obevakad, för att förhindra obehörigt användande av högskolans datorer.

### **Inkoppling av datorer i Högskolans nät.**

Denna policy och dessa regler gäller samtliga datorer och dess tillbehör såsom skrivare, skanner, PDA (handdatorer) m.m. som ägs av högskolan.

Det är inte tillåtet att ansluta egen dator, PDA eller annan datautrustning till högskolans fasta nätverk. Det är tillåtet att ansluta ovanstående utrustning till högskolans trådlösa nätverk för studenter.

### **Virusskydd**

Högskolan har ett antiviruskydd som möjliggör uppföljning av bl.a. antal virus per dator. Om det vid en sådan uppföljning framkommer att någon eller några datorer har onormalt mycket virus rapporteras det till närmaste enhetschef för utredning.

Det är ej tillåtet att ansluta en privat dator till ESH's trådlösa nätverk utan att ha ett uppdaterat och fungerande virusskydd.

### **Informationshantering och sekretess**

Alla studenter har ansvar för att skydda information från medveten eller omedveten förstörelse, ändring eller publicering.

Varje enhetschef skall med lämpliga mellanrum försäkra sig om att de system som används inom den egna verksamheten är säkra och uppfyller Person Uppgifts Lagen (PUL).

IT-enheten skall utveckla och publicera en Tekniskt PUL-handbok i enlighet med PUL-lagen. Dessutom skall IT-enheten försäkra sig om att regler och processer i handboken uppfyller krav från andra intressenter såsom landsting och kommuner.

All känslig personinformation skall vara skyddad från allmän insyn genom lämplig säkerhets- och tillgångskontroll.

### **Övervakning av system och systemanvändning**

IT-enheten skall säkerställa att alla system övervakas på ett sätt som gör det möjligt att tidigt identifiera användare i samband med missbruk eller intrång.