

## **Svenska handelshögskolans DATASÄKERHETSPOLICY**

Godkänd av Svenska handelshögskolans styrelse 10.2.2004.

Datasäkerhetspolicyn definierar datasäkerhetens mål, ansvarsområden och tillämpning vid Svenska handelshögskolan (nedan Hanken). Datasäkerheten är en del av Hankens kvalitetssystem och datasäkerhetsarbetet utgör en del av verksamhetens kvalitet. Datasäkerheten utgör en del av Hankens allmänna säkerhet.

### **Mål**

Syftet med datasäkerhetsarbetet är att förhindra en icke auktoriserad användning av data och datasystem eller en avsiktlig eller oavsiktlig förstörelse eller förvrängning av data samt att minimera skador som kan uppstå.

Hankens data, datasystem och datatjänster skyddas på ett adekvat sätt såväl under normala som under undantagsförhållanden med hjälp av administrativa, tekniska och övriga åtgärder.

Hankens mål är att arrangemangen gällande datasäkerheten är på god nationell och internationell nivå. Datasäkerhetens grundnivå täcker all databehandling inom Hanken. Olika enheters eller verksamheters eventuella behov av högre nivå av datasäkerhet skall kunna tillgodoses.

### **Datasäkerhet**

Med datasäkerhet avses tryggheten av databehandlingen. Datasäkerheten består av datas konfidentialitet, integritet och användbarhet samt till tillämpliga delar av oomtvistlighet och behörighetskontroll.

Konfidentialitet innebär att data är tillgängligt på överenskommet sätt på överenskomna tider endast för behöriga och att data inte röjs eller på annat sätt görs tillgängliga för obehöriga.

Integritet innebär att data och datasystem är tillförlitliga, korrekta och uppdaterade och inte har ändrats eller skadats av utrustnings- eller programfel, naturfenomen eller obehöriga mänskliga ingrepp.

Användbarhet innebär att data och databehandlingssystem är tillgängliga och användbara för behöriga användare inom en ur verksamhetens synvinkel rimlig tid.

Behörighetskontroll innebär att data eller datasystem inte kan användas utan tillstånd.

Oomtvistlighet innebär att man kan skapa en sådan bevisföring att ingen som har deltagit i databehandlingen eller dataöverföringen efteråt skall kunna förneka sin andel.

Datasäkerhetsarbetet innebär att planera och förverkliga åtgärder för att uppnå datasäkerhet. Till detta arbete hör de metoder, redskap och åtgärder som tryggar data, de resurser som avsätts för arbetet och redskapens datasäkerhetsegenskaper.

Datasäkerheten täcker Hankens alla databehandlingsuppgifter inklusive kontorsarbeten och därtill hörande arkivering. Datasäkerhetsåtgärderna omfattar elektronisk, audiovisuell, muntlig och skriftlig databehandling, dataöverföring och datalagring.

Hankens datasäkerhet baserar sig på nationell lagstiftning och internationella normer. Hankens datasäkerhet beaktar ytterligare de direktiv och rekommendationer som utfärdas angående statsförvaltningens datasäkerhet.

### **Ansvarsförhållanden**

Datasäkerheten är en gemensam angelägenhet för hela Hanken. Den utgör en del av den allmänna säkerheten.

Högsta ansvaret för datasäkerheten bär rektor och styrelse som beslutar om säkerheten inom Hanken.

Det operativa ansvaret för Hankens datasäkerhet hör till Datacentralen och ITR (Rådet för informationstjänster och informationsteknik).

Datasäkerhetschefen som verkar inom datacentralen har det operativa ansvaret för datasäkerhet och för utveckling och övervakning av datasäkerhetens förverkligande samt för utvecklingen av kunnandet om datasäkerhet vid Hanken inom ramen för de resurser och befogenheter datasäkerhetschefen har fått av Hankens ledning.

Var och en vid Hanken som behandlar data och som underhåller eller använder datasystem eller datanät är ansvarig för förverkligandet av datasäkerheten för sin del.

Varje datasystem eller del av ett sådant skall ha en entydig ansvarsperson. Ansvaret för registrerat data bärs av ansvarspersonen.

Hankens enheter beaktar i sina verksamhetsplaner de specifika kostnader som förverkligandet av datasäkerheten medför.

### **Verkställighet**

Hankens datasäkerhetspolicy ges för kännedom till hela personalen, studerande och alla användare av Hankens datasystem.

Uppnåendet av målen för datasäkerheten samt utvecklingen av densamma är en fortgående process som innehåller administrativa, fysiska och tekniska lösningar. De beskrivs i en datasäkerhetsplan för Hanken. Verksamheten regleras genom bestämmelser och anvisningar som ingår i datasäkerhetsplanen.

En säkerhetsklassificering av data och datasystem uppgörs. I den definieras datasäkerhetsnivåer och -åtgärder för varje datasäkerhetskategori.

Anvisningar och regelverk som styr datasäkerheten skall vederbörligen godkännas och delges varje målgrupp.

### **Information**

Datasäkerhetschefen ansvarar för information om datasäkerheten utanför Hanken och internt inom Hanken och ordnar utbildning för personalen.

### **Uppföljning och åtgärder**

Datasäkerhetschefen har rätt och skyldighet att kartlägga datasäkerheten för Hankens datasystem och vidta nödvändiga åtgärder för att avlägsna brister.

Varje användare av Hankens datasystem är skyldig att följa de regler och instruktioner som Hanken har godkänt för datasäkerhet.

Den som använder eller underhåller datasystem bör till datasäkerhetschefen anmäla brister i datasäkerheten, iakttaga missbruk som hör till datasäkerhetens område eller misstänkta datasäkerhetsbrott.

Missbruk kan leda till uppsägning av användaravtalet.