

# Informationssikkerhedspolitik

## for

# Københavns Universitet

Dette dokument er henvendt til alle, der er ansat eller studerer ved Københavns Universitet, eller i øvrigt har en tilknytning til Universitetet, og disse benævnes i det følgende interne brugere. Dokumentet er samtidigt en erklæring, henvendt til omgivelserne om at Universitetet forholder sig til Informationssikkerhed (IS) i overensstemmelse med anerkendte standards for at sikre og beskytte Universitetets informationsaktiver, samt for at bidrage til at understøtte Københavns Universitetets gode ry og anseelse.

## Indledning

Nærværende informationssikkerhedspolitik (IS-politik) er den overordnede ramme for informationssikkerheden på Københavns Universitet, i det følgende ofte blot benævnt KU eller Universitetet.

IS-politikken understøtter KU's strategiske handleplan – 2008 – 2012, der findes på <http://www.ku.dk/destination2012/>.

KU vil overholde den til enhver tid gældende danske standard for informationssikkerhed, samt dansk lovgivning og andre statslige retningslinjer.

Som et led i den overordnede sikkerhedsstyring tager Informations Sikkerheds Udvalget (ISU) på grundlag af den løbende overvågning og rapportering af hændelser informationssikkerhedspolitikken op til revurdering mindst én gang om året.

Revision af IS-politikken godkendes af Rektor efter indstilling fra ISU og behandling i hovedsamarbejdsudvalget.

## Formål

Data og informationer, samt informationssystemer til håndtering af disse, er nødvendige og vigtige for KU, og informationssikkerheden har derfor vital betydning for KU's troværdighed og funktionsdygtighed.

Formålet med informationssikkerhedspolitikken er at definere en ramme for beskyttelse af KU's informationer og særligt at sikre, at kritiske og følsomme informationer og informationssystemer bevarer deres fortrolighed, integritet og tilgængelighed, og derfor har KU's ledelse besluttet sig for et beskyttelsesniveau, der er afstemt efter risiko og væsentlighed samt overholder lovkrav og indgåede aftaler, herunder licensbetingelser.

Ledelsen vil oplyse alle KU's interne brugere om ansvarlighed i relation til KU's informationer og informationssystemer.

Hensigten med IS-politikken er at tilkendegive over for alle, at anvendelse af informationer og informationssystemer på KU er underkastet anerkendte standarder og retningslinjer, med det sigte at forebygge brud på informationssikkerheden, at begrænse skader som følge af disse, samt for at sikre muligheden for retablering af informationerne efter hændelsen.

## Omfang

Politikken omfatter KU's informationer, som er enhver information, der tilhører KU – herudover også informationer, som ikke tilhører KU, men som KU kan gøres ansvarlig for. Omfattet er fx således alle data om personale, data om finansielle forhold, alle data, som bidrager til administrationen af KU, forskningsdata, produktionsdata og anlægsdata samt informationer, som er overladt KU af andre. Disse data kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning eller enhver anden information, som kun er til intern brug.

Denne politik omfatter alle KU's informationer, ligegyldigt hvilken form de opbevares og formidles på.

Denne politik gælder for alle brugere uden undtagelse, både studerende, fastansatte og personer, som midlertidigt er tilknyttet KU.

Ved udlicitering af dele af eller hele IT-driften skal det sikres i samarbejdet med serviceleverandøren, at KU's sikkerhedsniveau fastholdes, således at serviceleverandøren, dennes faciliteter og de medarbejdere, som har adgang til KU's informationer, mindst lever op til KU's informationssikkerhedsniveau.

## Sikkerhedsniveau

Det er KU's politik at beskytte sine informationer og udelukkende tillade brug, adgang og offentliggørelse af informationer i overensstemmelse med KU's retningslinjer og under hensyntagen til den til enhver tid gældende lovgivning.

KU fastlægger på baggrund af en risikovurdering et sikkerhedsniveau som svarer til betydningen af de pågældende informationer. KU vil løbende gennemføre en afbalanceret risiko- og konsekvensvurdering under hensyntagen til de økonomiske forhold og Universitets formål.

Der gennemføres mindst en gang årligt, eller ved større forandringer i organisationen eller informationssystemerne, en risikovurdering, så ledelsen kan holde sig informeret om det aktuelle risikobillede.

Ledelsen har besluttet sig for at udvikle og administrere informationssikkerhedsstrategier, som sikrer et informationssikkerhedsniveau, der mindst svarer til de basale beskyttelsesforanstaltninger i DS 484:2005, og at dette er beskrevet i KU's IS-håndbog.

Det operationelle ansvar for den daglige styring af informationssikkerhedsindsatsen, jf. bilag 1, er placeret hos KU's it-sikkerhedsleder, der sikrer, at de aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger, der er beskrevet i sikkerhedshåndbogen, gennemføres og efterleves.

Ligeledes er det meget væsentligt, at informationssikkerhed integreres i alle relevante forretningsgange, driftsopgaver og projekter.

## **Sikkerhedsbevidsthed**

Informationssikkerhed vedrører universitetets samlede informationsflow, og gennemførelse af en informationssikkerhedspolitik kan ikke foretages af ledelsen alene. Alle brugere har et ansvar for at bidrage til at beskytte KU's informationer mod uautoriseret adgang, ændring og ødelæggelse samt tyveri. Alle brugere skal derfor løbende uddannes i informationssikkerhed i relevant omfang.

Alle interne brugere af KU's informationsaktiver skal følge informationssikkerhedspolitikken og de retningslinjer, der er afledt heraf.

Brugerne må kun anvende KU's informationsaktiver i overensstemmelse med den tilknytning, de har til universitetet, og skal beskytte disse på en måde, som er i overensstemmelse med deres følsomhed og/eller særlige kritiske natur.

## **Brud på informationssikkerheden**

Såfremt en bruger opdager trusler mod informationssikkerheden eller brud på denne, skal dette straks meddeles til den nærmeste ansvarlige for informationssikkerheden eller til ledelsen.

Hvem der er ens nærmeste ansvarlige for informationssikkerheden fremgår af KU's IS-hjemmeside, der findes på [informationssikkerhed.ku.dk](http://informationssikkerhed.ku.dk)

Brugere, som bryder informationssikkerhedspolitikken eller deraf afledte retningslinjer, vil blive udsat for disciplinære forholdsregler i overensstemmelse med KU's gældende regler og personalepolitik.

Revideret af ISU den 18.12.2008, behandlet på Direktørkoordineringsmødet den 19.01.2009, af Ledelsesteamet på mødet den 21.1.2009, af HSU på mødet den 18.2.2009 og herefter godkendt af rektor.

## Bilag 1 – Anvendelse i praksis

De retningslinjer samt sikkerheds- og kontrolforanstaltninger, der gælder på Københavns Universitet, er samlet i IS-Håndbogen, der følger den samme punktinddeling, som anvendes i DS 484:2005.

Sikkerhedshåndbogen indeholder en beskrivelse af de informationssikkerhedsområder, der er relevante for Københavns Universitet.

Det operationelle ansvar har til formål :

- at sikre, at informationssikkerhedspolitikken og afledte retningslinjer implementeres
- at sikre en bestemmelse af værdien af de informationer, som er nødvendige for KU, samt at træffe rimelige forholdsregler til beskyttelse af disse informationer, herunder at afse de nødvendige midler og ressourcer hertil
- at der udpeges system- og informationsejere for samtlige informationer og informationssystemer
- at klassificere og beskytte de informationer, som KU har ansvaret for
- at forebygge og begrænse risici til en for KU kendt og accepteret størrelse
- at udarbejde regler for informationskontrol og beskyttelse, som skal følges af de medarbejdere, der behandler og anvender informationerne
- at etablere regler for adgang og brug af informationer samt at sikre, at disse løbende bliver vedligeholdt og om nødvendigt revideret
- at definere reglerne for arkivering af informationer, således at disse altid kan genskabes senere inden for en kendt og accepteret tidshorisont
- at udarbejde en brugbar plan til at reetablere daglig drift, såfremt informationerne eller informationssystemerne ødelægges, uanset af hvilken grund, således:
  - at omfanget af og konsekvenserne ved nødsituationen kan minimeres
  - at væsentligste dele af den daglige forretningsmæssige drift på KU kan gennemføres via alternative forretningsgange
  - at alle relevante berørte parter holdes orienteret i fornødent omfang
  - at den fulde drift af informationssystemerne kan genoptages inden for en kendt og accepteret tidshorisont
- at sikre, at enhver sikkerhedsmæssig følsom informationsaktivitet kan henføres til den person, som har udført aktiviteten, samt at sikre gennemførelse af de fornødne kontroller til opdagelse af misbrug eller forsøg herpå
- at etablere regler for rettighedstildeling og funktionsadskillelse, som skal forebygge og begrænse konsekvenser af fejl, uheld og negative handlinger, der bevidst er foretaget af enkeltpersoner
- at sikre, at KU's udvikling og implementering af systemer udføres under iagttagelse af betryggende sikkerhedsforanstaltninger
- at sikre, at KU's leverandører overholder de sikkerhedsforskrifter, som er gældende for KU's informationer, faciliteter og medarbejdere i samarbejdet med universitetet
- at træffe de nødvendige forholdsregler for at sikre, at informationssikkerhedspolitikken og afledte retningslinjer bliver overholdt
- at sikre den fornødne ledelsesrapportering af status for informationssikkerheden, herunder aktiviteter og hændelser.