Handläggare, telefon
Gustavo Navarro 46 (0)790603180



KUNGL. KONSTHÖGSKOLAN
ROYAL INSTITUTE OF ART

# Policy för informations- och IT-säkerhet vid Kungl. Konsthögskolan

| | |
|---|---|
| Typ av dokument | Policy |
| Beslutat av | Rektor |
| Giltighetstid | 2024-02-19-tills vidare |
| Ersätter dokument | Policyhandbok för informationssäkerhet, beslutad av styrelsen 2010-11-08, senast uppdaterad 2014. |
| Ansvarig förvaltningsenhet | Fastighet och IT |

Handläggare, telefon
Gustavo Navarro 46 (0)790603180

Ert datum

Er referens

# Allmänt

Denna policy omfattar Kungl. Konsthögskolans ledningssystem för informationssäkerhet. Samtliga anställda och studenter ska få tillgång till policyn. Policyn ska finnas lättillgänglig på högskolans intranät. Informationssäkerheten ska bygga på en rimlig risknivå. IT-säkerheten vid KKH ska förhindra att störningar i datanät, datorer och datasystem och övriga digitala resurser orsakar allvarliga konsekvenser för KKH, för anställda eller studerande vid KKH.

Policyn tar upp grundförutsättningar för att skapa en god informationssäkerhet vid högskolan och utgör ledningens syn på verksamheten, samt ligger till grund för regler och ruiner inom organisationen.

# Policy för Informations- och IT-säkerhet

## Inledning

Informationssäkerhet omfattar all information och gäller dokument, indata och utdata samt det som hanteras med högskolans digitala resurser dvs. datorer, datornät och all annan utrustning som nyttjas i samband med hantering av information. Information ska arkiveras i enlighet med Riksarkivets föreskrifter. Målet för informationssäkerheten är att inom KKH skapa ett effektivt skydd mot olika hot genom att tillförsäkra följande:

- att informationen sparas i en säker miljö
- att informationen är lättillgänglig (Förutsätter central lagring)
- att informationen kan återskapas inom skälig tid efter gällande förutsättningar
- att informationen ska skyddas mot avsiktlig och oavsiktlig förvanskning
- att endast den som är behörig får tillgång till informationen
- att det är möjligt att spåra upphovspersonen
- att utförda bearbetningar och andra operationer skall vara möjliga att härleda genom befintliga rutiner till enskild användare och tidpunkt.

Handläggare, telefon
Gustavo Navarro 46 (0)790603180



## Allmänna säkerhetskrav

- Informationssäkerheten ska alltid vara anpassad till rådande hotbild och aktuella risker, till verksamhetens krav och till systemens utformning och användning,
- Informationssäkerhetsarbetet ska samordnas med övrigt säkerhetsarbete vid KKH.
- IT-säkerheten i nät, datorer och datasystem anslutna till SUNET (Swedish University Computer Network (”SUNET”) ska uppfylla SUNETs krav på anslutna organisationer.
- Tillgång till KKH:s datorer, nät, system och övriga digitala resurser förutsätter att ansvarsförbindelse tecknas mellan användare och KKH. Se bilaga 1 ansvarsförbindelse

## Ansvar

- Ansvaret och delegationsordningen för informations- och IT-säkerheten fastställs av rektor, se bilaga 2 delegationer.
- För datorer, datasystem, datanät eller datautrustning som används vid KKH ligger säkerhetsansvaret hos IT-ansvarig,
- KKH ska ha en gemensam central funktion som ansvarar för stöd, samordning och kontroll av informationssäkerheten vid KKH,
- IT-enheten ansvarar för att informationssäkerheten kontrolleras regelbundet, och att ledningen informeras om säkerhetsläget,
- Rutiner för kontinuitetsplanering, avbrottsplan och krisorganisation ska upprättas,
- För att säkerställa att rätt säkerhetsnivå upprätthålls ska systemansvariga eller verksamhetsansvariga ta fram detaljerade anvisningar för system inom ansvarsområdet där så är nödvändigt.
- Hantering, förvaring och arkivering av diarieförd information ska ske så att den skyddas mot förlust, skada samt obehörig användning.

## Avrop av IT-system och tjänster

- Vid avrop av nya datasystem, datorer, nät, datautrustning, datordrift eller relaterade tjänster ska IT-säkerhetskraven alltid beaktas och ingå i kravspecifikationen.
- Då leverantör utför tjänst eller uppdrag åt KKH, ska KKH genom avtal, försäkra sig om att leverantören följer KKH:s krav gällande Informationssäkerhet.

## Kontroll

- Informationssäkerheten vid KKH ska kontrolleras regelbundet.
- För digitala resurser som är av stor betydelse för KKH:s verksamhet och rykte, eller för KKH:s personal eller studerande, ska kontroll genomföras årligen.
- Resultaten av kontrollen ska redovisas för KKH:s ledning.

Handläggare, telefon
Gustavo Navarro 46 (0)790603180

Ert datum

Er referens

# Regler för användning av KKH:s digitala resurser

## Behörig användare

Vid nyttjande av högskolans IT-resurser ska hänsyn tas till KKH:s namn, anseende och goda varumärke. Behörig användare är den som tilldelats behörighet att använda högskolans IT-resurser. Behörig användare är inskriven student, personal, affilierad professor eller forskare. Doktorander som ej hunnit avsluta sitt studieprojekt kan få dispens av Prefekt och således förlängning av behörighet.

## Användning av e-post

- All kommunikation som avser högskolans verksamhet ska ske genom av högskolans tilldelat e-postkonto.
- Personal ska använda sitt tilldelade e-postkonto för intern och extern kommunikation.
- Kommunikation mellan personal och studenter ska primärt ske via ovanstående e-postkonto och
- studenternas e-postkonto tilldelat av KKH.
- E-post får inte användas för politiska, kommersiella eller andra syften som strider mot högskolans verksamhet eller statlig värdegrund.

## E-post kopplat till allmän handling

- Reglerna om allmänna handlingars offentlighet (Tryckfrihetsförordningen 2 kap.) omfattar även e-post.
- Information som kan bli föremål för sekretess i enlighet med Offentlighets- och Sekretesslagen ska hanteras enligt särskilda regler.
- Vid frånvaro ska inkommande e-post av brådskande karaktär hänvisas till info@kkh.se.

## Distansåtkomst

- Högskolan tillhandahåller de IT-tjänster som ska vara tillgängliga vid distansåtkomst.
- Dator, mobil/motsvarande som används för distansåtkomst ska vara säker utifrån informationssäkerhetssynpunkt.
- Användarreglerna i ansvarsförbindelsen ska respekteras även vid användande av högskolans IT-resurser via distansåtkomst.

## Regler för val av lösenord och autentisering

Lösenord ska hållas hemliga och väljas med omsorg i syfte att försvåra avslöjande. Hela systemets säkerhet är beroende på hur var och en hanterar sitt lösenord och sin identitet. Lösenord ska följa KKH:s lösenordspolicy se bilaga 7.
Samtliga anställda vid KKH ska använda tvåfaktorsautentisering.

## Allmänna handlingar och personuppgifter

Information som behandlas via högskolans IT-resurser kan utgöra allmän handling.
Allmänna handlingar ska behandlas i enlighet med tryckfrihetsförordningen.
Personuppgifter är skyddsvärd information och ska behandlas i enlighet med dataskyddsförordningen (GDPR).

### Kontroll och övervakning av IT-system

Användare som vid nyttjande av högskolans IT-resurser upptäcker fel eller annat som kan vara av betydelse för IT-resursernas driftsäkerhet eller systemdrift, ska genast rapportera detta till IT-enheten.

IT-resurserna övervakas kontinuerligt, och händelser på datornät och inom de övriga IT-resurserna loggas. Dessa loggar sparas och arkiveras i enlighet med gällande regler om gallring och arkivering och kan vid behov utgöra bevis för eventuell överträdelse av användarreglerna.

## Påföljder vid överträdelse av användarregler

### Avstängning från IT-resurs

Vid överträdelse av dessa användarregler kan användaren riskera att bli helt eller delvis avstängd från högskolans IT-resurser. Användaren kan dock bli anvisad till dator med begränsade resurser så att användaren kan fullgöra sina studier/arbetsuppgifter under tid för eventuell utredning.

### Disciplinära påföljder för studenter

Student kan vid överträdelse av ansvarsförbindelsen riskera att anmälas till rektor och disciplinnämnd i enlighet med 10 kapitlet Högskoleförordningen. De disciplinära påföljderna är varning eller avstängning under en viss tid från undervisningen och annan verksamhet vid högskolan.

### Disciplinära påföljder för medarbetare

Medarbetare kan vid överträdelse av användarreglerna riskera att anmälas till rektor och personalansvarsnämnd. De disciplinära påföljderna är varning eller avstängning.

### Brott

Användare som misstänks för brott enligt brottsbalken kan bli föremål för polisanmälan.

Handläggare, telefon
Gustavo Navarro 46 (0)790603180

Ert datum

Er referens

# Samordning av informationssäkerheten vid KKH

## Inledning

Ansvaret för informationssäkerheten följer den vid högskolan gällande delegationsordningen.
Den verksamhet som bedrivs på Högskolan förutsätts effektivt nyttja befintliga IT-resurser. En förutsättning för detta nyttjande är att dessa uppfattas som säkra och tillförlitliga.
Arbetet med informationssäkerheten vid högskolan bör därför ges en central betydelse.

## Uppgifter

IT- enheten har ett särskilt ansvar för att informationssäkerheten vid högskolan är tillräcklig för att skapa trovärdighet i hantering av högskolans information, samt har i uppdrag att samordna och revidera informationssäkerhetsarbetet vid högskolan. IT-enheten har i uppdrag att kontinuerligt se till att informationssäkerheten upprätthålls i enlighet med riktlinjer och övriga regler. IT-enheten har därtill uppdrag att föreslå, initiera utvecklingsprojekt samt följa upp informationssäkerhetsåtgärder. IT-enheten ska vidare ingå som expertfunktion i alla större IT-projekt. IT-enheten rapporterar löpande till ledningen vid högskolan. Se även sid 11 och avsnittet delegationer.

## Arbetsformer

- Uppdraget att tillse en hög informationssäkerhet utförs av IT-ansvarig. Som stöd ska Fastighets- och IT-chefen ansvara för revision informationssäkerhet.
- IT-ansvarig ställer krav på säker drift och ansvarar för att driften är säker i enlighet med högskolans riktlinjer och övriga regler.
- IT-ansvarig ska samverka med Fastighets- och IT-chefen samt även med systemansvariga och projektledare.

## Incidenthantering

IT-enheten ansvarar för bedömning beträffande vilka sorts incidenter som kan påverka säkerheten i KKH:s informationssystem. Vid bekräftat eller misstänkt intrång, ska IT-enheten agera snabbt och adekvat samt kontakta systemansvarig och SUNET Cert för vidare samverkan. Varje steg i incidenthanteringen inklusive jourutryckning ska dokumenteras. Samtliga drabbade ska informeras om incidenten snarast möjligt.

För utredning av incidenter används lagrade loggfiler. IT-enheten kan vid behov kopiera, flytta eller radera data, med respektive informationsägares godkännande. Radering får dock inte ske utan tillstånd, utom vid sparande av data på annan utrustning eller när lagring strider mot högskolans regler.
Om så krävs kan berörda delar av driften komma att stoppas.

### Vid allvarliga incidenter

En allvarlig incident innebär allvarlig påverkan på säkerheten i den informationshantering som KKH ansvarar för eller påverkan på KKHs förmåga att utföra sitt uppdrag.
Vid en sådan situation ska IT-enheten rapportera till Myndigheten för Samhällsskydd och Beredskap inom sex timmar.
IT-ansvarig ska säkerställa samverkan och överlägga med SUNETS expertgrupp inom rimlig tid.

# Ansvar för informationssäkerheten vid KKH

Varje verksamhetsansvarig ansvarar för att informationssäkerheten inom sin verksamhet bedrivs i enlighet med högskolans policy och övriga regler. Verksamhetsansvarig kan delegera uppgifter till särskilda funktioner. Se bilaga 2 delegationsordning.

**Utbildning**
Alla användare ska informeras om högskolans policy för Informationssäkerhet samt i förekommande fall ges undervisning i ämnet. Policyn ska finnas lättillgängliga via KKHs intranät.

**Kontinuitetsplanering och Avbrottsplan**
För de kritiska IT-systemen finns en plan över vilka system som ska prioriteras vid återställande.

**Krisorganisation**
I enlighet med högskolans Krishanteringsplan finns det instruktioner för hur IT-enheten ska hantera IT-relaterade frågor vid en krissituation.
I Krishanteringsplanen finns det definierat vad som behöver prioriteras samt checklistor för olika faser i krisen. Detta avser den initiala fasen såväl som fortsättningsfasen. IT-enheten har ett stort ansvar för initialt iordningsställa krisledningsrummet.

# Skyddsåtgärder

## Skydd av drift och datakommunikation

- Fysisk säkerhet
- Brandväggar
- Redundans i nät och utrustning
- Säkerhetskopiering
- Reservkraft
- Program mot skadlig kod

KKH använder brandväggar.
Serverhallen är skyddad mot brand, vatten och inbrott. Serverhallen är larmad 24/7/365.
Redundans erhålls genom dubbla speglade servrar.
Säkerhetskopiering sker varje dag med inkrementella backupper till disk på separat server, data sparas normalt ca 6 månader tillbaka i tiden.
Säkerhetskopieringen kontrolleras genom felrapporter och periodvisa återläsningstest.
Reservkraft finns inte, däremot används UPS på samtlig utrusning för kontrollerad nedtagning av maskinerna.
Det finns även en server med installerat övervakningssystem.

## Åtkomst och behörighetsstyrning

Se avsnitt användning av högskolans digitala resurser.

## Systemutveckling, systemanskaffning och systemavveckling

Vid utveckling, anskaffning och avveckling av system ska informationssäkerheten alltid beaktas. Avveckling av system ska ske så att befintlig information kan flyttas till nytt system eller arkiveras/gallras.

## Incidentrapportering och incidenthantering

Se avsnittet om incidenthantering

## Granskning och uppföljning

Se Bilaga 3 - IT-ansvarig

# Bilagor

1. **Ansvarsförbindelse**
2. **Delegationer**
3. **IT-ansvarig**
4. **Systemansvarig**
5. **Säker systemdrift**
6. **Arkivansvarig**
7. **Lösenordspolicy**

---

# Bilaga 1 – Ansvarsförbindelse

**Ansvarsförbindelse för användning av KKH:s dator-, nät- och systemresurser**

Datorresurser, datornät, kringutrustning och konton ägs och drivs av KKH för användning i av KKH auktoriserad verksamhet. All annan verksamhet, är enbart tillåten när den:

- ordinarie användningen inte störs
- inte innebär brott mot dessa föreskrifter
- inte står i strid med skolans regler, KKH:s föreskrifter, SUNET:s regler eller gällande lagstiftning

Med behörig i dessa föreskrifter avses person som tilldelats konto eller annan som fått tillåtelse att använda KKH:s dator-, nät- eller systemresurser.

**För innehavare av behörighet gäller följande:**

Behörigheten och därtill hörande resurser är personlig och ska inte delas med andra.
Lösenordet som tillhör behörigheten måste hållas hemligt. För detaljerad information om lösenordsregler se bilaga 7 KKH:s lösenordspolicy.
Behörigheten är tidsbegränsad och upphör när studierna, anställningen, projektet eller motsvarande avslutas. KKH har rätt att inaktivera behörighet som varit inaktiv i mer än sex månader om ingen annan överenskommelse finns.

**För användning av KKH:s dator-, nät- och systemresurser gäller följande:**

- Intrång eller försök till intrång, sabotage, störande verksamhet riktat mot KKH:s system, externa system, samt andra användarkonton är förbjudet
- Det är inte tillåtet att utnyttja felkonfigureringar, programfel eller andra metoder i syfte att skaffa utökade systemrättigheter eller åtkomst utöver dem som beviljas av systemadministratörer
- Kommersiell användning av KKH:s datorresurser är förbjuden om inte annat överenskommits. KKH kan i sådana fall inte ansvara för systemens funktion eller tillgänglighet
- Upptäckta fel, sårbarheter, överträdelser eller andra oegentligheter måste omedelbart rapporteras till systemadministratörerna via IT-support
- Bara material där det klart framgår att spridning är tillåten får kopieras eller distribueras. Upphovsrättsskyddat innehåll får endast delas med tillstånd från upphovsrättsinnehavaren

**IT-resurserna får inte användas på ett sätt som:**

- bryter mot gällande lagstiftning, till exempel hets mot folkgrupp, barnpornografibrott, olaga våldsskildring, förtal, ofredande, dataintrång eller upphovsrättsbrott,

**Påföljder och åtgärder vid regelbrott**

- KKH kommer att anmäla brott mot dessa föreskrifter samt gällande lagstiftning till disciplinnämnden och/eller polis, vilket kan leda till kontohavarens avstängning från studier och/eller rättsliga påföljd.
- Systemansvariga har rätt att vid grundad misstanke om regelbrott blockera användarkonton och hindra tillgång till KKH:s dator-, nät-, och systemresurser.

Gällande föreskrifter finns tillgängliga via KKH:s webbplats: http://www.kkh.se/.
Jag förbinder mig att hålla mig informerad om och följa gällande föreskrifter för användning av KKH:s datorsystem. Härmed intygas att jag idag tagit del av dessa föreskrifter.
Jag är även medveten om att ovarsam användning och underlåtenhet att följa KKH:s anvisningar kan medföra att tillgång till dator-, nät-, och systemresurser stängs av.

Underskrift

**Namnförtydligande**

Datum

Personnummer

**ID-kontroll** Ifylles ej av sökanden

Handläggare, telefon
Gustavo Navarro 46 (0)790603180

Ert datum

Er referens

# Bilaga 2 - Delegationer

I enlighet med denna delegation beslutar Rektor att informationssäkerheten ska organiseras enligt följande, där en medarbetare kan inneha fler funktioner:

- att det ska finnas en IT-ansvarig för samordning av informationssäkerhetsarbetet. IT-ansvarig rapporterar löpande till rektor/ledning
- att den verksamhetsansvarige är ansvarig för informationssäkerheten inom sitt verksamhetsområde i enlighet med lärosätets policy, riktlinjer och regler
- att den verksamhetsansvarige får delegera till en särskild person att vara informationssäkerhetsansvarig till exempel Systemadministratör
- att systemansvarig är ansvarig för informationssäkerheten i respektive IT-system
  att systemansvariga utdelar behörigheter, se bilaga 4 Systemansvarig
- att den verksamhetsansvarige utser en arkivansvarig med ansvar enligt beskrivning för Arkivansvarig. Se även bilaga 6 Arkivansvarig

Denna delegationsordning ses över minst en gång per år i anslutning till årsskiftet.

Handläggare, telefon
Gustavo Navarro 46 (0)790603180

Ert datum

Er referens

# Bilaga 3 - IT-ansvarig

Rektor delegerar till Förvaltningschef som delegerar till Fastighets- och IT-chef som vidaredelegerar ansvar, de befogenheter och skyldigheter som ankommer på IT-ansvarig

Huvudsakliga uppgifter för informationssäkerhetsfunktionen:

**Beredning och kontroll**
- Förbereda informationssäkerhetsfrågor för beslut
- Skapa och följa upp handlingsplaner och budgetar i samråd med IT-chef årsvis
- Utveckla och följa upp riktlinjer och regler
- Ansvara för utveckling av systematiska metoder för granskning av informationssäkerheten
- Genomföra årliga säkerhetsgranskningar av enheter och system
- Sammanställa och rapportera granskningsresultat till ledningen

**Krav och bevakning**
- Formulera och upprätthålla säkerhetskrav vid upphandling och avrop
- Ställa säkerhetskrav vid drift av system, datorer och nät
- Rapportera och koordinera incidenthantering med SUNET CERT
- Övervaka och följa upp IT-projekt och beslut

**Stödjande verksamhet**
- Fastställa och rekommendera säkerhetsnivåer och standarder för IT-system
- Utveckla åtgärdsförslag och handlingsplaner
- Tillhandahålla expertstöd och utbildning

**Tekniskt ansvar**
- Garantera att nya IT-system kan integreras utan att kompromissa med informationssäkerheten
- Registrera IT-system i systemförteckningen och genomföra säkerhetsanalyser
- Se till att systemansvarigas säkerhetskrav och kompetens uppfylls
- Vid behov, rapportera missbruk eller misstänkt missbruk av IT-resurser och medverka i efterföljande utredningar

**Övrigt**
- Vid misstanke om brott, bistå disciplinnämnd, polis och åklagare i utredning
- Tystnadsplikten inskränks inte av dessa uppgifter i enlighet med tryckfrihetsförordning och sekretesslagen

Handläggare, telefon
Gustavo Navarro 46 (0)790603180

Ert datum

Er referens

# Bilaga 4 - Systemansvarig

För varje system finns en systemansvarig. Utöver det ansvar som anges i IT-policyn har denne även ansvar för informationssäkerheten i sitt system och att gällande riktlinjer för informationssäkerhet följs
Samverkan och samråd ska ske kontinuerligt med IT-ansvarig

**Systemansvarig ansvarar dessutom för:**

Vid systemanskaffning- och utveckling:

- att det planerade IT-systemet utformas och förvaltas så att det uppfyller kraven på god informationssäkerhet
- att projektorganisationen har tillgång till erforderlig informationssäkerhetskompetens
- att i de fall personuppgifter kommer att ingå i det planerade systemet, att detta dokumenteras och anmäls till lärosätets personuppgiftsombud samt att systemet utformas så att det uppfyller personuppgiftslagens krav

Vid befintliga system:

- att analys av säkerhetsbehov genomförs med hänsyn till informationsinnehåll och verksamhetskrav
- att säkerhetskraven anges med inriktning på tillgänglighet, riktighet, sekretess och spårbarhet
- att samverka med IT-driftansvarig för systemets drift och underhåll
- att riktlinjer för behörighetstilldelning utarbetas i samverkan med informationssäkerhetsansvarig
- ansvarar för uppföljning av och tilldelning av behörighet i enlighet med av informationssäkerhetsansvarig fastställda riktlinjer
- ansvarar för inregistrering och avregistrering av behörighet
- ansvarar för att beslut om behörighetstilldelning arkiveras enligt fastställda arkivkrav.

Handläggare, telefon
Gustavo Navarro 46 (0)790603180

Ert datum

Er referens

# Bilaga 5 - Säker systemdrift

Fastighets- och IT-enheten ansvarar för en säker systemdrift genom

- att informationssäkerhetskraven appliceras på de system som de sköter driften för
- att ansvara för den fysiska säkerheten i serverrum med el, tillgänglighet, brandskydd, fuktskydd samt att endast behöriga tillåts komma in
- säkerhetskopiera i två generationer
- att samverka med och ta fram underlag till informationssäkerhetsansvarig
- att administrera konton för användning av högskolans digitala resurser
- hantera incidenter
- rapportera incidenter samt hantera samordning med SUNET CERT och MSV Iron
- att bevaka utveckling inom området
- sköta samverkan med övriga lärosäten, med SUSEC och SUNET

**Förteckning över Kungliga Konsthögskolans system och systemansvariga**
Tillhör bilaga 5.

| **Administrativa system** | **Systemansvarig** |
|---|---|
| Nätverk/Server | IT-ansvarig |
| Ladok | Chef Utbildnings- och forskningsenheten |
| Antagningssystem | Chef Utbildnings- och forskningsenheten |
| Ekonomisystem (Agresso) | Förvaltningschef |
| System för arkivering | Chef Utbildnings- och forskningsenheten |
| System för diarieföring | Chef Utbildnings- och forskningsenheten |
| Inpasseringssystem | Chef Fastighet och IT |
| Maskinbehörighetssystem | Lärare i metall/Trä |
| Telefonisystem | IT-ansvarig |
| Personalsystem | HR-chef |
| Intranät | Kommunikationsansvarig |
| Hemsida | Kommunikationsansvarig |

Handläggare, telefon
Gustavo Navarro 46 (0)790603180

Ert datum

Er referens

# Bilaga 6 - Arkivansvarig

Lärosätets arkiv ska spegla verksamheten och är en källa till nutida och framtida forskning såväl som ett stöd i den dagliga verksamheten.
Hantering och förvaring av information ska ske så att den skyddas mot förlust, skada och obehörig användning.

**Högskolans arkivarie ansvarar för**

- att offentlighet och sekretess, registrering, arkivbildning, arkivredovisning samt vård av arkiv sker i enlighet med Riksarkivets föreskrifter, lagar och förordningar
- att gallringsföreskrifter finns och uppdateras vid behov
- att hantering och förvaring av information sker i enlighet med lärosätets föreskrifter för informationssäkerhet.

Handläggare, telefon
Gustavo Navarro 46 (0)790603180



# Bilaga 7 - Lösenordspolicy

## 1 Inledning

Detta dokument anger Kungl. Konsthögskolans policy för kvalitet på samt hantering av lösenord i enlighet med identitetsfederationen SWAMIDs policy.

## 2 Ansvar

### 2.1 Efterlevnad

Som användare av Kungl. Konsthögskolans informationssystem ansvarar du själv för:

- att dina lösenord uppfyller den kvalitet och hantering som anges i denna policy.
- att du håller dina lösenord hemliga.
- att, som en del av ovanstående punkt, aldrig uppge dina lösenord till någon som efterfrågar dem via e-post, i telefon eller på annat sätt.

För system som är kopplade till Kungl. Konsthögskolans gemensamma inloggnings- och autentiseringsrutiner (Webbinloggning, LDAP och Active Directory) finns systemstöd för efterlevnad av policyn.

För system med egen lösenordshantering är det systemägare som ansvarar för efterlevnad av denna policy.

## 4 Syfte

Det övergripande syftet med denna policy är att så långt det är möjligt skydda Kungl. Konsthögskolans lösenordsskyddade informationssystem från obehöriga användare.

## 5 Strategier

Alla informationssystem (applikationer) ska vara kopplade till Kungl. Konsthögskolans gemensamma inloggningstjänst om inte särskilda skäl föreligger.

Kungl. Konsthögskolans gemensamma inloggningstjänst innehåller teknikstöd för god lösenordskvalitet och säker lösenordshantering, se pkt. 6.1 och 6.2.

Varje användare har ett lösenord för inloggning till Kungl. Konsthögskolans IT-tjänster. Därutöver kan verksamhets- och/eller systemspecifika lösenord finnas.

Tvåfaktorautentisering ska användas för åtkomst till IT-tjänster eller system (applikationer) som enligt Kungl. Konsthögskolans policy för informationsklassificering innehåller konfidentiell information med HÖGA eller SÄRSKILDA KRAV på att skydda informationen från obehöriga användare.

## 6 Omfattning

Policyn för lösenordshantering gäller för alla IT-tjänster och system (applikationer) vid Kungl. Konsthögskolan.
Policyn omfattar två områden, lösenordskvalitet och lösenordsskydd.

## 6.1 Lösenordskvalitet

### 6.1.1 Lösenordssammansättning

Ett lösenord ska vara sammansatt på följande sätt:

- Bestå av minst 8 tecken.
- Vara sammansatt av följande tecken:
- A – Z
- a – z
- 0 – 9
- mellanslag
- följande specialtecken: ~,!, @, #, $, %, ^, &, (, ), _, +, -, *, /, =, {, }, [, ], |, \, :, ;, ’ (enkelt
- citationstecken), ” (dubbelt citationstecken), <, >, , (kommatecken), . (punkt), och ?.
- Innehålla minst en versal, minst en gemen och antingen minst ett specialtecken eller en siffra.
- Användaren ska uppmanas att inte sätta samma lösenord som de använder i antingen andra interna eller externa IT-tjänster.

### 6.1.2 Lösenordskontroll

I Kungl. Konsthögskolans gemensamma inloggningstjänst finns teknikstöd för att säkerställa god lösenordskvalitet. Vid lösenordsbyte kontrolleras att dessa lösenord med avseende på att de:

- är sammansatta enligt pkt. 6.1.1 ovan,
- inte återfinns i en katalog med lösenord av dålig kvalitet (123456, egennamn, årstider, bilmärken etc.)[1],
- inte är detsamma som det närmast föregående och
- inte är samma som användarens övriga lösenord i den gemensamma inloggningstjänsten, t.ex. lösenordet för inloggning i trådlösa nät1.

Lösenordet går inte att spara förrän det uppfyller minimikraven.

[1]I Active Directory och andra nyckelfärdiga system är det inte alltid möjligt att genomföra kontroller enligt punkt två och fyra. Om detta gäller er är det rekommenderat att kravet på minsta lösenordslängd ökas med två tecken till tio tecken.

### 6.1.3 Undantag

Om det i enskilda system som inte är kopplade till den gemensamma inloggningstjänsten föreligger särskilda tekniska skäl för att inte följa ovanstående policy för god lösenordskvalitet ska undantag godkännas av systemägare och dokumenteras i systemets förvaltningsspecifikation eller motsvarande dokument. Vidare måste särskild hänsyn tas vid åtkomst av data hämtade från andra system.

## 6.2 Lösenordsskydd

### 6.2.1 Datalagring och transport av lösenord

För att reducera risken för obehörig åtkomst till lösenord gäller följande policy för lagring och transport av lösenord:

- Lösenord ska alltid lagras och transporteras i krypterad form. Detta gäller även backupmedia.

- Lösenord ska aldrig presenteras i läsbar form.
- Lösenord ska aldrig kommuniceras via epost, telefon eller motsv.
- IT-personal med teknisk åtkomst till de datorer och datamedia där lösenord lagras ska underteckna särskilda ansvarsförbindelser.

### 6.2.2 Skydd mot nätbaserade gissningsattacker (Rate limiting)

För att reducera risken för automatiserade gissningsattacker mot lösenord ska inloggningen vara skyddad genom s.k. rate limiting som förhindrar en inkräktare att göra många upprepade lösenordsgissningar på kort tid.

I Kungl. Konsthögskolans gemensamma inloggningstjänst är detta utformat enligt följande:

- 10 felaktiga gissningar innan automatisk kontolåsning.
- 5 minuters automatisk kontolåsning efter maximalt antal felaktiga gissningar.
- Räknaren över antalet felaktiga gissningar nollställs efter korrekt inloggning eller efter 60 minuter efter senaste felaktiga inloggningsförsök.

### 6.2.3 Lösenordsbyte

För att ytterligare reducera risken att en inkräktare avslöjar ett lösenord till Kungl. Konsthögskolans IT- och informationssystem ska varje användare kontinuerligt byta lösenord inom ett fastställt tidsintervall.

I Kungl. Konsthögskolans gemensamma inloggningstjänst gäller följande regler för lösenordsbyte:

- Tvingande lösenordsbyte senast inom 12 månader för anställda, övriga verksamma samt för s.k. funktionskonton.
- Tvingande lösenordsbyte senast inom 5 år för studenter.

### 6.2.4 Undantag

Om det i enskilda system föreligger särskilda tekniska skäl för att inte följa ovanstående policy för lösenordsskydd ska undantag godkännas av systemägare och dokumenteras i systemets förvaltningsspecifikation eller motsvarande dokument. Vidare måste särskild hänsyn tas vid åtkomst av data hämtade från andra system.

## 7 Definitioner

### 7.1 Lösenordskvalitet.

God lösenordskvalitet innebär att ett lösenord är tillräckligt långt och komplext sammansatt för att reducera risken för att en inkräktare kan gissa sig till rätt lösenord. Två saker avgör svårigheten i att gissa ett lösenord: längden och komplexiteten på lösenordet. Med hjälp av dessa kan man räkna ut lösenordets entropi. Ju högre entropi ett lösenord har desto svårare är det att gissa det. Se pkt. 6.1 och bilaga 1 för vidare information.

### 7.2 Lösenordsskydd.

Säker lösenordshantering innebär, förutom att varje användare ansvarar för att hålla sina lösenord hemliga, att inloggningstjänsten skyddar lösenord från otillbörlig åtkomst och användning. Se pkt. 6.2 för vidare instruktioner.

**7.3 Tvåfaktorautentisering.**
Inloggning med två skilda faktorer; till exempel ett lösenord och ett godkännande i en autentiseringsapp.