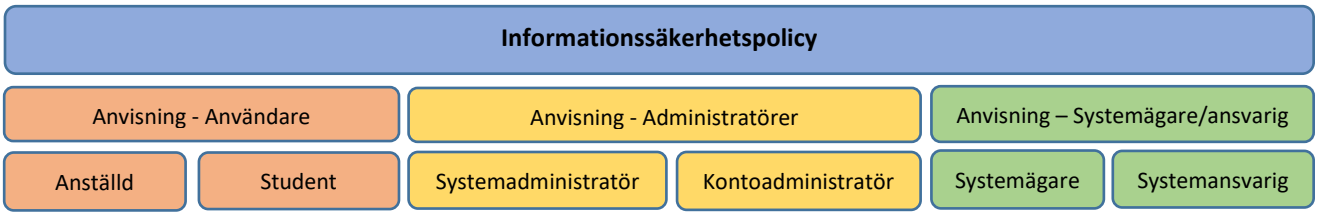
Dnr 2019-114-519

Högskolan Kristianstad
291 88 Kristianstad
044 250 30 00
www.hkr.se

Informationssäkerhetspolicy

Styrande dokument för informationssäkerhetsarbetet vid Högskolan Kristianstad:



Innehållsförteckning

Läsanvisningar

Informationssäkerhetspolicyn är avsedd för och gäller alla anställda på högskolan, oavsett anställningsform eller anställningsgrad. För regler och bestämmelser som gäller för studenter, se avsnittet *Anvisning – Användare: Student på HKR*.

Terminologi

Ska – tvingande krav som måste efterföljas.
Bör – ej tvingande, men stark rekommendation.

Inom informationssäkerhetspolicyn förekommer ämnen och områden som är mer eller mindre relevanta för olika befattningar. Således gäller nedan läsanvisningar, men rekommendationen är att ta del av hela informationssäkerhetspolicyn.

Allmänt om informationssäkerhet på HKR

Gäller för och är av relevans för ***samtliga anställda*** på Högskolan Kristianstad, oavsett anställningsform eller anställningsgrad.

Gäller också för och är av relevans för ***konsulter, inlånad extern personal*** *och* ***affilierade personer*** som eventuellt saknar anställning men som omfattas av högskolans ”Riktlinjer för Affiliering”.

Informationsklassning på HKR

Gäller för och är av relevans för ***samtliga anställda*** på Högskolan Kristianstad, oavsett anställningsform eller anställningsgrad.

Gäller också för och är av relevans för ***konsulter, inlånad extern personal*** *och* ***affilierade personer*** som eventuellt saknar anställning men som omfattas av högskolans ”Riktlinjer för Affiliering”.

Anvisning – Användare

Gäller för och är av relevans för ***samtliga anställda*** på Högskolan Kristianstad, oavsett anställningsform eller anställningsgrad samt för ***informationsägare***.

Gäller också för och är av relevans för ***konsulter, inlånad extern personal*** *och* ***affilierade personer*** som eventuellt saknar anställning men som omfattas av högskolans ”Riktlinjer för Affiliering”.

Med ”*Informationsägare*” avses anställd som ansvarar för en större mängd information/data i form av informationsresurser som inte klassas som ett system eller förvaltningsobjekt, exempelvis ett forskningsprojekt.

Anvisningen gör skillnad på ”student” och ”anställd”, och innehåller riktlinjer för de båda.

Konsulter, ***inlånad extern personal*** och ***affilierade personer*** omfattas av regelverken/avsnitten för ”anställd” i den grad det är tillämpligt.

Anvisning – Administratör

Gäller för och är av relevans för de som har någon form av ***systemadministrativ roll*** eller ***kontoadministration*** i sin tjänst.

Med ”systemadministrativ roll” avses arbetsuppgift där den anställde tilldelats någon form av utökad behörighet i gemensamt datasystem på HKR.

Några exempel på sådana arbetsuppgifter:

- Hantering och administration av serverplattform. (*Ex: systemadministratör*)
- Hantering och administration av användarkonton. (*Ex: kontoadministratör*)
- Hantering och administration av LADOK-resurser. (*Ex: studieadministratör*)
- Hantering och administration av digitala inventarier. (*Ex: bibliotekarie*).

Anvisningen omfattar även ***affilierade personer, konsulter*** och ***inlånad extern personal*** i de fall kontoadministration eller en systemadministrativ roll har tilldelats.

Om du är osäker på om din befattning/tjänst omfattas av en systemadministrativ roll, kan du vända dig till högskolans IT-avdelning för rådgivning.

Anvisning – Systemägare och systemansvarig

Gäller för och är av relevans för de som har någon form av roll som ***systemägare*** eller ***systemansvarig***

Med ”*Systemägare*” avses anställd som har ägandeskapet för ett förvaltningsobjekt med tillhörande informationsresurser.

Med ”*Systemansvarig*” avses anställd som ansvarar för den operativa eller tekniska driften av ett förvaltningsobjekt.

Riktlinjer för IT-system på HKR

Gäller för och är av relevans för ***systemadministratörer (IT)***, ***utvecklare (IT)*** och ***personal med tekniskt driftansvar*** på Högskolan Kristianstad.

Riktlinjerna omfattar även ***konsulter*** och ***inlånad extern personal*** i de fall tekniskt driftansvar, systemadministration, eller utvecklingsroll har tilldelats.

1 Allmänt om informationssäkerhet på HKR

1.1 Inledning

Myndigheten för samhällsskydd och beredskap (MSB) föreskriver i MSBFS 2016:1 att varje statlig myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet (5 §). Som myndighet ska högskolan upprätta en informationssäkerhetspolicy, andra styrande dokument samt den dokumentation som i övrigt krävs för att kunna bedriva ett ändamålsenligt arbete med informationssäkerhet (7 §).

Informationssäkerhetspolicyn omfattar anställda, studenter och andra samarbetspartner såsom konsulter och uppdragstagare inom högskolan.

Information är en av de viktigaste tillgångarna och utgör en förutsättning för att högskolan ska kunna bedriva sin verksamhet på ett effektivt sätt. Därför behöver information hanteras och skyddas på ett säkert sätt så att verksamheter och relationer inte skadas.

Med informationssäkerhet avses att rätt information är tillgänglig för rätt person när den behövs samt att informationen är och förblir riktig.

1.2 Målsättning och omfattning

Den övergripande målsättningen för informationssäkerhetsarbetet är att säkerställa att:

- känslig information och informationsresurser skyddas mot obehörig åtkomst (konfidentialitet),
- informationens riktighet säkras på ett sådant sätt så att informationen är fullständig och aktuell och inte är felaktig eller avsiktligt/oavsiktligt förvanskad (riktighet) och
- tillgång till information och system vid högskolan hålls på en sådan nivå att verksamhetens arbete kan bedrivas effektivt och utan störningar i enlighet med gällande verksamhetskrav (tillgänglighet).

samt att hantera risker för eventuella skador på verksamheten oavsett orsak.

Vidare ska informationssäkerhetsarbetet på högskolan säkerställa att:

- relevanta lagar och föreskrifter efterföljs
- all personal känner till var informationssäkerhetspolicyn finns tillgänglig
- all personal har fått ta del av informationssäkerhetspolicyn
- intern utbildning relevant till informationssäkerhet på HKR ska finnas tillgänglig för all personal
- krishanteringsförmåga upprätthålls
- omvärldsbevakning beaktas och arbetet anpassas till utveckling och trender
- årliga mål för arbetsområdet informationssäkerhet fastställs och följs upp.

1.3 Roller och ansvar

Rektor har det övergripande ansvaret för informationssäkerheten och verkställande av beslut gällande informationssäkerheten på högskolan.

Högskoledirektör har det övergripande ansvaret för förvaltningen av informationssystem på högskolan.

Kanslichef har det övergripande ansvaret för informationssäkerhetsarbetet och ansvarar för att styrande dokument inom informationssäkerhet revideras vid behov.

IT-chef har det övergripande ansvaret för IT-säkerheten på högskolan.

Systemägare ansvarar för ett förvaltningsobjekt med tillhörande informationsresurser. Hit räknas även ansvarar för att informationsklassning och riskanalyser genomförs för gällande system/objekt.

Systemansvarig ansvarar för den operativa eller tekniska driften av sitt förvaltningsobjekt. Till det ansvaret räknas även att upprätthålla systemets säkerhetsnivå, säkerställa korrekt hantering gällande behandling av personuppgifter samt revidering och uppdatering av tillhörande förvaltningsplan. Verkställande av teknisk drift och arbete kan tilldelas teknisk driftansvarig, utsedd av IT-chef. I de fall systemdrift är förlagd till/hos extern part, ansvarar Systemansvarig för att uppdatera objektet i systemlistan.

Driftansvarig ansvarar för verkställande av den tekniska driften och andra tekniska ingrepp i tilldelat system. Tillhörande ansvar räknas även att säkerställa att den tekniska informationen för förvaltningsobjektet i systemlistan är korrekt. Driftansvarig ska även korrigera information om ansvarsfördelning för objektet i systemlistan, på beställning av systemansvarig eller systemägare i de fall driften är förlagd internt (inom HKR).

Informationsägare ansvarar för informationsklassning, dokumentationsplan, upprätthållande av informationssäkerheten samt säkerställa korrekt personuppgiftsbehandling för sin information.

Alla anställda vid högskolan ska följa de bestämmelser som regleras i, de för tjänsten, relevanta anvisningar i informationssäkerhetspolicyn och tillhörande styrdokument.

Den som medvetet eller av grov oaktsamhet bryter mot dessa bestämmelser kan bli föremål för arbetsrättsliga åtgärder.

1.4 Revidering och uppföljning

Uppföljning är en viktig del i informationssäkerhetsarbetet för att säkerställa att:

- informationssäkerhetspolicyn efterlevs och vid behov revideras,
- omvärldsbevakning beaktas och arbetet anpassas med utvecklingen/trend,
- årliga mål för arbetsområdet informationssäkerhet är fastställda,
- årliga mål är uppföljda,
- relevanta lagar och föreskrifter efterlevs.

1.5 Kommunikation och utbildning

All personal ska regelbundet få tillgång till den information och utbildning som behövs för att informationssäkerheten ska kunna upprätthållas. Det är dock varje medarbetares ansvar att hålla sig uppdaterad om och följa informationssäkerhets-policyn.

Policyn finns tillgänglig på högskolans intranät och eventuella revideringar ska löpande informeras om på intranätet.

2 Informationsklassning

2.1 Allmänt

Syftet med att klassificera information är att bedöma och fastställa:

- hur högskolans information och informationssystem ska hanteras avseende säkerhetsaspekter,
- vilken betydelse informationen har för verksamheten, samt
- vilka konsekvenser det medför om informationen skulle hanteras felaktigt, försvinna eller komma i orätta händer.

Informationsklassningen underlättar val av relevanta tekniska och administrativa skyddsåtgärder.

2.2 Modell för informationsklassning

Information vid högskolan klassificeras utifrån aspekterna konfidentialitet, riktighet och tillgänglighet. Information ska klassas enligt dessa aspekter när användare upprättar dokument och sparar information. Resultatet av informationsklassningen styr hur användaren ska hantera informationen.

Konsekvensnivåer

I modellen används tre nivåer (informationsklasser) för värdering av konsekvenser till följd av att konfidentialitet, riktighet och tillgänglighet inte kan upprätthållas.

Nivå	Konsekvenser
Infoklass 1 – *Öppen, Låg*	Inget obehag eller begränsad skada för enskilda personer, högskolan eller tredje part
Infoklass 2 – *Medel, Betydande*	Omfattande skada för enskilda personer, högskolan eller tredje part
Infoklass 3 – *Hög, Allvarlig*	Allvarlig skada eller omfattande obehag för enskilda personer, omfattande skada för ett stort antal personer, eller allvarlig skada för högskolan eller tredje part.

Allvarlig skada
Med *allvarlig skada* avses så pass omfattande skada att förtroendet för högskolan som organisation påverkas långsiktigt, eller en betydande ekonomisk förlust.

2.3 Konfidentialitet

Informationen ska klassificeras utifrån konfidentialitet vilket innebär att den ska skyddas från obehörig insyn.

Med *skyddsvärd* information avses information som innehåller känsliga personuppgifter, personnummer, integritetskänsliga personuppgifter eller information som på annat sätt är att betrakta som skyddsvärd.

Med *kryptering* avses i sammanhanget antingen:

- att dataöverföringen krypteras mellan avsändare och mottagare eller
- att själva informationen/datan krypteras (exempelvis genom fil- eller e-postkryptering).

Informationsklass 1

- Informationen får lagras utan kryptering på lokal hårddisk, högskolans server, flyttbar lagringsmedia eller i godkänd molntjänst.
- Informationen får skickas med e-post utan kryptering.
- Informationen får sändas med vanlig post, såväl internt som externt.

Informationsklass 2

- Informationen får lagras utan kryptering på lokal hårddisk, högskolans server, flyttbar lagringsmedia eller i godkänd molntjänst.
- Informationen får överföras elektroniskt utan kryptering inom högskolans egna datorsystem. (dvs skicka e-post internt på högskolan).
- Överföring till/från externt datorsystem utanför högskolan kräver kryptering. (dvs skicka e-post externt).
- Informationen får skickas med intern post genom förseglat kuvert.
- Informationen får skickas med extern post genom normal posthantering.

Informationsklass 3

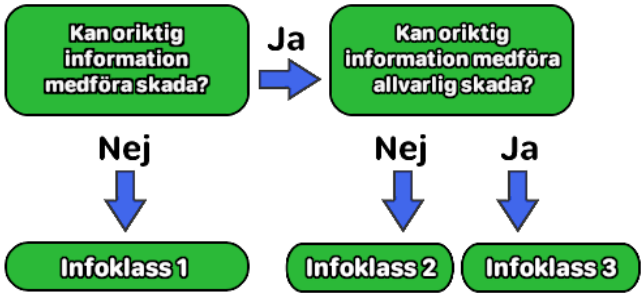
- Informationen ska lagras på lokal hårddisk på tjänstedatorn, högskolans server, på krypterad flyttbar lagringsmedia eller i för ändamålet godkända molntjänster.
- All elektronisk överföring av informationen ska vara krypterad.
- Informationen får skickas med intern post genom förseglat kuvert.
- Informationen får skickas med extern post endast genom REK brev.
- Vid byte eller kassering av lagringsmedia där information av infoklass 3 lagrats, ska högskolans IT-avdelning kontaktas för säker destruering och säkerställande av krypteringsimplementation.

Hemlig information

Med hemlig information avses uppgifter som enligt Säkerhetsskyddslag (2018:585) rör säkerhetskänslig verksamhet samt handlingar som innehåller säkerhetsskydds-klassificerade uppgifter. Om sådan information behöver hanteras av medarbetare på högskolan (exempelvis i ett forskningsprojekt) ska IT-avdelningen kontaktas för en bedömning av säkerhetsåtgärder i det enskilda ärendet.

2.4 Riktighet

Informationen ska klassificeras utifrån riktighet, vilket syftar till att säkerställa att den är korrekt och inte ändras på ett obehörigt sätt.



Informationsklass 1

- Inga krav ställs på verifiering av riktigheten i informationen.
- Inga krav ställs på skydd mot förvanskning av informationen.

Informationsklass 2

- Informationen ska vara spårbar avseende upprättandet.
- Informationens riktighet ska kunna verifieras genom signering eller logg.

Informationsklass 3

- Informationen och dess riktighet ska vara spårbar avseende upprättande, förändringar och tillägg genom signering eller logg.
- Informationen ska förses med ett högt skydd mot oavsiktlig eller avsiktlig förändring genom ett anpassat behörighetskontrollsystem.

2.5 Tillgänglighet

Informationen ska klassificeras utifrån tillgänglighet, vilket innebär att informationen finns tillgänglig vid rätt tid.

Informationsklass 1

- Inga krav ställs på tillgänglighet för tjänst/information.
- Förlust av tillgänglighet (nedtid) accepteras.
- Informationen behöver inte säkerhetskopieras.

Informationsklass 2

- Vissa krav kan ställas på tillgänglighet för tjänst/information.
- Förlust av tillgänglighet (nedtid) kan accepteras, men ska i så fall redogöra för längst acceptabla tjänstebortfall.
- Informationen ska säkerhetskopieras.

Informationsklass 3

- Direkta krav på tillgänglighet ställs för tjänsten/informationen.
- Förlust av tillgänglighet (nedtid) accepteras inte, såvida det inte sker på utsatt servicefönster.
- Informationen ska säkerhetskopieras.

Tillämpning

Kravet på tillgänglighet ska redovisas i gällande förvaltningsplan och ska uttryckas i tidstermer utifrån följande frågeställningar:

- hur länge ska informationen finnas tillgänglig? (bakåtlagring)
- hur många timmar per dygn ska informationen vara tillgänglig? (upptid)
- vad är längsta acceptabla förlust av tillgänglighet (avbrott)?
- hur och när görs säkerhetskopiering, samt vilka tidskrav som gäller för återställning vid avbrott.
- hur och när underhållsarbeten ska bedrivas, baserat på vilken nertid som accepteras.
- hur säkerställs systemets tillgänglighet genom övervakning/monitorering?

3 Anvisning – Användare

3.1 Anvisningens roll i informationssäkerhet

Informationssäkerhetsanvisning - Användare redovisar hur varje enskild användare på högskolan ska verka för att upprätthålla en god informationssäkerhet.

Anvisningen gör skillnad på ”student” och ”anställd”, och innehåller riktlinjer för de båda.

Konsulter, ***inlånad extern personal*** och ***affilierade personer*** omfattas av regelverken/avsnitten för ”anställd” i den grad det är tillämpligt.

3.2 Anställd på HKR

3.2.1 Användarens ansvar

Information är en viktig tillgång för högskolan. För att skydda informationen krävs ett riskmedvetande hos alla medarbetare. Som användare har du därför en del i ansvaret för säkerheten i informationshanteringen och du är som anställd skyldig att ta reda på vilka regler som gäller.

3.2.2 Åtkomst till information

3.2.2.1 Behörighet

Högskolan har system för behörighetskontroller för att säkerställa att endast behöriga användare kommer åt information.

De behörigheter du blir tilldelad beror på dina arbetsuppgifter och avgörs av systemansvarig och/eller närmaste chef.

Det är inte tillåtet att själv skaffa eller försöka skaffa sig högre behörighet i system som du inte är systemansvarig eller systemägare för.

3.2.2.2 Lösenord

Innan du loggar in första gången får du ett slumpgenererat lösenord för åtkomst till högskolans IT-miljö. Lösenordet ska efter tilldelning, och i samband med datorutlämning, bytas till ett personligt lösenord.

Lösenord och användaridentitet är personliga och får inte under några omständigheter lånas ut till någon annan. Det är även förbjudet att använda någon annans inloggningsuppgifter, även om denne har gett sitt medgivande.

Anteckna inte lösenord där det kan återfinnas av obehörig.
Samma lösenord får inte lov att återanvändas på externa hemsidor eller tjänster.

Lösenord ska väljas så att de är svårgissade – vid oklarhet, kontakta IT-avdelningen.

Lösenord måste uppfylla följande kriterier avseende komplexitet:

- Ej innehålla användarens namn eller användarnamn.
- Bestå av minst 8 tecken.

- Ej innehålla något av följande tecken: Å, å, Ä, ä, Ö, ö
- Innehålla tecken från tre (3) av följande fyra (4) grupper:
    - Små bokstäver (gemener): a-z
    - Stora bokstäver (versaler): A-Z
    - Siffror: 0-9
    - Specialtecken: ! @ # $ % / ( ) [ ] = ? + \ * , ; . : - _ |
- Vara unikt utifrån de tio (10) senaste lösenorden för användarkontot.

Den anställde ska omgående byta lösenordet vid misstanke om att lösenordet blivit känt av någon annan.

Det är tillåtet att använda lösenordshanterare i mobiltelefon eller dator. Dock bör sådan skyddas av ett annat unikt lösenord än de som lagras i den. Lösenord får inte antecknas och förvaras där det kan återfinnas av obehörig.

3.2.2.3 Lagring av digital information

Anställda ska i första hand lagra sina filer i "*Min Hemkatalog*" (även kallad ”H:”) på tjänstedatorn. ″Min Hemkatalog″ synkroniseras per automatik till högskolans servrar när dessa är nåbara. Synkronisering är således endast möjlig när datorn är ansluten till högskolans nätverk på campus eller via VPN.

Data som lagras på den lokala hårddisken (C:) säkerhetskopieras inte.
Arbetsmaterial ska därför alltid lagras i ”*Min Hemkatalog*” (H:) så att materialet inte riskerar att förloras.

Gemensamma filutrymmen (ex: L:, S:) gör att flera användare kan få tillgång till data och filer. Åtkomst till dessa styrs genom användarens behörigheter.
Likt hemkatalogen, säkerhetskopieras även gemensamma filutrymmen.

Filer får även lagras i molntjänster som är godkända av högskolan. I dagsläget har högskolan godkänt molnbaserad fillagring genom Sharepoint, OneDrive och Box i webbaserad variant samt via synkroniseringsklient som installeras lokalt på datorn.

Andra molntjänster för fillagring, exempelvis Dropbox och Google Drive, får endast användas om samtliga nedan kriterier uppfylls:

- Molntjänsten används för att dela filer mellan HKR och en organisation som ej har stöd för OneDrive eller Box.
- HKRs roll i samarbetet är en icke ledande- och deltagande roll.

I de fall där högskolan har en ledande roll i samarbetet, ska endast godkända molntjänster för fillagring användas, t.ex. OneDrive eller Box.

Det är inte tillåtet att lagra privat data i- eller använda högskolans molntjänster i privata syften.

Information som innehåller känsliga personuppgifter eller sekretesskyddade uppgifter enligt Offentlighets- och sekretesslagen, OSL, (2009:400) får inte lagras i Microsofts molntjänster, dvs i SharePoint och OneDrive, såvida det inte godkänts för ändamålet utifrån genomförd riskanalys. Beslut om godkännande fattas av kanslichef, efter samråd med IT-chef och högskoledirektör.

Lagring på extern lagringsmedia (tex USB-minnen, externa hårddiskar eller minneskort) kan utgöra en säkerhetsrisk om känslig eller sekretessbelagd information lagras på mediet och bör därför undvikas i så stor utsträckning som möjligt. Om känslig eller sekretessbelagd information ändå lagras på externa lagringsmedia, ska dessa vara krypterade för att förhindra obehörig åtkomst vid förlust. För hjälp med kryptering, kontakta IT-avdelningen. Den anställde ansvarar själv för säkerhetskopiering av externa lagringsmedia, samt för att eventuella krypteringsnycklar förvaras säkert.

3.2.2.4 Lagring av icke-digital information (exempelvis pappershandlingar)

Handlingar som innehåller känslig eller sekretessbelagd information ska förvaras på ett sätt som förhindrar obehörig åtkomst.

Utrymmen som är specifikt avsedda för förvaring av handlingar med känslig eller sekretesskyddad information (informationsklass 3) ska vara utrustade med:

- spårbar tillträdeskontroll och inbrottslarm
- brandskydd och brandlarm
- översvämningslarm

Mer information om fysisk säkerhet för förvaring av icke-digital information, se avsnittet: *Fysisk säkerhet – förvaring av icke-digital information*.

För lagring av icke-digital information så som pappershandlingar, gäller samma informationsklassningsmodell som för digital lagringsmedia (se avsnittet: *Informationsklassning*).

3.2.3 Din arbetsplats

3.2.3.1 Tilldelad utrustning

Utrustning som tilldelas den anställde i tjänsten, som dator och mobiltelefon, upplåtes temporärt i syfte att användas som arbetsredskap. Det är högskolan som äger utrustningen, såvida annat inte skriftligen har överenskommit. Vid tilldelning och återlämning ska en skriftlig kvittens upprättas mellan högskolan och den anställde.

Privat användning av tilldelad utrustning är tillåten så länge det inte påverkar arbetet negativt eller medför säkerhetsrisker för högskolan.

Det är inte tillåtet att använda tilldelad utrustning i annan tjänst eller affärs-verksamhet utanför högskolan.

Det är inte tillåtet att låna ut tilldelad utrustning till andra personer utanför tjänsten.

Anställda ansvarar för att tilldelad utrustning

- hanteras och förvaras så att den inte utsätts för uppenbar stöldrisk.
- hanteras varsamt
- inte utsätts för onödiga risker vid installation av programvara

- återlämnas i sådant skick att återanvändning är möjlig. Detta omfattar såväl själva hårdvaran som den information som lagras på den. T.ex. bör datorn låsas eller loggas ut ifrån när den lämnas kvar på arbetsplatsen.

Vid uppenbara övertramp ifrån dessa bestämmelser kan den anställde komma att bli ersättningsskyldig för tilldelad utrustning som kommit till skada, förlorats, stulits eller på annat sätt gjorts obrukbar.

Skador och förlust av tilldelad utrustning ska anmälas till IT-avdelningen. Den anställde ansvarar för att förlust av tilldelad utrustning polisanmäls personligen och att kopia på polisanmälan tillhandahålls IT-avdelningen.

Reparationer och andra fysiska ingrepp på tilldelad utrustning får endast utföras av IT-avdelningen.

Tilldelad utrustning som ägs av högskolan kan komma att omhändertas och undersökas vid säkerhetsincidenter eller som åtgärd för att säkerställa att gällande regelverk och lagkrav efterlevs.

Avveckling och kassering av utrustning får endast göras av IT-avdelningen.

3.2.3.2 Privat utrustning

Det är tillåtet att använda privat utrustning i tjänsten, under förutsättning att den anställde säkerställer att utrustningen inte utsätter högskolan för onödiga säkerhetsrisker eller hot. För att privat utrustning ska få användas i tjänsten krävs att operativsystem hålls uppdaterat och att enheten är utrustad med uppdaterat antivirusskydd.

Det är tillåtet att ansluta privat utrustning till högskolans trådlösa nätverk (Eduroam), däremot är det inte tillåtet att försöka ansluta privat utrustning till högskolans trådbundna nätverk.

Vid avvikelse ifrån ovan bestämmelser eller om det i övrigt anses nödvändigt ur säkerhetsaspekt, reserverar högskolan rätten att blockera och förhindra sådan utrustning åtkomst till resurser och nätverk.

3.2.3.3 Programvaror

Anställda på högskolan har behörighet att själva ladda ner och installera programvara på tilldelad utrustning. Detta sker på användarens eget ansvar, och det är upp till användaren att säkerställa att programvarans avtals- och licensvillkor följs. Användaren ansvarar även för att programvaran inte utsätter datorsystemet och den information som behandlas däri för onödiga risker.

Det är inte tillåtet att installera, lagra, göra tillgängligt eller använda piratkopierad programvara, media eller annat material på tilldelad utrustning eller i annat datorsystem på högskolan.

högskolan reserveras rätten att förhindra och blockera åtkomst till programvaror och tjänster som bedöms vara direkt olämpliga, olagliga eller på annat sätt utsätter verksamheten för allvarliga säkerhetsrisker.

3.2.4 Internet

högskolan förser personal, studenter och gäster med internetuppkoppling via SUNET. Högskolan strävar efter att bevara internetåtkomsten så öppen och fri som möjligt. För att så ska kunna ske ställs det oundvikligen vissa etiska krav på användarna av högskolans internetuppkoppling och det är därför inte tillåtet att:

- försöka få tillgång till nätverksresurser eller andra IT-resurser utan att ha rätt till det,
- försöka störa eller avbryta den avsedda användningen av nätverken eller anslutna IT-resurser,
- försöka skada eller förstöra den datorbaserade informationen,
- uppenbart slösa med tillgängliga resurser (personal, maskinvara eller programvara),
- göra intrång i andras privatliv,
- försöka förolämpa eller förnedra andra.

Till ovan bestämmelser tillkommer även de bestämmelser som regleras i svensk lag. Detta avser exempelvis 4 kap 9 c § Brottsbalken - Dataintrång och upphovsrättsbrott enligt Lag om upphovsrätt till litterära och konstnärliga verk, URL, (1960:729).

Vid användning av högskolans internetuppkoppling kan trafik- och användarloggar komma att sparas och analyseras i specifika fall.

Vid övertramp av ovan bestämmelser eller om det i övrigt anses nödvändigt ur säkerhetsaspekt, reserverar högskolan sig rätten att blockera och begränsa innehåll i internettjänsten för samtliga eller enskilda användare.

3.2.5 E-post

E-postadresser på högskolan tilldelas anställda, studenter samt anlitade konsulter och inhyrd personal. Anställdas e-postkonton aktiveras den dag anställningen börjar, och avslutas den dag anställningen upphör.

Innehavare av en e-postadress på högskolan ansvarar personligen för att e-posten hanteras i enlighet med gällande regelverk, och med insikt om att e-postadressen representerar högskolan som statlig myndighet.

Användare som innehar en e-postadress på högskolan ansvarar personligen för att bevaka och skyndsamt ta del av inkommande e-post.

För längre frånvaro vid exempelvis semester eller sjukdom, ska e-posten programmeras med automatiskt svarsmeddelande som informerar avsändaren att mottagaren inte är tillgänglig och vart de kan vända sig vid akuta ärenden.

Som statlig myndighet omfattas högskolan av offentlighetsprincipen och rätten att ta del av allmänna handlingar. E-postloggen, det vill säga rubrik, avsändare och datum på inkomna e-postmeddelanden är en offentlig allmän handling som ska lämnas ut på begäran. Innehållet i inkommande e-postmeddelanden kan vara allmän handling. Vid begäran om utlämnande kan IT-avdelningen alternativt jurist få tillgång till den anställdes inkorg för att gå igenom e-post.

Det är viktigt att kontrollera att mottagaradressen är korrekt innan e-postmeddelandet skickas för att undvika felsändning, speciellt om meddelandet innehåller känsliga personuppgifter. E-post med personuppgifter som skickas till fel mottagare kan utgöra en personuppgiftsincident som ska anmälas och utredas av högskolans dataskyddsombud.

Det är inte tillåtet att använda högskolans e-post i privata syften och e-postadressen får inte registreras hos externa tjänsteleverantörer om arbetsuppgifterna inte specifikt kräver detta.

Som anställd är det inte tillåtet att skicka e-post från externa epostleverantörer där avsändaradressen anges tillhöra domänen ”hkr.se”, utan att detta skriftligen har godkänts av IT-chef.

Det är inte tillåtet att använda högskolans e-post för att skicka sekretessbelagd information, såvida inte detta sker genom av högskolan godkända krypterings-metoder. För mer information kontakta IT-avdelningen. Det är inte heller tillåtet att skicka lösenord via e-post.

Massutskick, exempelvis utskick till alla anställda, är endast tillåtna om detta skriftligen har godkänts av både högskolans IT-chef och kommunikationschef. Massutskick som inte godkänts kommer att blockeras.

Åtkomst till funktionsadresser som omfattar ”@hkr.se” får endast tilldelas studenter som arbetar på uppdrag av högskolan genom någon form av anställning.

Förhandsprogrammerade svar på inkommen e-post (*auto-svar*), får aktiveras på obevakade funktionsbrevlådor om syftet är att styra och hänvisa kommunikationen till annat medium eller mottagare.

Vid osäkerhet eller misstanke om bedrägligt eller skadligt innehåll i e-posten, ska högskolans IT-avdelning rådfrågas innan innehållet öppnas.

Vid övertramp av ovan bestämmelser eller om det i övrigt anses nödvändigt ur säkerhetsaspekt, reserverar högskolan sig rätten att blockera och begränsa åtkomst till användares e-postkonton.

Om ett e-postmeddelande bryter mot ovanstående bestämmelser kan det anmälas till högskolans IT-avdelning genom att skicka e-post till: 3030@hkr.se.

3.2.6 Utskrifter och kopieringsmaskiner

Utskrifter på papper till skrivare kan antingen göras som direktutskrift eller genom kösystem (PullPrint).

Utskrifter som kan innehålla känsliga uppgifter ska skrivs ut genom skrivarens kösystem (PullPrint), vilket kräver inloggning och fysisk närvaro vid skrivaren innan utskrift sker.

Det är inte tillåtet att låna ut sina inloggningsuppgifter, passerkort eller tag för skrivaren till andra personer.

Det är inte tillåtet att använda högskolans skrivare och tillhörande utrustning för privata utskrifter.

3.2.7 Avslutning av anställning

Vid avslut av anställning ansvarar den anställde för att:

- rådgöra med chef om arbetsmaterial som ska sparas. Arbetsmaterial som framställts kan vara allmän handling eller del av statligt finansierad forskning och ska då bevaras hos högskolan,
- privat material (ej tjänsterelaterat) raderas,
- tilldelad utrustning återlämnas i sådant skick att återanvändning är möjlig,
- tilldelade nycklar och passerkort återlämnas,
- beställa autosvar för e-postkonto med hänvisning till kontaktinfo (frivilligt),
- följa övriga riktlinjer vid avslut av anställning.

3.3 Student på HKR

3.3.1 Användarens ansvar

Som användare av högskolans IT- och informationsresurser ska även studenter följa vissa regler och bestämmelser för hur dessa resurser ska hanteras.

3.3.2 Åtkomst till information

3.3.2.1 Behörighet

Högskolan har system för behörighetskontroller för att säkerställa att endast behöriga användare kommer åt information.

Det är inte tillåtet att själv skaffa eller försöka skaffa sig högre behörighet i system som man inte är behörig till.

3.3.2.2 Användaridentitet, e-postadress och lösenord

Studenter tilldelas en användaridentitet med tillhörande inloggningsuppgifter första gången de blir antagna till en utbildning på högskolan. Användaridentiteten består av en e-postadress och ett användarnamn som baseras på automatiskt hämtade uppgifter från Skatteverket. Användarnamn och e-postadress kan komma att ändras vid ändringar i namnuppgift hos Skatteverket.

Studenters användaridentitet och e-postkonton aktiveras den dag de blir antagna till en utbildning på högskolan. Studenters användaridentitet och e-postkonton avslutas 18 månader efter sista avslutade kursen.

Till användaridentiteten skapas ett slumpgenererat lösenord, vilket inte tilldelas studenten. Detta lösenord fungerar endast som en så kallad placeholder, tills att lösenordet ändras. Studenter tilldelas istället en länk till högskolans portal för lösenordsbyten, varpå ett personligt lösenord måste väljas.

Lösenordet har inget utgångsdatum och det finns inga krav på lösenordsbyten utöver det initiala. Högskolan rekommenderar dock att lösenordet byts vid varje ny termin.

Lösenord och användaridentitet är personliga och får inte under några omständigheter lånas ut till någon annan. Det är även förbjudit att använda någon annans inloggningsuppgifter, även om denne har gett sitt medgivande.

Anteckna inte lösenord där det kan återfinnas av obehörig.

Samma lösenord bör undvikas att återanvändas på externa hemsidor eller tjänster.

Lösenord bör väljas så att de är svårgissade och måste uppfylla högskolans lösenordskriterier avseende komplexitet:

- Ej innehålla användarens namn eller användarnamn.
- Bestå av minst 8 tecken.
- Ej innehålla något av följande tecken: Å, å, Ä, ä, Ö, ö
- Innehålla tecken från tre (3) av följande fyra (4) grupper:
    - Små bokstäver (gemener): a-z
    - Stora bokstäver (versaler): A-Z
    - Siffror: 0-9
    - Specialtecken: ! @ # $ % / ( ) [ ] = ? + \ * , ; . : - _ |
- Vara unikt utifrån de tio (10) senaste lösenorden för användarkontot.

Lösenordet ska omgående bytas vid misstanke om att lösenordet blivit känt av någon annan.

Vid avvikelse från ovan bestämmelser eller om det i övrigt anses nödvändigt ur säkerhetsaspekt, reserverar högskolan rätten att blockera och förhindra åtkomst till användarkonton och informationsresurser.

3.3.2.3 Användning av högskolans utrustning

Vid användning av högskolans datorer ska studenter i första hand lagra sina filer i "*Min Hemkatalog*" (även kallad ”H:”) på datorn. "*Min Hemkatalog*" synkroniseras per automatik till högskolans servrar när dessa är nåbara, innebärande att data säkerhetskopieras till server.

Studenter tillåts även använda och lagra data i personligt tilldelad OneDrive-yta.

Det är inte tillåtet att lagra privat data i eller använda högskolans molntjänster i privata syften. Detta omfattar även ”*Min Hemkatalog*” (även kallad ”H:”).

Data som lagras på den lokala hårddisken (C:) säkerhetskopieras inte och kan komma att raderas då högskolans datorer nollställs automatiskt.

Det är inte tillåtet att installera, lagra, använda eller göra tillgängligt piratkopierad mjukvara eller media (såsom film och musik) på utrustning eller annat datorsystem som tillhör högskolan.

Högskolan reserveras rätten att förhindra och blockera åtkomst till programvaror och tjänster som bedöms var direkt olämpliga, olagliga eller på annat sätt utsätter verksamheten för allvarliga säkerhetsrisker.

Vid avslut av studier ansvarar studenten för att:

- eventuellt tilldelad lånedator återlämnas i helt och rent skick.
- eventuellt tilldelad lånedator återlämnas i sådant skick att återanvändning är möjlig.

I vissa fall kan dock lånedatorn köpas loss av studenten efter fullföljda studier och överenskommelse med högskolan.

Lagring av insamlat material som innehåller personuppgifter ska behandlas med försiktighet. Om känsliga personuppgifter eller sekretessbelagd information lagras på externa lagringsmedia (exempelvis USB eller minneskort), ska dessa vara krypterade för att förhindra obehörig åtkomst vid förlust. För hjälp med kryptering kontakta IT-avdelningen.

3.3.2.4 Användning av privat utrustning

Det är tillåtet att ansluta privat utrustning till högskolans trådlösa nätverk (Eduroam) under förutsättning att utrustningen inte utsätter högskolan för uppenbara säkerhetsrisker/hot. Däremot är det inte tillåtet att försöka ansluta privat utrustning till högskolans trådbundna nätverk.

Vid avvikelse från ovan bestämmelse eller om det i övrigt anses nödvändigt ur säkerhetsaspekt, reserverar högskolan rätten att blockera och förhindra sådan utrustning åtkomst till informationsresurser och nätverk.

Högskolan reserveras rätten att förhindra och blockera åtkomst till programvaror och tjänster som bedöms var direkt olämpliga, olagliga eller på annat sätt utsätter verksamheten för allvarliga säkerhetsrisker.

3.3.3 Internet

Högskolan förser personal, studenter och gäster med internetuppkoppling via SUNET. Högskolan strävar efter att bevara internetåtkomsten så öppen och fri som möjligt. För att så ska kunna ske ställs det oundvikligen vissa etiska krav på användarna av högskolans internetuppkoppling och det är därför inte tillåtet att:

- försöka få tillgång till nätverksresurser eller andra IT-resurser utan att ha rätt till det,

- försöka störa eller avbryta den avsedda användningen av nätverken eller anslutna IT-resurser,
- försöka skada eller förstöra den datorbaserade informationen,
- uppenbart slösa med tillgängliga resurser (personal, maskinvara eller programvara),
- göra intrång i andras privatliv,
- försöka förolämpa eller förnedra andra.

Till ovan bestämmelser tillkommer även de bestämmelser som regleras i svensk lag. Detta avser exempelvis dataintrång och upphovsrättsbrott

Vid användning av högskolans internetuppkoppling kan trafik- och användarloggar komma att sparas och analyseras efter behov vid exempelvis felsökning.

Vid övertramp av ovan bestämmelser eller om det i övrigt anses nödvändigt ur säkerhetsaspekt, reserverar högskolan sig rätten att blockera och begränsa innehåll i internettjänsten för samtliga eller enskilda användare.

Högskolan reserveras rätten att förhindra och blockera åtkomst till tjänster som bedöms vara direkt olämpliga, olagliga eller på annat sätt utsätter verksamheten för allvarliga säkerhetsrisker.

3.3.4 E-post

Studenter ska regelbundet ta del av sin e-post då information från högskolan om utbildningen skickas till student-e-postadressen. Det är, som student, tillåtet att automatiskt vidarebefordra inkommande e-post till andra externa epostleverantörer, exempelvis till den adress som används privat.

Som statlig myndighet omfattas högskolan av offentlighetsprincipen och rätten att ta del av allmänna handlingar. Det innebär att e-post som en student skickar till en anställd på högskolan, exempelvis en lärare, anses som en inkommen handling och kan lämnas ut på begäran, om innehållet inte är sekretesskyddat.

Åtkomst till funktionsadresser som omfattar ”@hkr.se” får endas tilldelas studenter som arbetar på uppdrag av högskolan genom någon form av anställning.

Som student är det inte tillåtet att skicka e-post från externa epostleverantörer där avsändaradressen anges tillhöra domänen ”hkr.se” eller ”stud.hkr.se”, utan att detta skriftligen har godkänts av IT-chef.

Studenter bör undvika att registrera sin student-e-postadress hos externa tjänste-leverantörer.

Kedjebrev och andra massutskick är endast tillåtna om detta skriftligen har godkänts av både högskolans IT-chef och kommunikationschef. Massutskick som inte godkänts kommer att blockeras.

Om ett e-postmeddelande bryter mot ovan bestämmelser kan detta anmälas till högskolans IT-avdelning genom att skicka e-post till: 3030@hkr.se.

Vid osäkerhet eller misstanke om bedrägligt- eller skadligt innehåll i e-posten, ska högskolans IT-avdelning rådfrågas innan innehållet öppnas.

Vid övertramp av ovan bestämmelser eller om det i övrigt anses nödvändigt ur säkerhetsaspekt, reserverar högskolan sig rätten att blockera och begränsa åtkomst till studenters e-postkonton.

3.3.5 Utskrifter och kopieringsmaskiner

Studenter tilldelas en gratis startsumma i form av utskriftskrediter. När dessa är förbrukade måste studenten själv köpa ytterligare utskriftskrediter av högskolan för att kunna använda utskriftsresurserna.

Utskrifter och papper kan innehålla känsliga uppgifter och bör behandlas därefter. Utskrifter kan göras genom kösystem (PullPrint) och i vissa fall som direktutskrift.

Då känsliga uppgifter skrivs ut ska detta göras genom skrivarens kösystem (PullPrint), vilket kräver inloggning och fysisk närvaro vid skrivaren innan utskrift sker.

Det är inte tillåtet att låna ut sina inloggningsuppgifter eller tillkopplat passerkort eller tag för skrivaren till andra personer.

4 Anvisning – Administratörer

4.1 Anvisningens roll i informationssäkerhet

Informationssäkerhetsanvisning - Administratörer redovisar hur systemadministratörer, administratörer för användarkonton, och övrig personal som administrerar datorsystem på högskolan ska verka för att upprätthålla en god informationssäkerhet.

Med system- och kontoadministratör avses personer som innehar utökad behörighet utöver den vanliga användarbehörigheten i högskolans datorsystem och övriga IT-baserade tjänster.

För administratörer som arbetar med eller ansvarar för datorsystem och digitala tjänster, se avsnittet: *Systemadministratör*

För administratörer som arbetar med- eller ansvarar för administration av gäst- och användarkonton, se avsnittet *Kontoadministratör.*

4.2 Systemadministratör

4.2.1 Ansvarsfördelning

Systemadministratörer kan tilldelas ”Tekniskt” (*Driftansvarig*) och ”Operativt” (*Systemansvarig*) driftansvar.

Information om systemadministratörer med tekniskt och operativt driftansvar för respektive system på högskolan finns beskrivet i högskolans systemlista (systemlista.hkr.se).

Systemägaren för gällande system ansvarar för att tilldela ansvar och säkerställa att utvalda systemadministratörer är medvetna om deras ansvarsfördelning och ansvarstilldelning.

4.2.2 Behörighetstilldelning

Behörighet och åtkomst till IT-system på högskolan tilldelas efter system-administratörens roll, arbetsuppgifter och kompetens.

Behörighetsbegäran eller annan förändring i behörighet ska komma ifrån eller godkännas av någon av följande:

- Systemägare
- Avdelningschef
- Systemansvarig

Hierarkisk ordning gäller med tillåten ansvarstilldelning nedåt. Exempelvis, för att ”Avdelningschef” ska tillåtas godkänna administratörsrättigheter, krävs att detta godkänts eller tillförordnats av ovanordnade (Systemägare) för gällande system.

4.2.3 Behörighet och särskilda rättigheter

4.2.3.1 Administratörskonton

Av tillverkaren inbyggda administratörskonton (exempelvis ”admin” eller ”root”) eller andra icke-personliga administratörskonton får endast användas om uppgiften specifikt kräver det.

I alla andra fall ska personliga administratörskonton tilldelas och användas.

Inte under några omständigheter är det tillåtet att aktivera, använda eller aktivt möjliggöra användning av standardiserade administratörskonton med av tillverkaren angivna standardlösenord.

I de fall möjligheten finns, ska Multi-faktorsautentisering användas för administratörskonton vid autentisering.

4.2.3.2 Administration – allmän hantering

Systemadministratörer har behörighet och rättigheter som möjliggör övervakning av system och data som flödar genom dessa. Syftet med detta är bland annat att hantera och säkerställa systemets driftsäkerhet. Med ”system” och ”data” omfattas även IT-infrastruktur och nätverkstrafik.

Systemadministratörer ska sträva efter att värna om användarnas personliga integritet så långt detta är möjligt för att lösa arbetsuppgifterna.

Systemadministratörer ska vid uträttande av arbetsuppgifterna undvika och minimera risken att enskilda användares data granskas, så långt detta är möjligt.

I de fall data behöver behandlas som omfattar känsliga personuppgifter ska sådana data anonymiseras om möjligt.

4.2.3.3 Administration – e-postsystem

Systemadministratörer med behörighet till högskolans e-postsystem har rätt att hantera och rensa i andra användares e-postlådor. Detta bör dock endast göras om det föreligger särskilda skäl till det ur säkerhetsaspekt eller om användaren uttryckligen bett om hjälp samt om det förekommit missbruk, felanvändning, eller otillåten användning av tjänsten. Hantering kan även ske vid utlämnande av allmän handling i e-postlådan. Ingrepp i tjänsten som omfattar rensning av enskilda användares eller avdelningars data, bör föregås av kontakt och information till berörda parter.

4.2.3.4 Administration – lagringsutrymmen

Systemadministratörer med behörighet till högskolans lagringsutrymmen har rätt att hantera och rensa i användares lagringsutrymmen på server. Detta bör dock endast göras om det föreligger särskilda skäl till det ur säkerhetsaspekt eller om användaren uttryckligen bett om hjälp samt om det förekommit missbruk, felanvändning, eller otillåten användning av tjänsten. Ingrepp i tjänsten som omfattar rensning av enskilda användares eller avdelningars data, bör föregås av kontakt med och information till berörda parter.

4.2.3.5 Administration – inskränkning av tjänst

Systemadministratörer har rätt att utan förvarning – och om det i övrigt anses nödvändigt ur säkerhets- eller driftaspekt – blockera, begränsa och förhindra åtkomst till högskolans IT-resurser och infrastruktur. I den mån det är möjligt ska

systemadministratören sträva efter att koordinera ingreppet i förväg med berörda parter och systemansvarig.

4.2.3.6 Administration – säkerhetsgranskning

Systemadministratörer med drift- eller systemansvar för gällande system, har rätt att utvärdera och testa säkerheten i det berörda IT-systemet. Om systemadministratören avser att testa och utvärdera säkerheten i annat system än det som denne ansvarar för, ska detta i förväg meddelas system- eller driftansvarig för gällande system.

4.2.4 Särskilda skyldigheter

Utöver särskilda rättigheter åläggs även systemadministratörer med vissa särskilda skyldigheter, som alltid ska efterföljas om inte annat uttryckligen anges.

4.2.4.1 Tystnadsplikt

Då systemadministratörer ofta har särskild insyn i system och information som kan innehålla känsliga och integritetskränkande uppgifter, ska tystnadsplikt vidtas.

Tystnadsplikten innebär att uppgifter och information inte får upprepas eller vidarebefordras till annan än behörig individ, och då endast om så krävs för arbetsuppgiften.

4.2.4.2 Rapporteringsplikt

Systemadministratörer är skyldiga att rapportera misstänkta säkerhetsincidenter rörande informations- och IT-säkerhet på högskolan. Detta omfattar hela högskolans IT-miljö och är inte begränsat till det egna systemansvaret. Vid misstanke om avvikelser gällande konfidentialitet, riktighet och tillgänglighet ska detta omgående rapporteras till systemansvarig för gällande system, alternativt till systemägaren.

Vid säkerhetsincidenter och upptäckt av säkerhetsbrister som påverkar hela eller stora delar av högskolans verksamhet eller IT-miljö, ska IT-chef alltid informeras.

Vid personuppgiftsincidenter eller misstanke om personuppgiftsincident, ska detta alltid rapporteras till högskolans dataskyddsombud. Berörd systemägare bör även underrättas.

4.3 Kontoadministratör

4.3.1 Ansvarsfördelning

Kontoadministratörer grupperas i två kategorier.

4.3.1.1 Kontoadministratör – Typ 1

Kontoadministratörer med rättighet att skapa, ändra och radera användarkonton tillhörande:

- Studenter antagna till eller registrerade på utbildning vid högskolan.
- Hel- och deltidsanställd personal på högskolan.
- Externt anlitad personal (exempelvis konsulter) på högskolan.
- Tillfälliga gäster och besökare.

Kontoadministratör Typ 1 har behörighet att hantera användarkonton tillhörande följande domäner:

- @hkr.se
- @stud.hkr.se
- @ext.hkr.se

Kontoadministratörer av Typ 1 är administratörer som typiskt sett är anställda på högskolans IT-avdelning som Systemadministratörer och besitter behörighet till så väl Active-Directory (AD), MIM/FIM, samt tjänster för tillfälliga användarkonton (Tillf-ID)

4.3.1.2 Kontoadministratör – Typ 2

Kontoadministratörer med rättighet att skapa, ändra och radera användarkonton tillhörande:

- Externt anlitad personal (exempelvis konsulter) på högskolan.
- Tillfälliga gäster och besökare.

Kontoadministratör Typ 2 har behörighet att hantera användarkonton tillhörande följande domäner:

- @ext.hkr.se

Kontoadministratörer av Typ 2 är administratörer som typiskt sett är anställda på någon annan avdelning än IT på högskolan. Dessa administratörer har tilldelats behörighet för att kunna skapa, ändra och radera användarkonton genom tjänsten Tillf-ID, som behandlar extern personal och tillfälliga gäster & besökare.

4.3.2 Behörighetstilldelning

Behörighet och åtkomst till IT-system på högskolan tilldelas efter konto-administratörens roll, arbetsuppgifter och kompetens.

Behörighetsbegäran eller annan förändring i behörighet ska komma ifrån- eller godkännas av någon av följande:

Kontoadministratör - Typ 1 och Typ 2

- IT-chef
- Systemägare
- Avdelningschef

Hierarkisk ordning gäller med tillåten ansvarstilldelning nedåt. Exempelvis, för att ”Avdelningschef” ska tillåtas godkänna administratörsrättigheter, krävs att detta godkänts eller tillförordnats av ovanordnade (Systemägare och IT-chef) för gällande system.

4.3.3 Behörighets- och särskilda rättigheter

4.3.3.1 Administratörskonton

Av tillverkaren inbyggda administratörskonton (exempelvis ”admin” eller ”root”) eller andra icke-personliga administratörskonton får endast användas om uppgiften specifikt kräver det.

I alla andra fall ska personliga administratörskonton tilldelas och användas.

Inte under några omständigheter är det tillåtet att aktivera, använda eller aktivt möjliggöra användning av standardiserade administratörskonton med av tillverkaren angivna standardlösenord.

I de fall möjligheten finns, ska Multi-faktorsautentisering användas för administratörskonton vid autentisering.

4.3.3.2 Kontoadministration – Allmän hantering

Kontoadministratörer har behörighet och rättigheter som möjliggör insyn i system och information som kan anses som integritetskänslig. Således ska kontoadministratörer värna om användarnas personliga integritet så långt detta är möjligt för att lösa arbetsuppgifterna.

Kontoadministratörer ska vid uträttande av arbetsuppgifterna undvika och minimera risken för att enskilda användares data granskas, så långt detta är möjligt genom att t.ex. dölja data som inte är relevant att ta del av.

Kontoadministratörer ansvarar för att utfärdade användarkonton och behörigheter tas bort och avslutas när dessa inte längre behövs eller efter avslutat uppdrag.

Kontoadministratörer av Typ 1 och Typ 2 som utfärdar användarkonto till extern personal eller tillfällig gäst, ansvarar för att:

- upplysa om högskolans informationssäkerhetspolicy och regelverk.
- säkerställa personens identitet innan utfärdande av användarkonto***.
- säkerställa att personen tilldelas utfärdade kontouppgifter.

*** = Omfattar inte konton för tjänsten ”HKR-Guest” (*Öppet gäst-WiFi*).

4.3.3.3 Kontoadministration – Inskränkning av tjänst

Kontoadministratörer har rätt att utan förvarning, och om det i övrigt anses nödvändigt ur säkerhets- eller driftaspekt, blockera, begränsa och förhindra åtkomst till användarkonton tillhörande högskolan.

4.3.4 Särskilda skyldigheter

Utöver särskilda rättigheter åläggs även kontoadministratörer med vissa särskilda skyldigheter, som alltid ska efterföljas om inte annat uttryckligen anges.

4.3.4.1 Tystnadsplikt

Då kontoadministratörer ofta har särskild insyn i system innehållande personuppgifter och annan integritetskänslig information, ska tystnadsplikt vidtas.

Tystnadsplikten innebär att uppgifter och information inte får upprepas eller vidarebefordras till annan än behörig individ, och då endast om så krävs för arbetsuppgiften.

4.3.4.2 Rapporteringsplikt

Kontoadministratörer är skyldiga att rapportera misstänkta säkerhetsincidenter rörande användarkonton till högskolans IT-avdelning.

Vid personuppgiftsincidenter eller misstanke om personuppgiftsincident, ska detta alltid rapporteras till högskolans dataskyddsombud.

4.4 Systemägare och systemansvarig

Anvisningen redogör för hur personal med systemförvaltningsansvar i någon grad på högskolan ska verka för att upprätthålla en god informationssäkerhet.

4.4.1 Definition och roll

Till varje system och förvaltningsobjekt ska det finnas en utsedd systemägare. Systemägare utses av högskoledirektören.

Systemägare är den som ur ett ansvars- och budgetperspektiv tilldelats ägande- eller förfogandeansvar för ett eller flera system.

Systemägare ansvarar även för systemets tillhörande informationsresurser. Hit räknas även ansvar för att informationsklassning och riskanalyser genomförs för gällande system/objekt.

Systemägaren ansvarar för systemets budgetering, avtal (inkl. personuppgifts-biträdesavtal) och bemanning.

Systemägaren ansvarar för att tilldela ansvar för och säkerställa att utvalda systemansvariga är medvetna om deras ansvarstilldelning och eventuell fördelning.

Systemägaren ansvarar för att fatta beslut om respektive förvaltningsobjekts nyutveckling, vidareutveckling och avveckling.

Systemägare ansvarar för att anmäla förändringar i ansvarsfördelningen (avseende systemägare) till förvaltningsobjektets driftsansvarige. Den driftsansvarige ansvarar sedan för att uppdatera informationen i högskolans systemlista.

Information om systemägare för respektive system på högskolan återfinns i högskolans systemlista (systemlista.hkr.se).

4.4.2 Nyanskaffning av IT-system

Inför nyanskaffning och införande av nytt IT-system ansvarar systemägaren för att en införandeplan upprättas.

Införandeplanen ska inledas med en informationsklassning av den information och data som kan komma att hanteras i systemet.

Införandeplanen ska även inkludera en riskanalys som baseras utifrån resultatet av informationsklassningen. Riskanalysen ska sedan ligga till grund för att utröna de säkerhets- och integrationskrav som det nya systemet kommer att ställa.

I införandeplanen ska det även beskriva om personuppgifter kommer att behandlas och vilken typ av personuppgifter det gäller. En ny eller ändrad personuppgiftsbehandling ska anmälas till högskolans dataskyddsombud så att behandlingen förs in i högskolans registerförteckning över personuppgiftsbehandlingar.

Om behandlingen av personuppgifter kan leda till en hög risk för fysiska personers rättigheter och friheter, som t.ex. när en större mängd känsliga personuppgifter hanteras, ska en konsekvensbedömning genomföras innan behandlingen påbörjas. Konsekvensbedömningen görs i samråd med högskolans dataskyddsombud.

Systemägaren ansvarar för att införandeplanen upprättas. Verkställande av denna uppgift kan dock tilldelas tilltänkt systemansvarig, men det är systemägaren som ansvarar för att det genomförs.

Systemägaren ska sedan förbereda och överlämna det tekniska och operativa ansvaret till tilldelad systemansvarige. Den systemansvarige ansvarar för utvecklings- och integrationsarbetet, men det är systemägaren som beslutar när övergång ska ske ifrån ’utveckling’ till ’test’, till produktionssättning.

4.4.3 Avveckling av informationssystem

Inför avveckling av informationssystem ska systemägaren fatta beslut om avveckling. Vid avveckling av informationssystem ansvarar systemägaren för att säkerställa att så kan ske utan konflikt med verksamhetens behov eller eventuella avtal med extern leverantör.

Om personuppgifter har behandlats i informationssystemet ska personuppgiftsbehandlingen avanmälan till dataskyddsombudet så att behandlingen tas bort från registerförteckning över personuppgiftsbehandling.

Systemägaren bör upprätta och tillämpa en avvecklingsplan enligt föreslagen process:

1 Säkerställ att avveckling kan ske utan förhinder.
2 Besluta om avveckling av systemet.
3 Planera avveckling (praktiskt genomförande)
4 Planera avveckling (tidsåtgång)
5 Signalera / informera om avveckling.
6 Stänga / avsluta tjänster och allmän tillgång till systemet.
7 Inventera informationen och arkivera vid behov.

8 Avsluta eventuella avtal.
9 Avveckla och kassera eventuell utrustning/hårdvara.

4.5 Systemansvarig

Ansvarsfördelning – definition och roll

Till varje system och förvaltningsobjekt ska det finnas en utsedd systemansvarig.

Systemansvarig ska utses av systemägaren eller högskoledirektören. Systemägare eller högskoledirektör bör även utse en biträdande systemansvarig.

Den som utses till systemansvarig eller biträdande systemansvarig, bör vara en person i verksamheten med god insyn- och vana i att arbeta i systemet.

Systemansvarig ansvarar för den operativa eller tekniska driften av sitt informationssystem eller förvaltningsobjekt. Tillhörande ansvar är även att upprätthålla systemets säkerhetsnivå, samt revidering och uppdatering av tillhörande förvaltningsplan. Verkställande av teknisk drift och arbete kan tilldelas teknisk driftansvarig, utsedd av IT-chef.

Systemansvarig ansvarar för att följa utvecklingen av systemet och samordna arbetet för detta samt införa beslutade förändringar på uppdrag av systemägare.

Systemansvarig ansvarar i en beslutsfattande roll, för att hantera- och tilldela behörigheter för systemet samt säkerställa att de som tilldelas behörighet innehar eller förses med relevant utbildning för systemet. Verkställandet av behörighets-tilldelning kan förordnas exempelvis till teknisk driftansvarig.

Systemansvarig ansvarar för att anmäla förändringar i ansvarsfördelningen (avseende systemansvarig) till förvaltningsobjektets driftsansvarige. Den driftsansvarige ansvarar sedan för att uppdatera informationen i högskolans systemlista.

Information om systemansvarig för respektive system på högskolan återfinns i högskolans systemlista (systemlista.hkr.se).

Systemansvarig ansvarar för att ta fram eventuellt budgetunderlag för förvaltningsobjektet som denne ansvarar över. Det är alltså systemägaren som beslutar för- och ansvarar för budget, medan systemansvarig ansvarar för verkställandet.

Systemansvarig ansvarar för att en informationsklassning görs för systemet och att denna inkluderas i gällande förvaltningsplan. Den systemansvarige ansvarar även för att koordinera och implementera de säkerhetskrav som ställs på systemet ur teknisk aspekt ihop med driftansvarig, utifrån informationsklassningen.

Systemansvarig ansvarar för att eventuella personuppgifterna i systemet behandlas på ett korrekt sätt. Vid behov ska samråd ske med högskolans dataskyddsombud. Systemansvarig ska säkerställa att den registrerade kan tillvarata sina rättigheter

gällande behandling av sina personuppgifter i systemet. Systemansvarig ska se till att registrerade får information om personuppgiftbehandlingen, att begäran om registerutdrag hanteras, att rättelse, komplettering och i förekommande fall, borttag av personuppgifter kan ske samt att uppgifter gallras eller bevaras enligt gällande föreskrifter. Systemansvarig ska även rapportera och hantera personuppgifts-incidenter i systemet i samråd med högskolans dataskyddsombud.

För mer information om högskolans systemförvaltning och hantering av förvaltningsobjekt, se Högskolan Kristianstads *Systemförvaltningsmodell* som återfinns i intranätet under avsnittet *Systemförvaltning*.

5 Riktlinjer för IT-system på HKR

5.1 Syfte och roll

5.1.1 Allmänt

Riktlinjerna i detta avsnitt beskriver och redovisar de generella krav och bestämmelser som finns för högskolans IT-system, relaterat till drift, utveckling och förvaltning. Riktlinjerna är utformade för att initialt kunna appliceras på samtliga IT-system.

5.1.2 Avsteg

Avsteg ifrån riktlinjerna och tillhörande bestämmelser kan förekomma i de fall det anses befogat ur ett säkerhets- och verksamhetsperspektiv. Avsteg ifrån dessa riktlinjer ska vara godkända av IT-chef.

5.2 Grundläggande säkerhet – tjänstedator

Följande riktlinjer ska gälla för samtliga tjänstedatorer som tilldelas personal på högskolan, om inte annat uttryckligen har beslutats enligt ovan rutin avseende avsteg ifrån riktlinjer.

Vid tilldelning och återlämning av tjänstedatorer ska en kvittens upprättas skriftligen eller digitalt mellan högskolan och den anställde. Den anställde ska erbjudas kopia på kvittensen såväl vid tilldelning som vid återlämning.

Vid tilldelning ska tjänstedatorn omfattas av giltig tillverkargaranti. Tjänstedatorer bör ersättas innan eller så fort tillverkargarantin utgår.

Samtliga tjänstedatorer ska vara stöldmärkta.

Samtliga tjänstedatorer ska vara medlemmar i och inventerade i högskolans Active Directory (AD) trädstruktur.

Samtliga tjänstedatorer och eventuellt tillhörande nätverksadaptrar ska vara registrerade i högskolans AAA-system för nätverksautentisering (t.ex. 802.1x), om så inte automatiskt sker genom AD-medlemskap.

Samtliga tjänstedatorer ska vara inventerade i högskolans inventarier för tilldelad utrustning (CMDB). Här ska även framgå vem som tilldelats och förfogar över tjänstedatorn.

Samtliga Windowsbaserade tjänstedatorer ska utrustas med SCCM-klient (eller motsvarande), som regelbundet återrapporterar status och möjliggör för fjärradministration.

Samtliga tjänstedatorer ska utrustas och konfigureras med klient för att säkert kunna fjärransluta till högskolans VPN-tjänst.

Samtliga tjänstedatorer ska löpande hållas uppdaterade avseende operativsystem och tillhörande säkerhetspatchar.

Samtliga tjänstedatorer ska vara utrustade med mjukvara för antivirus, och ska hållas uppdaterad avseende virusdefinitioner och signaturer. Om annan antivirusmjukvara används (ihop med eller istället för) den som förses av högskolan, ska detta uttryckligen godkännas av IT-chef.

Samtliga tjänstedatorer ska begränsas avseende administratörsrättigheter genom funktionen LAPS. Dock ska möjlighet finnas att tillfälligt erhålla administratörs-behörighet för exempelvis installation av mjukvara genom LAPS.

Samtliga tjänstedatorer ska omfattas av krav på lösenord vid inloggning och återupptagning efter vilo- eller strömsparläge. Tjänstedatorn ska i sitt standard-utförande, låsas automatiskt vid inaktivitet efter maximalt 30 minuter.

Tjänstedatorn ska automatiskt synkronisera- och säkerhetskopiera filer och data ifrån användarens hemkatalog (H:), till högskolans filserver (DFS-share), förutsatt att datorn har kontakt med högskolans server, genom uppkoppling via HKR:s trådbundna- och trådlösa nätverk, samt VPN.

Hemkatalog (H:) behöver inte göras tillgänglig om denna ersätts med personligt ansluten ”OneDrive för Företag” som levereras av högskolan, under förutsättning att motsvarande säkerhetskopiering ingår i tjänsten.

5.3 Grundläggande säkerhet – tjänstetelefon

Följande riktlinjer ska gälla för samtliga tjänstetelefoner som tilldelas personal på högskolan, om inte annat uttryckligen har beslutats enligt ovan rutin avseende avsteg ifrån riktlinjer.

Vid tilldelning och återlämning av tjänstetelefon ska en kvittens upprättas skriftligen eller digitalt mellan högskolan och den anställde. Den anställde ska erbjudas kopia på kvittensen såväl vid tilldelning som vid återlämning.

Vid tilldelning ska tjänstetelefonen omfattas av giltig tillverkargaranti. Tjänstetelefonen bör ersättas innan eller så fort tillverkargarantin utgår.

Samtliga tjänstetelefoner ska vara medlemmar i och inventerade i högskolans MDM-system (SnowDM eller Microsoft Intune).

Samtliga tjänstetelefoner ska vara inventerade i högskolans inventariesystem för mobiltelefoner och abonnemang (TFN). Här ska även framgå vem som tilldelats- och förfogar över tjänstetelefonen.

Samtliga tjänstetelefoner ska vara inventerade i högskolans inventarier för tilldelad utrustning (CMDB). Här ska även framgå vem som tilldelats och förfogar över tjänstetelefonen.

Samtliga Android-baserade tjänstetelefoner ska utrustas med MDM-klient (Snow eller Microsoft Företagsportal), som regelbundet återrapporterar status och möjliggör för fjärradministration.

Nya iOS-baserade tjänstetelefoner som tilldelas anställda fr.o.m. 2021-01-01 ska vara utrustade med MDM-klient (Microsoft Företagsportal), som regelbundet återrapporterar status och möjliggör för fjärradministration.

Senast 2021-12-31 ska samtliga iOS-baserade tjänstetelefoner vara utrustade med MDM-klient (Microsoft Företagsportal), som regelbundet återrapporterar status och möjliggör för fjärradministration.

Samtliga tjänstetelefoner ska utrustas och konfigureras med WLAN-profil för att säkert kunna ansluta till högskolans trådlösa nätverk Eduroam.

Samtliga tjänstetelefoner ska löpande hållas uppdaterade avseende mjukvara som förses av högskolan.

Samtliga tjänstetelefoner ska vid utlämningstillfället vara uppdaterade med de senaste säkerhets- och operativsystemuppdateringarna för enheten.

Samtliga tjänstetelefoner ska omfattas av krav på minst 4-siffrig PIN-kod vid uppstart och upplåsning. Tjänstetelefonen ska i sitt standardutförande, låsas automatiskt vid inaktivitet efter 2 minuter. Upplåsning genom biometriska metoder (t.ex. fingeravtryck) är tillåtet som ett komplement till kraven för skärmlås.

Om en tjänstetelefon tappas bort ska det anmälas till IT-avdelningen.

5.4 Grundläggande säkerhet – server och infrastruktur

Följande riktlinjer ska gälla för samtliga serversystem som används på högskolan, om inte annat uttryckligen har beslutats enligt ovan rutin avseende avsteg ifrån riktlinjer.

Programvara, säkerhetspatchar och operativsystem ska löpande hållas uppdaterade med de uppdateringar som tillverkaren tillhandahåller för gällande plattform/OS. Uppdateringar ska installeras snarast möjligt eller vid nästkommande servicefönster, beroende på hur akut implementeringskravet är.

Upptäckta sårbarheter ska åtgärdas skyndsamt och i de fall säkerhetsfixar eller motåtgärder inte är tillgängliga, ska beslut fattas av IT-chef i samråd med teknisk driftansvarig huruvida risken kan accepteras eller om systemet ska göras otillgängligt i väntan på åtgärd.

Driftstatus för produktionsisatta serversystem med tillhörande resurser ska övervakas genom högskolans tjänst för systemmonitorering (OP5), för att möjliggöra snabb upptäckt och åtgärd vid driftsbortfall.

Produktionsisatta serversystem med tillhörande resurser ska säkerhetskopieras så att återställning systemet kan ske efter haveri och driftsbortfall. Hur ofta säkerhetskopiering ska göras regleras i respektive systems förvaltningsplan, men för virtuella serversystem (VM) rekommenderas en daglig systemspegling (Snapshot).

Standardiserade administratörskonton (exempelvis admin och root) eller andra icke-personliga administratörskonton får endast användas om uppgiften specifikt kräver det. I alla andra fall ska personliga administratörskonton tilldelas och användas.

Inte under några omständigheter är det tillåtet att aktivera, använda eller aktivt möjliggöra användning av standardiserade administratörskonton med av tillverkaren angivna standardlösenord.

I de fall möjlighet finns, ska Multi-Faktorsautentisering användas för administratörskonton vid autentisering.

Lösenord som lagras i eventuella konfigurationsfiler ska i högsta möjliga mån lagras i krypterad eller hashad form, på ett icke reversibelt sätt. Det ska alltså inte vara möjligt att matematiskt räkna ut lösenordet, enbart baserat på den obfuskerade datan.

Överföringar av lösenord vid autentisering ska ske krypterat och tillåts inte att skickas i klartext- eller över okrypterade anslutningar.

Administratörsinloggningar i system och tjänster tillåts kopplas direkt mot Active-Directory (AD) och LDAP i de fall systemet inte besitter inbyggt stöd för autentisering mot ADFS.

Administratörs- och användarbehörigheter ska gå att styra baserat på grupp-tillhörighet i Active-Directory (AD).

Användarinloggning i webbaserade system och webbtjänster ska kopplas till- och ske över ADFS. Undantag ges system som driftsatts i produktionsmiljö innan 2019. Undantagna system ska vara anpassade och använda ADFS-autentisering senast april 2020.

Säkerhetskopior, loggar och konfigurationsfiler ska lagras krypterat om så är möjligt- och kan ske utan förhinder för systemets dagliga drift.

System som utvecklas på/av högskolan som produktionsätts i verksamheten, ska inte ställa krav på insticksmoduler och plugin ifrån tredje part i webbläsare (exempelvis Java och Flash).

System som utvecklas på/av högskolan som produktionsätts i verksamheten och som använder autentisering/inloggning, ska använda säkra anslutningar via HTTPS, krypterade med TLS 1.2.

System som utvecklas på/av högskolan som produktionsätts i verksamheten och som använder HTTPS, ska använda ett giltigt SSL-certifikat som utfärdats genom HKR:s CA (DigiCert).

Systemnamn ska anges enligt HKR:s namngivningsstandard för system i formatet: **HK**XXXNN.
X ska vara beskrivande i möjligast mån, genom förkortning eller akronym.
X ska bestå av versaler: A-Z.
N ska bestå av siffror och fungera som löpnummer med start på 01.
Exempel: HKAPP02, HKSQL01, osv

Domänadresser (URL) för webbaserade system och tjänster ska anges enligt KHR:s namngivningsstandard för webtjänster i formatet: *tjänst.hkr.se*, där tjänst ska vara beskrivande för systemet och utgöras av alfanumeriska tecken (a-z, 0-1).
Exempel: 3030.hkr.se, studentportal.hkr.se, osv.

Nätverksanslutna system och resurser som kräver speciella säkerhetsundantag, som till exempel analysinstrument med mycket gammalt OS, ska skyddas med dedikerad nätverksbrandvägg med ändamålsenlig konfiguration.

6 Fysisk säkerhet

6.1 Systemdriftsmiljö

Serversystem med tillhörande resurser ska verka och huseras i en ändamålsenlig driftsmiljö. Sådan driftsmiljö ska vara anpassad till systemets krav avseende tillämpning och övervakning av:

- tillträdeskontroll och inbrottslarm
- brandskydd och brandlarm
- temperatur- och luftfuktighetsreglering
- översvämningslarm
- oavbruten elförsörjning (UPS)

6.1.1 Tillträdeskontroll och inbrottslarm

Tillträde till utrymmen där serversystem och lagringsresurser förekommer ska omfattas av elektroniskt passagesystem, krävandes personligt passerkort (eller motsvarande) och personlig PIN-kod. Passagesystemet ska även möjliggöra spårbarhet på vilka personer som passerar, med tillhörande tidsstämpel.

Tillträde till slutna utrymmen där nätverksinfrastruktur (exempelvis ethernet-switch) förekommer, ska omfattas av godkänd låsenhet med krav på personlig nyckel för passage. I de fall möjlighet finns bör dessa utrymmen utrustas med elektroniskt passagesystem, som kräver personligt passerkort (eller motsvarande) och personlig PIN-kod. För utrustning som placeras utanför slutna utrymmen (t.ex. i datorsal), ska denna monteras i ett ändamålsenligt fastmonterat och låsbart kabinett/skåp.

Behörighet till dessa utrymmen ska endast tilldelas till personal vars arbetsuppgifter kräver tillträde till lokalerna.

Samtliga utrymmen där serversystem, lagringsresurser och nätverksinfrastruktur förekommer, ska vara utrustade med centrallarm. Med ”centrallarm” avses larmsystem med direktkoppling till det företag/tjänst som ansvarar för utryckning vid larm. Ljudlösa inbrottslarm är tillåtna såvida de uppfyller samma krav som- eller kan anses likgiltiga övriga larmsystem.

6.1.2 Brandskydd och brandlarm

Driftsmiljöer och slutna utrymmen för serversystem, nätverksinfrastruktur och lagringsresurser ska vara utrustade med centralt kopplat brandlarm/rökdetektor. Med ”centralt” avses brandlarm med direktkoppling till räddningstjänsten som svarar för utryckning vid larm. Brandlarm bör även vara utrustade med detektorer som triggas vid mycket snabb värmeökning.

Driftsmiljöer i form av serverhall eller datacenter ska vara utrustade med ändamålsenlig släckutrustning, bestående åtminstone av typgodkänd och besiktigad koldioxidbrandsläckare.

Korskopplingsrum och slutna utrymmen för nätverksinfrastruktur bör vara utrustade med ändamålsenlig släckutrustning, bestående åtminstone av typgodkänd- och besiktigad koldioxidbrandsläckare. I de fall släckutrustning inte förekommer i eller inom utrymmet, ska släckutrustning finnas nära tillhanda på ett avstånd om maximalt 50 meter (fågelväg).

Pulverbrandsläckare bör undvikas och endast användas som sista släckningsalternativ, då pulvret orsakar stor skada i elektronisk utrustning.

6.1.3 Temperatur- och luftfuktighetsreglering

Driftsmiljöer i form av serverhall eller datacenter ska vara utrustade med ändamålsenlig temperatur- och luftfuktighetsreglering (HVAC). Utrymmena ska kunna övervakas avseende temperatur och luftfuktighet i realtid, och ska vara inställda att larma/informera driftspersonal vid avvikelser om ej optimala klimatförändringar.

Korskopplingsrum och slutna utrymmen för nätverksinfrastruktur där mycket utrustning huseras i till ytan små utrymmen, bör vara utrustade med system för åtminstone temperaturreglering eller kylning.

Hyresvärden äger och ansvarar för drift och underhåll av samtliga HVAC-system.

Kontaktuppgifter till ansvarig för HVAC-system, samt eventuellt journummer, ska finnas tillgängligt för IT-avdelningen.

6.1.4 Översvämningslarm

Driftsmiljöer i form av serverhall eller datacenter ska vara utrustade med översvämningslarm. Översvämningslarm utgörs förslagsvis av en nätverksansluten sensor/probe som placeras i ett hörn på golvet för att triggas vid kontakt med vattensamlingar. Översvämningslarm ska kunna övervakas i realtid, och ska vara inställda att larma/informera driftspersonal vid problem.

Korskopplingsrum och slutna utrymmen för nätverksinfrastruktur bör vara utrustade med översvämningslarm. I de fall översvämningslarm inte används, bör utrustningen monteras högt i racket/ställningen.

6.1.5 Oavbruten elförsörjning (UPS)

Driftsmiljöer, datacenter och slutna utrymmen för serversystem, nätverks-infrastruktur och lagringsresurser ska vara utrustade med oavbruten elförsörjning (UPS).

I de fall samtliga strömvägar inte kan tillföras UPS-kraft, ska system och utrustning inom det fysiska utrymmet prioriteras efter klassificering och krav på tillgänglighet (se avsnittet *Informationsklassning*).

UPS-system ska regelbundet besiktigas enligt de rekommendationer som ges av tillverkaren. Vid besiktningsanmärkningar ska fel åtgärdas snarast möjligt om de

annars kan medföra negativa konsekvenser för driftskapaciteten vid strömbortfall (exempelvis byte av batteripaket).

UPS-system ska kunna övervakas i realtid, och ska vara inställda att larma/informera driftspersonal vid problem.

Utrymmen som huserar UPS-system ska vara utrustade med temperatur- och luftfuktighetsreglering (HVAC), samt översvämningslarm.

6.2 Förvaring av icke-digital information

Handlingar som innehåller känslig eller sekretessbelagd information ska förvaras i en ändamålsenlig miljö som förhindrar obehörig åtkomst, exempelvis säkerhetsskåp med lås.

Utrymmen som är avsedda att specifikt användas för förvaring av känsliga pappershandlingar ska vara utrustade med:

- spårbar tillträdeskontroll och inbrottslarm
- brandskydd och brandlarm
- översvämningslarm

6.2.1 Tillträdeskontroll och inbrottslarm

Tillträde till utrymmen avsedda för förvaring av känsliga eller sekretessbelagda handlingar ska omfattas av elektroniskt passagesystem, som kräver personligt passerkort (eller motsvarande) och personlig PIN-kod. Passagesystemet ska även möjliggöra spårbarhet på vilka personer som passerar, med tillhörande tidsstämpel.

Behörighet till dessa utrymmen ska endast tilldelas till personal vars arbetsuppgifter kräver tillträde till lokalerna.

Samtliga utrymmen där känsliga eller sekretessbelagda handlingar förekommer, ska vara utrustade med centrallarm. Med ”centrallarm” avses larmsystem med direktkoppling till det företag/tjänst som ansvarar för utryckning vid larm. Ljudlösa inbrottslarm är tillåtna såvida de uppfyller samma krav som eller kan anses likgiltiga övriga larmsystem.

6.2.2 Brandskydd och brandlarm

Samtliga utrymmen där känsliga eller sekretessbelagda handlingar förekommer, ska vara utrustade med centralt kopplat brandlarm/rökdetektor. Med ”centralt” avses brandlarm med direktkoppling till räddningstjänsten som svarar för utryckning vid larm. Brandlarm bör även vara utrustade med detektorer som triggas vid mycket snabb värmeökning.

Utrymmena bör vara utrustade med ändamålsenlig släckutrustning, bestående åtminstone av typgodkänd och besiktigad pulverbrandsläckare, undantaget pappersarkiv. Pappersarkiv ska istället utrustas med typgodkänd och besiktigad skumbrandsläckare.

I de fall släckutrustning inte förekommer i eller inom utrymmet, ska släckutrustning finnas nära tillhanda på ett avstånd om maximalt 25 meter (gångavstånd).

6.2.3 Översvämningslarm

Samtliga utrymmen där känsliga eller sekretessbelagda handlingar förvaras bör vara utrustade med översvämningslarm. Översvämningslarm utgörs förslagsvis av en nätverksansluten sensor/probe som placeras i ett hörn på golvet för att triggas vid kontakt med vattensamlingar. Översvämningslarm ska kunna övervakas i realtid, och ska vara inställda att larma/informera fastighetspersonal vid problem.

I de fall översvämningslarm inte används, bör materialet förvaras och placeras så högt upp som möjligt.

Ordlista

2-faktorsautentisering (2FA)	Autentisering / inloggning som kräver ytterligare en autentiseringsmetod i kombination med lösenordet, exempelvis engångskod eller smartkort.
3030	Högskolan Kristianstads service- och helpdesk.
3030@hkr.se	E-postadress till 3030 där supportärenden skapas automatiskt när man e-postar.
802.1X	Teknikstandard för säker nätverksautentisering av betrodda enheter.
@hkr.se	E-postdomän som används av anställda på Högskolan Kristianstad.
@stud.hkr.se	E-postdomän som används av studenter på Högskolan Kristianstad.
@ext.hkr.se	E-postdomän som används av extern personal (exempelvis konsulter) på Högskolan Kristianstad.
AAA-system	Authentication, Authorization, Accounting. System för identitetshantering som även styr behörighet, tillgänglighet, osv.
ADFS	Active Directory Federation Services. Tjänst/system som möjliggör SSO-inloggning (Single-Sign-On), så att användaren endast behöver logga in en gång på ett ställe för att få tillgång till flera skyddade tjänster.
Active Directory (AD)	Microsofts katalogtjänst för IT-miljöer, innehållandes information om en organisations IT-tillgångar, användare, användargrupper, osv.

Admin & root	Standardiserade administratörskonton som ofta finns förkonfigurerade i system av tillverkaren.
CA - Certificate Authority	Företag eller organisation som är en godkänd, registrerad och betrodd utfärdare av digitala certifikat.
CMDB	Configuration Management Database. Inventariedatabas för IT-relaterade enheter och tjänster.
DFS	Distributed File System. Microsofttjänst för distribuerad fillagring. (t.ex. “Gemensam”, “L:”)
Datacenter	Synonymt med serverhall. Stor samling av ofta sammankopplade IT-resurser i form av server, lagring och nätverksinfrastruktur.
Dataintrång	Att olagligt och olovligt bereda sig tillgång till, ändra, störa eller radera information och uppgift som man saknar behörighet för.
Dataskyddsförordningen (GDPR)	Förordning som gäller i hela EU och som innehåller bestämmelser om skydd för fysiska personer avseende behandling personuppgifter
Dataskyddsombud	Utsedd person i en organisation som ansvarar för att bland annat kontrollera att dataskyddsförordningen efterföljs och fungerar som kontaktperson i frågor rörande personuppgifter.
DigiCert	DigiCert är ett företag som är en godkänd, registrerad och betrodd utfärdare av digitala certifikat. Används av HKR för utfärdande av digitala certifikat.
FRP	Factory-Reset Protection. Säkerhetsfunktion i Android OS och Googles Play-tjänster som förhindrar återanvändning av enheten om denne nollställts på ett icke-auktoriserat sätt.

Flyttbar lagringsmedia	Exempelvis USB-minnen och externa hårddiskar.
Förvaltningsobjekt	IT-system som är driftsatt i produktion och förvaltas genom en bestämd förvaltningsplan, med tydligen roll och ansvarsfördelning.
Förvaltningsplan	Dokument innehållande beskrivning och regelverk för hur det gällande systemet och dess innehåll ska hanteras, samt tydliggör roller och ansvarsfördelning för systemet.
Google-tjänster	Samling applikationer och tjänster i Android OS som kopplas till en identitet eller användarkonto hos Google, för att exempelvis kunna avvända Play-Butiken och ladda ner appar.
HTTPS	Hyper Text Transport Protocol / Secure. Protokoll för krypterad transport av data mellan enheter. Exempelvis mellan dator och websida.
HVAC	Heating, Ventialtion, Air Conditioning. System för temeperatur- och luftfuktighetsreglering.
Icke-reversibel	Omöjligt att repetera en process i bakvänd ordning för att återskapa ursprungsförhållandet/originaldata.
Insticksmoduler (ex: Java & Flash)	Kompletterande mjukvara som krävs för att kunna nyttja vissa interaktiva funktioner på t.ex. en webbplats.
Intranät	I sammanhanget en informationsresurs och samarbetsyta avsedd för internkommunikation på högskolan (Sharepoint)
Kedjebrev	E-postmeddelande vars syfte är att uppnå omfattande spridning, med uppmaning om att skicka vidare.

Klartext	I sammanhanget, information som ej obfuskerats eller krypterats som vid lagring eller överföring enkelt kan utläsas.
Korskopplingsrum	Utrymme där nätverksinfrastruktur för det lokala närområdet sammankopplas med distributionspunkten av nätverksresurserna.
Kryptering	Att göra information oläsbar för obehöriga vid lagring eller överföring, och endast läsbar för de som förfogar över krypteringsnyckeln för informationen.
Krypteringsimplementation	Vilken metod eller tillvägagångssätt som kryptering har införts genom.
Krypteringsnycklar	Nycklar (data/fil) som används för att kryptera- eller dekryptera information.
Känsliga personuppgifter	Känsliga personuppgifter är uppgifter om etniskt ursprung, politiska åsikter religiös eller filosofisk övertygelse medlemskap i en fackförening, hälsa en persons sexualliv eller sexuella läggning samt genetiska uppgifter, biometriska uppgifter som entydigt identifierar en person.
L: och S:	Distribuerade lagringsytor på högskolans DFS-server/tjänst.
LAPS	Local Administrator Password Solution. System för att begränsa användar- och administratörsrättigheter på en dator, men samtidigt möjliggöra för tillfälligt utökad behörighet vid behov.
LDAP	Lightweight Directory Access Protocoll. Äldre protokoll som används för att hämta information ur katalogserver, t.ex. AD.

Lösenordshanterare	Program för att spara, hantera och skydda lösenord. Skyddas ofta av ett huvudlösenord, så att användaren endast behöver memorera ett lösenord men samtidigt har tillgång till alla sparade lösenord.
MDM-system	Mobile Device Management. System för att hantera- och fjärradministrera mobila enheter, exempelvis smartphones.
MIM/FIM	Microsoft/Forefront Identity Manager. System för centraliserad och automatisk hantering av användarkonton och behörigheter.
Min Hemkatalog	Ofta kallad ”H:”. Anställds- eller students personliga lagringsutrymme på HKR:s fillagringstjänst (DFS).
Molntjänster	Plattform/tjänst som tillgängliggörs över internet där information som högskolan ansvarar för lagras eller behandlas av en extern part.
Mottagarbevis	Tjänst ifrån postdistributören som möjliggör bevis/spårbarhet på att avsedd mottagare har tagit emot brevet.
Mottagarkontroll	Metod för att säkerställa att mottagaren faktiskt är den avsedda mottagaren och den de påstår sig vara.
Nätverksbrandvägg	System för att filtrera och begränsa vad för typ av data som tillåts passera mellan de förgrenande kopplingarna.
Oklassificerad information	Information utan något skyddsvärde eller reellt behov av säkerhet.
OP5	System för resurs- och prestandaövervakning av IT-system och tjänster.
Ordboksattacker	Automatiserad- och ofta distribuerad attack där man försöker gissa sig fram till rätt lösenord mot en lista av vanligt

	förekommande ord och teckentillägg. T.ex. ”Sommar2016”
OS	Förkortning för Operativsystem. T.ex. Microsoft Windows, Apple MacOS eller Linux.
Personuppgiftsincident	Säkerhetsincident där personuppgifter olovligen eller otillåtet oaktsamt hanterats, gjorts tillgängliga-, ändrats- eller raderats.
Piratkopierad	T.ex. mjukvara eller media som olovligen har kopierats och ofta distribuerats utan upphovsrättsinnehavarens tillstånd.
Placeholder	Utfyllnadsdata utan riktig funktion, mer än att uppta plats i väntan på att bli ersatt av reella och relevanta data.
Produktionssättning	Att officiellt lansera, drifta och supportera ett system eller tjänst i verksamheten.
PullPrint	Kösystem för utskrifter som möjliggör hämtning av utskrifter från valfri skrivare efter inloggning.
REK-brev	Rekommenderat brev. Typ av brev där försändelsen enbart lämnas ut mot en mottagarkvittens och legitimationskontroll.
RFID-kort	Radio Frequency Identification. Personligt smartkort med trådlös RFID-teknik. T.ex. passerkort.
Rack	Hyllplansbaserad monteringslösning (ofta i skåp) för teknikutrustning så som servrar och nätverkshårdvara.
Riskanalys	Metodiskt analysarbete för att identifiera och kvantifiera risker och konsekvenser, ofta ur ett säkerhetsperspektiv.

SCCM	System Center Configuration Manager. System ifrån Microsoft för att administrera klientdatorer.
SCCM-klient	Programvara körandes på klientdatorer i syfte att ansluta datorn till det centraliserade administrationssystemet (SCCM).
SSL-certifikat	Secure Socket Layer. Digitalt och kryptografiskt validerat(unikt) certifikat. Ofta för att verifiera en webbplats påstådda riktighet.
SUNET	Swedish University Computer Network. Organisation som tillhandahåller datanät och tjänster på nationell nivå för bl.a. institutioner inom högre utbildning.
Servicefönster	Tilldelad och ofta återkommande tidsperiod där underhållsarbeten kan utföras och förlust av tillgänglighet tillfälligt accepteras.
Snapshot	En ögonblicksbild/spegling av en virtuell server, som möjliggör för mycket snabb återställning av systemet till det stadie som det befann sig i vid tidpunkten för speglingen.
Snow	Mobil-app/klient som möjliggör fjärradministration av bl.a. smartphones via SnowDM.
SnowDM	Snow Device Manager. System/server ifrån Snow Software för att fjärradministrera anslutna smartphones.
Standardlösenord	Lösenord som satts av tillverkaren som en placeholder i väntan på att ändras av användaren/adminstratören.
Switch	Nätverksutrustning som sammankopplar enheter och resurser till resten av nätverket.
Systemlista (systemlista.hkr.se)	högskolans lista över samtliga system och tjänster som omfattas av

	förvaltningsmodellen, samt tillhörande metadata och information om ansvarsfördelning.
Säker destruering	Att på ett säkert sätt förstöra- eller göra data och media permanent och icke-reversibelt oläsbar/obrukbar.
TFN	System för att hantera och inventera tjänstetelefoner och tillhörande abonnemang.
TLS	Transport Layer Security. Kommunikationsprotokoll för säkert utbyte av krypterad information mellan datorsystem.
Tillf-ID	System för att administrera användarkonton och identiteter för extern personal (t.ex. konsulter) vid högskolan.
UPS	Uninterruptable Power Supply. System bestående av flertalet seriekopplade batterier, avsedd att användas som reservkraft vid strömbortfall.
URL	Uniform Resource Locator. Internetadress/sökväg till en resurs, tjänst eller webbplats. T.ex. ”www.hkr.se”
Upphovsrättsbrott	Att olovligen och olagligt inneha, kopiera eller material och media utan upphovsrättsinnehavarens tillstånd.
Utskriftskrediter	Krediter som studenter köper och används som valuta vid utskrifter.
VM	Virtual Machine. Virtualiserat system, oftast server.
VPN	Virtual Private Network. Krypterad- och tunnlad förbindelse mellan anslutande klientdator/enhet och högskolans nätverk. Möjliggör för säker tillgång av interna resurser på distans.

WLAN	Wireless Local Area Network. Även kallat för Wi-Fi eller trådlöst nätverk.
WLAN-profil	Personliga eller gemensamma inställningar för ett specifikt trådlöst nätverk (WLAN).