BESLUT

2022-06-29 Diarienummer 22/420

Peder Hofmann
Informationssäkerhetsansvarig
Elisabeth Smedberg
IT-chef

Riktlinjer för informationssäkerhet inkl. IT- och cybersäkerhet vid KMH

1. Bakgrund

Detta beslut ersätter tidigare riktlinjer, beslut 11/456 samt 11/274 avseende ”*Föreskrifter för IT-området*”.

1.2 Normgivande regelverk

Som grund för högskolans riktlinje gällande informationssäkerhet finns ett antal lagar och förordningar:

- *Säkerhetsskyddslagen (2018:585)*
- *Säkerhetsskyddsförordningen (2018:658)*
- *Myndigheten för samhällsskydd och beredskaps föreskrifter (2020:6-8) om statliga myndigheters informationssäkerhet, säkerhetsåtgärder samt rapportering av IT-incidenter.*
- *Riksarkivets författningssamling, kap 6 (RA-FS 2009:1)*
- *Krisberedskapsförordningen (2015:1052)*
- *Högskoleförordningen (2003:100)*
- *Förvaltningslagen (2017:900)*
- *Offentlighets- och sekretesslagen (2009:400)*
- *Förordning (2022:524) om statliga myndigheters beredskap*

2. Inledning

Med informationssäkerhet avses att högskolans verksamhet i alla dess delar har etablerat ett systematiskt arbete i syfte att skydda information i alla dess former. Det gäller oavsett hur information lagras, bearbetas och kommuniceras.

Information kan till exempel vara i form av text, ljud, bilder och film, och kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal.

I begreppet informationssäkerhet avses förutom ovanstående även IT-säkerhet, och cybersäkerhet. IT-säkerhet omfattar det tekniska skydd som behöver finnas för att skydda information i IT-systemens mjukvara och hårdvara, i datakommunikation i och mellan IT-system/-tjänster som finns i IT-plattformen.

Även fysiskt skydd av informationstillgångar såsom skydd av lokaler där det finns IT-utrustning som innehåller information utgör en del av informationssäkerheten.

Fysisk säkerhet som helhet återfinns i KMH:s ”Riktlinjer för fysisk säkerhet och person-/personalsäkerhet”.

Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån tre aspekter:

- Konfidentialitet: att information inte tillgängliggörs eller avslöjas till obehörig.
- Riktighet: att information är korrekt, aktuell och fullständig.
- Tillgänglighet: att information är åtkomlig och användbar av behörig.

Informationssäkerheten ska vara en integrerad del av arbetsuppgifter som utförs i verksamheten, i alla KMH:s verksamhetsprocesser, såväl i kärn- som i stödproccesser. Alla som hanterar information på KMH har därmed ett ansvar för att upprätthålla informationssäkerheten.

En central och viktig grundförutsättning för upprätthållande av informationssäkerhet på högskolan är att skapa en medvetenhet hos personal och studenter kring vikten av att behandla information på ett tillförlitligt sätt.

En annan viktig förutsättning för att kunna utveckla och förbättra informationssäkerheten är att årligen följa upp arbetet. IT-incidenter ska rapporteras, analyseras och åtgärder planeras för att minska risken för att liknande incidenter uppstår igen.

Uppföljning av genomförda hot- och riskanalyser ska göras utifrån förändrat omvärldsläge och nya hot- och risker som kan ha uppstått. Den årliga uppföljningen ska resultera i åtgärdsplaner i syfte att anpassa och förbättra informationssäkerheten.

För att uppnå en informationssäkerhet som ständigt är aktuell samt anpassas utifrån förekomna IT-incidenter och tillkomna hot och risker ska högskolan arbeta metodiskt med denna riktlinje som utgångspunkt.

2.1 Mål

KMH:s övergripande mål är att KMH ska ha en informationssäkerhet inkl. IT- och cybersäkerhet vilken uppfyller gällande lagar och förordningar genom att löpande utföra ett systematiskt och riskbaserat informationssäkerhetsarbete.

Med systematiskt och riskbaserat informationssäkerhetsarbete ska följande:

- att KMH:s ledning är förtrogen med informationssäkerhetsfrågor och insatt i högskolans systematiska informationssäkerhetsarbete
- att all personal och alla studenter har relevant kunskap om informationssäkerhet
- att informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för medarbetare, studenter, samverkande partners och tredje man
- att det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation
- att fortlöpande analysera hotbilden för varje enskilt informationssystem som är av vikt för verksamheten
- att förebygga negativa konsekvenser i informationssystemen
- att upprätthålla krishanteringsförmågan och ha utarbetade kontinuitetsplaner för fortsatt bedrivande av verksamheten även vid oförutsedda händelser och vid avbrott i IT-system eller IT-miljö.

Chefer på alla nivåer ska aktivt verka för en positiv attityd till säkerhetsarbetet. Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för organisationens informationstillgångar.

2.2 Roller och ansvar

Grundprincipen är att ansvaret för informationssäkerhet ska följa det ordinarie verksamhetsansvaret. Detta gäller från ledning ner till enskilda medarbetare.

Särskilda roller och ansvar vid KMH är som följer:

Rektor är också myndighetschef och har därmed det yttersta ansvaret för informationssäkerheten inklusive att säkerställa att KMH har en uppdaterad kontinuitetsplan.

Högskoledirektör har övergripande ansvar för säkerheten för samtliga informationstillgångar och utser ansvariga för respektive informationstillgång samt systemägare för respektive informationssystem.

Akademicheferna har ansvar för att säkerställa att studenter har tillräckliga kunskaper och är medvetna om aktuella rutiner för informationssäkerhet inkl. IT- och cybersäkerhet så att de kan följer gällande riktlinjer.

Avdelningschefer och *akademichefer* har i sina chefsroller ansvar för att säkerställa att medarbetare har tillräckliga kunskaper om riktlinjer och rutiner för informationssäkerhet inkl. IT- och cybersäkerhet vid utförande av sina arbetsuppgifter.

Informationssäkerhetssansvarig utses av högskoledirektören och har samordningsansvar för det systematiska informationssäkerhetsarbetet.

IT-chef har övergripande ansvar för IT-säkerheten på högskolan avseende IT-infrastruktur och teknisk plattform samt ansvar för att upprätta en kontinuitetsplan för dessa områden.

Driftsansvarig på IT-avdelningen ansvarar för att bevaka att en säker drift finns i KMH:s IT-plattform med ingående IT-system/-tjänster.

Driftsansvarig har även i ansvar att innan driftsättning av nya IT-system/-tjänster bedöma om driftsättning kan godkännas. Bedömningen görs med hänsyn tagen till att driftsäkerheten i KMH:s IT-plattform inte kommer att påverkas negativt eller utgör en säkerhetsrisk för denna och övriga informationssystem i plattformen. Driftsansvarig kan om IT-säkerheten vid en driftsättning inte kommer att kunna garanteras, neka driftsgodkännande med information om vilka nödvändiga säkerhetsåtgärder som först måste vara uppfyllda innan driftsgodkännande kan ske.

IT-säkerhetsansvarig ansvarar för att KMH:s IT-infrastruktur, IT-plattform (inklusive ingående IT-system/-tjänster), nätverk och datakommunikation i IT-plattform och mellan IT-system uppfyller *tekniska* krav på IT-säkerhet.

IT-säkerhetsansvarig ansvarar även för att anmäla och behandla inkomna IT-incidentrapporter från driftsansvarig respektive systemägare samt i aktuella fall vidareförmedla dessa vidare till MSB inom fastställd tidsperiod. I ansvaret ingår även att årligen sammanställa och analysera de IT-incidenter som förekommit i IT-plattform, infrastruktur, drift och kommunikation och föreslå övergripande förbättringar för IT-säkerhet inom området.

Dataskyddsombud har ansvar för följa upp att KMH efterlever dataskyddsförordningen (GDPR) samt har rapporteringsskyldighet till integritetsmyndigheten (IMY) gällande IT-incidenter som rör personuppgifter.

Systemägare ansvarar för ett eller flera informationssystem och har det övergripande ansvaret för sina IT-system/-tjänster såsom juridiskt och ekonomiskt samt för att säkerställa att informationssäkerhet inkl. IT- och cybersäkerhet upprätthålls för IT-system/tjänst oavsett vem som operativt utför

uppgifterna. I ansvaret ingår upprättande av kontinuitetsplaner för aktuella IT-system/-tjänster.

Systemägaren har också ansvar för att genomföra systematiskt informationssäkerhetsarbete enligt gällande riktlinjer för upprätthållande av informationssäkerheten samt att säkerställa att korrekta personuppgiftsbehandlingar utförs av sin information. Detta ansvar kan (av högskoledirektören) delegeras till en informationsägare i förekommande fall, se nedan.

Systemägaren har även rapporteringsansvar till IT-chef respektive dataskyddsombud rörande IT-incidenter.

Systemägaren kan i förekommande fall delegera det operativa ansvaret till en systemförvaltare, men kan inte delegera vidare det övergripande ansvaret för IT-systemet avseende informationssäkerhet, juridiska och ekonomiska ansvaret.

Systemförvaltare utses av systemägaren när så behövs. Systemförvaltaren har i ansvar att efter delegation från systemägaren förvalta IT-systemet i enlighet med överenskomna ramar. Se även ovan under Systemägare.

Informationsägare har ansvar för att ett givet informationsområde innehåller rätt information och har det säkerhetsskydd som motsvarar informationssäkerhetsnivån oavsett var denna information återfinns inom olika informationssystem. Informationsägare kan utses av högskoledirektören vid behov men ligger annars på den chef som ansvarar för aktuell information. Se ovan under *chef* respektive *systemägare*.

Driftsleverantör (kan i förekommande fall även vara en extern part) ansvarar för verkställande av angivna säkerhetskrav i den tekniska driften i enlighet med avtal/överenskommelse med systemägaren.

Systemleverantör (kan i förekommande fall även vara en extern part) ansvarar för verkställande av angivna tekniska säkerhetskrav vid utveckling, support och underhåll i avtal för mjukvaran i aktuellt IT-system/-tjänst.

Medarbetare på KMH ansvarar för att i sitt arbete ha kunskaper om och följa framtagna riktlinjer och rutiner för informationssäkerhet inkl. IT- och cybersäkerhet.

Studenter har ansvar att följa regler för användning av KMH:s IT-resurser samt dessa riktlinjer avseende informationssäkerhet under genomförandet av studier vid KMH. Studenter har även ett ansvar för att säkerställa att vid behandling av personuppgifter följa angivna rutiner i enlighet med dataskyddsförordningen

(GDPR) t.ex. i självständiga arbeten/examensarbeten/konserter eller motsvarande.

Följande uppställning ger exempel på vem som räknas som system- eller informationsägare i olika fall, om inget annat beslutats.

Kategori	Ägare (om ej annat anges)
Fastställda dokument	Den som fastställt dokumentet
Data i informationssystem	Systemägaren eller processägare
All annan information	Utfärdaren

3 Metod för systematiskt informationssäkerhetsarbete

3.1 Övergripande beskrivning av informationssäkerhetsarbetet

För att leva upp till gällande lagar och förordningar samt för att uppnå KMH:s mål för informationssäkerhet inkl. IT- och cybersäkerhet ska ett metodiskt arbetssätt användas.

Som ett led i denna systematik ska nedanstående steg genomföras i KMH:s systematiska informationssäkerhetsarbete:

1. Identifiering av informationstillgångar
2. Riskanalys och informationsklassificering
3. Beslut om skyddsåtgärder och åtgärdsplan
4. Uppföljning av det systematiska informationssäkerhetsarbetet

3.2 Beskrivning av tillvägagångssätt

3.2.1 Identifiering av informationstillgångar

Samtliga informationstillgångar som hanteras på KMH ska vara identifierade och förtecknade i KMH:s *dokumenthanteringsplan*.

Dokumenthanteringsplanen ägs av Arkivet på avdelningen för ledningsstöd och ekonomi. Den ger en översikt över KMH:s samtliga informationstillgångar och är i första hand utformad för att tillgodose arkivkrav. KMH har valt att använda denna även som underlag för att informationsklassa informationstillgångarna. Dokumenthanteringsplanen ska löpande uppdateras när nya informationstillgångar tillkommer.

I dokumenthanteringsplanen är respektive informationstillgång förtecknad med uppgift om vilken arbetsprocess de hör till, vilken typ av handling som avses,

vilka gallringsregler som gäller och var informationen förvaras fysiskt eller digitalt.

Dokumenthanteringsplanen återfinns på KMH:s intranät.

3.2.2 Riskanalys och informationsklassning av informationstillgångar

IT-chef, systemägare och informationsägare är ansvariga för att genomföra riskanalys och informationsklassning av sin information.

Med dokumenthanteringsplanen som utgångspunkt ska först en riskanalys genomföras av respektive informationstillgång för kriterierna riktighet, konfidentialitet och tillgänglighet. Arbetet fokuserar på vilka konsekvenser det medför för KMH:s verksamhet om dessa kriterier inte uppfylls.

Utifrån resultatet från riskanalyserna bedöms vilken *nivå av informationsklassning* som aktuell för informationstillgången har och därmed vilket *säkerhetsskydd* som informationen behöver omgärdas av.

Informationsklassningen ska säkerställa att informationen erhåller en lämplig skyddsnivå. Som hjälp används kriterierna konfidentialitet, riktighet och tillgänglighet (samt för spårbarhet)

Med konfidentialitet avses att informationen inte får göras tillgänglig eller avslöjas för obehöriga.

Med riktighet avses att informationen inte ska kunna förändras och förvanskas, tas bort av misstag eller av någon obehörig.

Med tillgänglighet avses att informationen ska finnas till hands för behöriga användare då den behövs.

Utöver ovanstående kriterier finns spårbarhet vilket kan relatera till alla ovanstående kriterier. Med spårbarhet avses att skapande, borttag och förändringar av information ska kunna härledas till den som gjort det, vad som ändrats och när.

Resultatet från de tre huvudklassificeringarna ska utgöra det samlade kravet på nivån för skyddet av den aktuella informationen eller IT-systemet.

Riskanalys för *en* informationstillgång genomförs separat för respektive kriterium vilka bedöms var för sig. Varje kriterium ska resultera i en bestämd värdeskala för hur verksamhetskritisk eller känslig informationen är. Bedömningen görs utifrån vilka konsekvenser det får för verksamheten om konfidentialiteten, riktigheten inte kan upprätthållas eller att data inte är tillgänglig (av olika skäl och under kort/lång tid).

En sammanvägd bedömning görs därefter utifrån samtliga kriteriers analysvärde så att *ett enda värde* definieras på nivå av informationsklassning för informationstillgången.

Nivån på informationsklassificeringen anges med en skala från 1-4, där informationsklass 1 är lägsta klassificeringsnivå och 4 högsta vilket innebär informationsklass vilka får konsekvenser för rikets säkerhet.

I riskanalysen ska även den fysiska säkerheten i förhållande till informationssäkerhet beaktas. Med fysisk säkerhet menas här hur informationen sprids och ska skyddas från fysiska hot såsom inbrott, sabotage eller annat som kan riskera informationssäkerheten.

Risker rörande den fysiska säkerheten bedöms utifrån hur KMH:s skalskydd ser ut, var informationen förvaras fysiskt eller digitalt. I många fall kan informationen förekomma på flera digitala lagringsplatser och/eller på fysiska platser (t.ex. både på dator, backupsystem, i arkiv, i pärmar, i kopior hos olika medarbetare, i skrivarens minne, etc.). En säkerhetsåtgärd kan därför beroende på informationsklassningsnivå innebära rutinmässiga begränsningar i hur informationen får spridas, förvaras och om den får lämna KMH:s lokaler eller inte.

Behandling av information som innehåller personuppgifter ska anmälas till KMH:s dataskyddsombud som ger anvisningar om hur informationen får hanteras.

Vid bedömning av om en handling utgör en allmän handling eller ej hänvisas till avdelningen för ledningsstöd och ekonomi.

Kontinuitetsplaner

Riskanalyser ska även genomföras för respektive IT-system/-tjänster för att upprätta kontinuitetsplaner. Syftet med en kontinuitetsplan är att vara förberedd innan ett riskscenario inträffar med stöd av en åtgärdslista som beskriver hur verksamheten ska kunna fortgå trots t.ex. elavbrott, ett IT-system ligger nere, vid en hackerattack etc.

Riskanalysen görs genom att diskutera olika möjliga riskscenarier som dokumenteras i en kontinuitetsplan vilken beskriver vilka åtgärder som behöver företas i det fall respektive scenario skulle inträffa så att verksamheten fortsatt kan *bedrivas på en acceptabel nivå*.

3.2.3 Beslut om skyddsåtgärder och åtgärdsplan

Efter genomförd riskanalys fattas beslut om vilka skyddsåtgärder som behöver vidtas, vilka skyddsåtgärder som redan finns och om ytterligare skyddsåtgärder behöver upprättas beroende på vilken informationsklassning informationen har.

Beroende på vilken informationsklassning informationen har finns ett antal givna minsta nivåer för hur informationen bör hanteras digitalt.

Om den angivna informationstillgången har ett lägre säkerhetsskydd idag mot vad som krävs för informationsnivån behöver åtgärder företas för att öka säkerhetsskyddet. Denna åtgärd ska föras upp på en särskild åtgärdsplan.

KMH:s virtuella säkerhetsorganisation har som uppgift att analysera och bedöma vilka skyddsåtgärder som kan anses vara nödvändiga att genomföra.

Informationssäkerhetsansvarig och IT-säkerhetsansvarig sammanställer årlig lägesbeskrivning av KMH:s informationssäkerhet inkl. IT- och cybersäkerhet och en samlad rekommendation av åtgärdsplan över skyddsåtgärder för att förbättra KMH:s informationssäkerhet inkl. IT- och cybersäkerhet för informationstillgångar.

Högskoledirektören fattar beslut om skyddsåtgärder och när de ska genomföras.

3.2.4 Revidering och uppföljning

Uppföljning är en viktig del i informationssäkerhetsarbetet.
Informationssäkerhetsansvarig har i uppgift att bevaka att:

- beslutade säkerhetsåtgärder är genomförda
- årliga mål är uppfyllda
- regler och riktlinjer följs
- riktlinjer och vägledande material för användare med säkerhetsinstruktioner revideras vid behov
- årliga uppföljningar att nya informationstillgångar som tillkommit (och som behöver informationsklassas), är dokumenterade i dokumenthanteringsplanen
- riskanalyser, informationsklassning och behov av skyddsåtgärder revideras (om nya hot och risker tillkommit, incidenter förekommit) av aktuella ansvariga.
- årlig åtgärdsplan med rekommenderade skyddsåtgärder för informationssäkerhet inkl. IT- och cybersäkerhet upprättas som underlag för beslut

Uppföljning ska ske en gång per år av ovanstående punkter. Det vilar ett gemensamt ansvar på den virtuella säkerhetsorganisationen att den årliga uppföljningen genomförs.

Resultatet av systemägares och informationsägares årliga uppföljningar av informationssäkerhet inkl. IT- och cybersäkerhet för sina informationstillgångar vilka ska ha resulterat i åtgärdsplaner för förbättrad informationssäkerhet inkl. IT- och cybersäkerhet ska lämnas till informationssäkerhetsansvarig i samband med verksamhetsplaneringen för vidare bearbetning till en åtgärdsplan för hela KMH.

Informationssäkerhetsansvarig ansvarar för att i dialog med IT-säkerhetsansvarig ta fram en övergripande lägesbeskrivning utifrån inrapporterade IT-incidenter under året samt utarbeta en rekommenderad årlig åtgärdsplan för KMH:s alla planerade säkerhetsåtgärder för nästkommande verksamhetsår.

Underlaget för lägesbeskrivning och rekommenderad åtgärdsplan tas upp i säkerhetsgruppen som gör eventuella slutjusteringar. Därefter redovisas detta för rektor. Beslut fattas av högskoledirektören när resurser för skyddsåtgärder är avsatta och finns inplanerade i verksamhetsplanen.

Förutom ovanstående har informationssäkerhetsansvarig ett samordningsansvar och för att löpande informera/utbilda KMH:s chefer, medarbetare och studenter i informationssäkerhet vilket innebär följande:

- samordna interna utbildningsinsatser på akademier och avdelningar
- påminna högskoleledning, akademichefer och avdelningschefer om sitt chefsansvar gällande informationssäkerhetsfrågor
- informera medarbetare och studenter om eventuella förändringar inom lag och förordning gällande informationssäkerhetsfrågor.

3.3 IT-incidentrapportering

IT-incidenter ska enligt MSB:s föreskrift 2020:08 anmälas omgående till MSB och rapport inlämnas inom giltig tid. IT-säkerhetsansvarig samordnar rapportering av KMH:s samtliga IT-incidenter till MSB.

Samtliga myndigheter har även rapporteringsskyldighet till integritetsmyndigheten (IMY) rörande incidenter som rör personuppgifter som röjs. Dataskyddssamordnare samordnar rapportering av sådana incidenter till IMY.

Varje medarbetare och student har ett eget ansvar för att rapportera IT-incidenter och incidenter avseende röjande av personuppgifter till IT-säkerhetsansvarig respektive dataskyddsansvarig,

Respektive chef, systemägare och informationsägare har ansvar att rapportera incidenter inom sina respektive områden. Dessa har även ansvar för att ta fram förslag till åtgärder för att minska risken för att incidenten uppstår igen.

Inkomna rapporter om IT-incidenter och incidenter rörande röjande av personuppgifter inom ramen för dataskyddsförordningen tjänar som underlag för vilka förbättringar som kan behöva göras inom informationssäkerhetsområdet.

3.3.1 Beredskap gällande IT-incidenter

På liknande sätt som högskolan har en krisgrupp med definierade arbetsuppgifter och checklistor, ska även en beredskap för IT-incidenter finnas i form av kontinuitetsplaner. Ansvaret för upprättande av kontinuitetsplaner ligger på IT-chef, systemägare och informationsägare för sina respektive områden.

Syftet med kontinuitetsplaner är att säkerställa att högskolan kan bedriva sin verksamhet så bra som möjligt, trots eventuella avbrott, kriser, IT-incidenter, stölder, sabotage m.m.

4 Användning av KMH:s IT- resurser

4.1 Allmänt

KMH:s IT-resurser ägs av högskolan och är avsedda att användas i och för högskolans verksamhet att tillhandahålla utbildning, forskning och därtill knuten administration samt för att samverka med det omgivande samhället. Resurserna får inte tas i anspråk för ändamål genom vilka högskolans namn, anseende och goda rykte kan skadas.

Med IT-resurser avses datorer, mobiltelefoner, surfplattor, programvaror, programvarulicenser, kommunikationsnät och all annan kringutrustning som nyttjas i samband med kommunikation och hantering av information i digital form.

4.2 Regler för användning

4.2.1 Begränsningar i nyttjandet av KMH:s IT-resurser

Högskolans IT-resurser får inte nyttjas för att på otillbörligt eller oetiskt sätt sprida, förvara eller förmedla information

- i strid mot gällande lagstiftning, t.ex. hets mot folkgrupp, barnpornografibrott, olaga våldsskildring, förtal, ofredande, dataintrång eller upphovsrättsbrott
- som, utan koppling till användares roll vid KMH, är att betrakta som politisk, ideologisk eller religiös propaganda
- i strid mot GDPR om den personliga integriteten
- som är personligt kränkande eller stötande
- som syftar till att marknadsföra produkter eller tjänster som saknar anknytning till högskolan
- i strid mot av KMH:s ingångna avtal avseende IT-resurser
- eller på annat sätt störa KMH:s IT-verksamhet
- Högskolans IT-resurser användas endast i begränsad omfattning för privat bruk.

4.2.2 Ansvar och befogenheter

Innan användare ges behörighet att nyttja KMH:s IT-resurser ska hen informeras om gällande regler för användning och bekräfta att hen tagit del av KMH:s ansvarsförbindelse för användning av IT-resurser".

En användare ska verifiera sin identitet med stöd av giltig ID-handling, bankID eller motsvarande för att användarkontot ska aktiveras.

Användaridentiteten ska alltid kunna spåras. Det är därför inte tillåtet att använda någon annans behörighet eller utnyttja felaktiga konfigurationer, programfel eller på annat sätt manipulera IT-resurserna.

Den tilldelade behörigheten är tidsbegränsad och är kopplad till studier, anställning, projektdeltagande eller uppdrag. Användaren ska själva meddela omständigheter som medför att behörigheten ska upphöra.

4.3 Regler för användning av Internet och e-post

4.3.1 Allmänt

KMH:s nätverk är anslutet till SUNET:s nätverk. En dator ansluten till nätverket är ständigt utsatt för intrångsförsök. Information som sänds eller görs åtkomlig via Internet kan även bli åtkomlig för obehöriga. Varje användare har ett ansvar att skydda KMH:s IT-resurser mot intrång och information mot åtkomst för obehöriga.

Därför ska:

- datorer och datorsystem alltid vara skyddade med säkert konstruerat lösenord, se punkt 1.5, eller annan teknisk behörighets- och användaridentifikation
- datorer som ägs av KMH ska ha av KMH licensierade antivirusprogram och andra av KMH rekommenderade skyddssystem.
- övriga datorer som ansluts till KMH:s IT-resurser ha likvärdigt skyddssystem installerat för att uppnå ett tillräckligt skydd.
- användaren ska aldrig ladda ner program och filer till en dator som är ansluten till KMH:s IT-resurser utan att först analysera säkerhetsrisken
- alla intrångsförsök ska anmälas till IT-support.
- konfidentiell eller information som innehåller känsliga personupgifter ska inte skickas med e-post eller göras åtkomlig via Internet.

Vid osäkerhet om ovanstående reglers tillämpning ska IT-support kontaktas.

4.3.2 Användning av Internet

Det är förbjudet att nyttja KMH:s IT-resurser för att ladda ner upphovsrättsskyddat material utan rättighetsinnehavarens tillstånd.

Text som publiceras på KMH:s webbplats ska ske via samverkansavdelningen för säkerställande av att innehållet följer rådande lagstiftning avseende personuppgifter (GDPR) eller upphovsrätt.

Den medarbetare som inom ramen för sin anställning använder sig av socialt media eller molntjänst ska, innan användningen, ta ställning till de risker i förhållande till informationen/materialet, som kan kopplas till användning av mediet och tjänsten. Det avser t.ex. upphovsrätt, personlig integritet och innehållet i användarförbindelsen eller annat avtal. Riskbedömningen görs utifrån KMH:s regler för informationsklassning.

4.3.3 E-post

All e-post som skickas från en adress inom KMH representerar högskolan. I e-post ska det finnas korrekta uppgifter om avsändarens namn och e-postadress.

Innan man skickar e-postmeddelanden ska e-postadressen kontrolleras noga, så att brevet når rätt adressat.

4.3.4 E-post som hanteras av KMH:s medarbetare

E-post omfattas av reglerna för allmänna handlingar. Registrering (diarieföring) av allmänna handlingar, i form av e-post, ska därför ske enligt samma regler som vanliga pappersdokument.

Varje medarbetare har ansvar för att hantera inkommande e-post samt att vid frånvaro se till att den tas emot och vid behov handläggs.

All mottagning och sändning av e-post till/från KMH ska ske via KMH-e-postadress.

Det är inte tillåtet att automatiskt vidaresända e-post innehållande verksamhetsinformation riktad till en KMH-adress till en extern adress. E-post ställd till KMH ska också besvaras från en KMH-e-postadress.

4.4 Regler för medarbetares distansåtkomst mot KMH:s IT-resurser

4.4.1 Allmänt

För att upprätthålla god säkerhet vid distansåtkomst ställs det krav på hög säkerhet i hela kommunikationskedjan från användare, utrustning och program fram till nyttjad IT-tjänst.

För åtkomst av vissa IT-tjänster ska användaren själv ta reda på vilka regler och anvisningar som informationsägare och/eller systemägare, drifts- eller systemleverantörer satt upp för den aktuella IT-tjänsten och ingående IT-system.

För åtkomst till vissa IT-system i KMH:s IT-miljö kan användning av virtuel private network (VPN) krävas.

4.4.2 Distansarbete från privat dator

I syfte att upprätthålla god säkerhet även vid arbete från privat datorutrustning mot någon av KMH:s IT-resurser ska denna ha minst motsvarande skydd som av KMH-ägda datorer. Den privata datorutrustningen ska ha

- individuella lösenord, se pkt 4.5 nedan
- uppdaterat antivirusprogram
- säkerhetsmässigt uppdaterade programvaror

Vid bredbandsuppkoppling ska ett extra intrångsskydd genom en så kallad brandvägg vara installerat.

4.5 Regler för lösenord och inloggning

Högskolans IT-system respektive varje användare, ska skyddas med lösenord och/eller annan teknisk behörighets- och användaridentifikation.

För att skyddet genom lösenord ska fungera effektivt ska följande kriterier vara uppfyllda.

- Användaridentitet, lösenord och tilldelad behörighet ska vara personlig.

- Lösenorden ska hållas hemliga och får inte lånas ut.
- Ett lösenord ska vara konstruerat med minst 8 tecken som är blandade med versaler, gemener, siffror och något specialtecken. Det får inte anknyta till den egna personen såsom namn, födelsedatum, utgöra enkla ord eller dylikt och inte heller bestå av tangenter som sitter i grupp.
- Lösenordet ska bytas regelbundet eller så fort det blir känt för någon utomstående.
- Funktionen för automatisk skärmlåsning (energisparläge) efter max 30 min inaktivitet bör alltid vara inkopplad. För fortsatt arbete på datorn måste den alltså låsas upp med ett lösenord.
- Användaren ska alltid logga ut från datorn när den lämnas utan egen uppsikt.

4.6 Påföljder och åtgärder vid regelbrott

Överträdelse av dessa regler kan medföra att användare helt eller delvis stängs av från nyttjande av högskolans IT-resurser. Beslut tas av verksamhetsansvarig för det aktuella ansvarsområdet.

Drifts- eller systemleverantör kan, i den akuta situationen, med omedelbar verkan stänga av misskött eller missbrukad IT-resurs.

Överträdelse av dessa regler anmäls av akademichef/ avdelningschef eller motsvarande till

- rektor beträffande studenter. Rektor har att ta ställning till om ärendet ska hänskjutas till disciplinnämnd. De disciplinära påföljderna är varning eller avstängning under viss tid från undervisningen och annan verksamhet vid universitetet
- personalansvarsnämnd beträffande anställd. Påföljden kan bli disciplinansvar eller avstängning.

Misstanke om brott kan medföra polisanmälan.

5 Systemanskaffning och systemutveckling

5.1 Allmänt

Dessa regler är i första hand avsedda att styra anskaffnings- respektive utvecklingsprocessen för IT-system med flera användare, men ska även i tillämpliga delar beaktas vid anskaffning och utveckling av mindre en- och fåanvändarsystem.

5.2 Organisation och ansvar

5.2.1 Organisation

Vid anskaffning och utveckling av mindre system leder systemägare och drifts- och systemleverantör i samråd anskaffnings- och utvecklingsfaserna direkt via projektledaren.

Vid anskaffning respektive utveckling av större IT-system med många användare och/eller komplexa IT-system ska en särskild projektorganisation skapas.

Projektorganisationens styrgrupp leder anskaffnings- och utvecklingsarbetet fram till överlämnandet av det färdiga och dokumenterade IT-systemet till förvaltningsorganisationen, som ska ansvara för den framtida driften.

5.2.2 Systemägare

Systemägare ska utses tidigt i anskaffnings- respektive utvecklingsprocessen. Det bör ske redan under *förstudiefasen*.

Systemägaren ansvarar för:

- att identifiera informationsägaren för informationen som systemet ska hantera
- att informationsägarens säkerhetskrav genomförs. Säkerhetskraven ska anges med inriktning på konfidentialitet, riktighet och tillgänglighet samt spårbarhet
- att det planerade systemet utformas och förvaltas så att det uppfyller kraven på god informationssäkerhet
- att projektorganisationen har tillgång till erforderlig informations- och IT- säkerhetskompetens
- att i de fall personuppgifter kommer att ingå i det planerade IT-systemet ska detta dokumenteras och anmälas till högskolans dataskyddsombud. IT- systemet ska utformas så att det uppfyller GDPR-krav
- att en systemförvaltningsorganisation med utöver systemägare utsedd systemförvaltare, system- och driftsleverantör skapas för IT- systemets drift och underhåll.

5.2.3 Drifts- och systemleverantörer

Ansvarar för:

- att informationsägarens och systemägarens säkerhetskrav uppfylls tekniskt
- att säkerhetstekniska lösningar följer KMH:s standarder

- att systemet i förekommande fall kan integreras med befintliga IT-system utan att IT-säkerheten försämras
- att drifts- och systemleverantör utses till av systemägare föreslagen systemförvaltningsorganisation
- att IT-systemet förs in i KMH:s systemförteckning som hålls av IT-avdelningen.

5.2.4 Projektledare

Projektledaren ansvarar för:

- att föreskrivna informationssäkerhetsaktiviteter genomförs och dokumenteras i projektets olika faser
- att incidenter och andra händelser som ur säkerhetssynpunkt påverkar projektet eller IT-systemets slutliga säkerhet rapporteras till systemägare samt till drifts- och systemleverantör
- att föreskrivna informationssäkerhetsaktiviteter genomförs och dokumenteras i projektets olika faser
- att incidenter och andra händelser som ur säkerhetssynpunkt påverkar projektet eller IT-systemets slutliga säkerhet rapporteras till systemägare och IT- leveransägare.

5.3 Säkerhetsstyrning i de olika anskaffnings- och utvecklingsfaserna

I syfte att åstadkomma kostnadseffektiva och fungerande säkerhetslösningar ska säkerhetsaspekterna belysas och säkerhetskrav successivt arbetas in i de olika anskaffnings- och utvecklingsfaserna.

För att kunna planera in resurser samt undvika resursbrist under anskaffnings- och utvecklingsfaserna ska alla IT-projekt som rör nyanskaffning/utvecklingsinsatser vara prioriterade och förankrade i verksamhetsplanen innan arbetet startar. IT-avdelningen har en samordnande roll gällande IT-utvecklingsinsatser för hela KMH och sammanställer årlig IT-handlingsplaner i samband med verksamhetsplaneringen.

5.3.1 Förstudiefasen

I förstudiefasen ska en övergripande informationsklassning genomföras av den information som IT-systemet ska hantera.

Informationsklassningen ska ge svar på

- förekomst av personuppgifter

- krav på konfidentialitet t.ex. förekomst av sekretessbelagd eller annan information av känslig karaktär
- krav på informationens riktighet och spårbarhet
- krav på tillgänglighet.

5.3.2 Analysfasen

Under analysfasen ska en säkerhetsanalys genomföras. I säkerhetsanalysen ska hot och risker analyseras och dokumenteras samt förslag till åtgärder utformas.

5.3.3 Upphandlings- och/eller konstruktionsfasen

Beslutade systemspecifika säkerhetskrav och -åtgärder inarbetas i kravspecifikationen och förfrågningsunderlaget tillsammans med de generella IT- säkerhetskraven enligt pkt 3.5 nedan, respektive regler för ”Drift och underhåll”.

Avvikelser från beslutade säkerhetskrav ska dokumenteras och anmälas till informationsägarare, systemägare samt till drifts- och systemleverantör för analys och beslut.

I förekommande fall ska anmälan göras till KMH:s dataskyddsombud.

5.3.4 Dokumentation

Leverantör/ konstruktör ska tillhandahålla användar-, utbildnings-, drift- och systemdokumentation samt teknisk dokumentation. Dokumentation ska utformas så att justeringar eller uppdateringar kan ske i efterhand av annan än den ursprunglige konstruktören av IT-systemet.

5.3.5 Test och överlämnande

Test och kontroll av verkan av säkerhetsåtgärder/-lösningar ska dokumenteras och godkännas av systemägare samt drifts- och systemleverantör innan IT-systemet sätts i produktion.

Uppgraderingar och revideringar av IT-system ska testas innan de sätts i produktion.

Test ska genomföras i särskild testmiljö. Om test i särskild testmiljö inte är möjlig ska andra lämpliga kontroller göras för att undvika driftstörningar eller felaktig funktion när IT-systemet sätts i produktion.

5.3.6 Utbildning

Systemägare ansvarar för att erforderlig utbildning av systemförvaltare och användare planeras och genomförs.

Drifts- och systemleverantör ansvarar för att erforderlig utbildning av systemförvaltare och systemadministratörer planeras och genomförs.

6 Krav på anlitade externa leverantörer

6.1 Krav på externt anlitade drifts- och systemleverantörer

Leverantörsbedömning

I syfte att säkerställa externa leverantörers framtida åtaganden ska en bedömning av leverantören göras i samråd med KMH:s ekonomiska kontroller på avdelningen för ledningsstöd.

Med hänsyn till resultatet från genomförd informationsklassning samt risk- och säkerhetsanalys ska leverantör, samverkande part eller annan levererande organisation bedömas utifrån samma krav som framgår av avsnittet ”Grundläggande säkerhetskrav vid IT-drift genom extern leverantör”.

6.1.1 Säkerhetsorganisation

Hos externa leverantörer ska det finnas en säkerhetsorganisation med en ansvarig chef och en namngiven kontaktperson för säkerhetsfrågor. Kontaktpersonen för säkerhetsfrågor bör anges i avtalet med leverantören.

Leverantören ska för KMH redovisa företagets gällande säkerhetspolicy och riktlinjer avseende:

- fysisk säkerhet
- IT-säkerhet
- sekretess

Eventuella ändringar av nämnda policy och riktlinjer ska anmälas till av KMH utsedd kontaktperson. Efter bedömning kan vid behov hela eller delar av aktuella riktlinjer bifogas avtalet.

Generellt ska leverantören följa KMH:s riktlinjer för Informations- och IT-säkerhet samt därtill knutna regler och riktlinjer.

Efter avslutat uppdrag ska

- leverantören återlämna sekretessbelagt och känsligt material
- leverantören återlämna all data i systemet som av KMH anger ska bevaras samt i digitalt format
- kvarvarande digitalt lagrade uppgifter hos leverantören som avser KMH-data raderas/förstöras enligt KMH:s direktiv
- all systemdokumentation återlämnas till KMH.

6.1.2 Sekretess och personalkontroll

I avtalet om IT-drift genom extern leverantör ska följande sekretessklausul ingå:

Leverantören förbinder sig att följa gällande säkerhetsregler som KMH från tid till annan fastställer samt se till att berörd personal/konsult och anlitad underleverantör iakttar dessa.

I de fall leverantören ges tillgång till, enligt Offentlighets- och sekretesslagen (2009:400), skyddad information ska tillämpliga bestämmelser i nämnda lag beaktas. Leverantören ska informera personal/konsult och anlitad underleverantör om gällande sekretess. Sekretess gäller även om avtalet i övrigt upphört att gälla.

Leverantören får inte till tredje man lämna ut handlingar eller på annat sätt återge uppgifter om KMH:s verksamhet som kan vara att betrakta som affärs- eller yrkeshemlighet eller som i övrigt rör KMH:s interna förhållanden, i annan utsträckning än som behövs för uppdragets genomförande.

Leverantören ska redogöra för vilken typ och omfattning av säkerhetsprövning man gör innan enskild medarbetare får arbeta med uppdraget för KMH.

Prövningen ska minst omfatta

- personlig kännedom
- uppgifter som framgår av betyg, intyg och referenser.

En säkerhetsbedömning görs av leverantörens svar utifrån resultatet av genomförd informationsklassning och säkerhetsanalys.

6.1.3 Hantering av sekretessbelagd information

Uppdraget som externt anlitad leverantör innebär att leverantören och eller dennes underleverantör

- arbetar i högskolans lokaler och hanterar eller kan få del av sekretessbelagd och känslig information
- tilldelas egen personlig behörighet till KMH:s IT-resurser.
- Ska undertecknar en sekretessförbindelse i anslutning till att uppdraget startar

6.1.4 Hantering av utrangerade minnesmedia

Utrangering av minnesmedia ska ske enligt dessa riktlinjer.

6.1.5 Säkerhetsorganisation

Hos leverantören ska det finnas en säkerhetsorganisation med en ansvarig chef och en namngiven kontaktperson för säkerhetsfrågor. Kontaktpersonen för säkerhetsfrågor bör anges i avtalet med leverantören.

Endast i avtalet namngiven personal får nyttjas för uppdraget. Förändring av namngivna personer ska skriftligt godkännas av KMH.

Personalen ska kunna legitimera sig med av leverantören utfärdad legitimation.

6.1.6 Fysisk säkerhet

I uppdragsavtalet ska

- leverantören förbinda sig att följa högskolans säkerhetsriktlinjer avseende tillträde till lokalerna
- leverantören förbinda sig att inte föra ut några sekretessbelagda eller känsliga handlingar, filer, bärbar media, material eller annan information utanför högskolans lokaler samt att följa KMH:s regler och riktlinjer för förvaring av denna typ av material och information.

6.1.7 IT-säkerhet

Leverantören ska följa KMH:s riktlinjer för informations- och IT-säkerhet samt därtill knutna regler och riktlinjer.

Någon överföring av filer eller programvara till nät utanför KMH:s nät får inte ske utan godkännande av ansvarig uppdragsgivare på KMH.

Sekretessbelagd och känslig information ska av leverantören hanteras enligt följande:

- Sekretessbelagd och känslig information ska hanteras och förvaras så att obehörig inte kan ta del av den. Förvaring ska ske i datamediaskåp som utöver miljökraven uppfyller kravet för säkerhetsskåp enligt SS 3492.
- All elektronisk kommunikation av sekretessbelagd eller känslig information ska ha det säkerhetsskydd som fastställts efter genomförd informationsklassning.
- Transport av handlingar och flyttbart medium som innehåller sekretessbelagd eller känslig information ska ske i låst portfölj av leverantörens eller KMH:s personal.
- Eventuell postbefordran ska ske med ESS-brev, REK.

7. Grundläggande säkerhetsskydd för IT-plattform och IT-system/-tjänster

7.1 Autentisering

Varje användare ska ha ett unikt individuellt användarkonto (-identitet) för att säkerställa att endast behöriga användare har tillgång till KMH:s nätverk och interna IT-system/-tjänster som kräver inloggning. En förteckning över nyttjade användaridentiteter ska kunna skapas med koppling till användarens personuppgifter (namn och personnummer).

IT-system/-tjänster ska kunna använda sig av och anslutas till extern autentiseringtjänst såsom t.ex. SAML-federering eller Microsoft ADFS.

All autentisering ska ske i krypterad form.

7.2 Behörighetskontrollsystem

KMH:s nätverk, IT-system/-tjänster ska ha rollbaserade behörighetskontrollsystem som kan anpassas till informationsägarens och systemägarens krav på säkerhet utifrån organisation och genomförd säkerhetsanalys.

Vid behov ska behörighet till olika nivåer inom organisationen vad avser tillgänglighet av information kunna skapas. Med nivåer avses t.ex. när aktuella användare av systemet ska se olika typer av data i systemet beroende på sin roll.

En lista över behörigheter i IT-systemet ska finnas tillgängligt som visar:

- användarens identitet
- gällande behörigheter kopplat till datum för tilldelning och borttagande respektive tidsbegränsning av behörighet.

Om tekniskt möjligt bör denna lista kunna tas ut ur IT-systemet.

Endast de som tilldelats behörighet ska ha åtkomst till KMH:s nätverk, IT-system och -tjänster och till den information och de processer som de hanterar.

IT-chef ansvarar för att behörighet till användarkonto som ger tillgång till KMH:s nätverk och KMH:s IT-resurser och lokaler följer fastställda riktlinjer för tilldelning av användarkonto och passerkort.

Systemägare och informationsägare ansvarar för att behörighetsrutiner finns upprättade för sina respektive IT-system/-tjänster och information.

För att kunna spåra, upptäcka och åtgärda felaktigheter och oegentligt användande av information i IT-system/-tjänster ska loggning finnas i respektive IT-system/-tjänst.

7.3 Kontinuitets-, avbrotts- och krisplanering

Kontinuitets-, avbrotts- och krisplaneringen ska beskriva vad som avses med normalt respektive onormalt läge för IT-system/-tjänst och IT-plattform. Förebyggande och skadebegränsande hanteringsrutiner ska finnas.

Det ska finnas fastställda kontinuitets-, avbrotts- och krisplaner för KMH:s verksamhetskritiska IT-system samt för IT-plattformen som helhet.

Högskoledirektören beslutar i dialog med Rektor vilka system som är verksamhetskritiska för säkerställande av KMH:s verksamhet.

För övriga IT-system/-tjänster fastställer systemägare eller informationsägare om kontinuitets-, avbrotts- och krisplaner behöver upprättas.

Vid upprättande av kontinuitets-, avbrotts- och krisplanering ska detta arbete föregås av en riskanalys. Hänvisning görs till avsnittet om ”*Metod för systematiskt informationssäkerhetsarbete*” och ”*riskanalys*”.

Inom ramen för det normala läget ska det klarläggas hur man bibehåller kontinuitet, samt vilka krav det ställer avseende driftshanteringen i fråga om förebyggande av avbrott, begränsad skada samt återställande av data.

För det onormala läget ska krisplanering klarlägga krisscenarier och därtill kopplade hanteringsrutiner för IT-verksamheten, i syfte att begränsa skador och på sikt återställa normal driftsituation.

7.4 Kommunikation

KMH:s krav på konfidentialitet, riktighet och tillgänglighet i datakommunikationen i KMH:s nätverk och mellan IT-system ska följa standardkrav. Kommunikationslösningen ska motsvara dessa krav och endast användas för sådan information den är anpassad för.

7.5 Loggning

IT-system bör ha funktioner och rutiner för loggning av säkerhetsrelaterade händelser i systemet för att kunna säkerställa spårbarhet, underlätta framtida utredningar av driftstörningar och eventuella oegentligheter.

Loggning bör ske automatiskt och inte kunna förvanskas eller förstöras. Endast i undantagsfall, när automatisk loggning inte kan lösas tekniskt, ska manuell loggning övervägas utifrån skyddsvärdet.

7.6 Brandväggar

Anskaffning och konfigurering av brandväggar ska följa KMH:s standard.

7.7 Virusskydd
IT-avdelningen ska tillhandahålla antivirusskydd för arbetsdatorer.

7.8 Certifikat
I de fall där IT-system nyttjar certifikat ska ett av KMH:s IT- avdelning rekommenderat certifikat användas.

7.9 Trådlösa nätverk
Vid nyetablering av trådlösa nätverk inom KMH ska, den gemensamma lösningen som tagits fram för högskolan användas.

7.10 Extern åtkomst
All extern åtkomst till KMH:s nätverk ska ske genom av KMH fastställd säker anslutning.

7.11 Källkodsdeponering
Deponering av källkod till KMH:s IT-system ska vara väl dokumenterad och ske på ett sätt som säkerställer framtida drift, kompletteringar och underhåll av IT- systemen. Vidare gäller följande:

- Vid upphandling av IT-system ska källkodsdeponering regleras i avtal.
- Vid egenutveckling av IT-system ansvarar intern systemleverantör för att källkoden deponeras/arkiveras på ett säkert sätt.
- Deponeringen/arkiveringen ska uppfylla ”Riksarkivets föreskrifter och allmänna råd om arkivlokaler” (RA-FS 2013:4).

7.12 Driftsäkerhet
För att behålla hög tillgänglighet och minska risken för informationsförluster ska KMH:s IT-system ha en konstruktion som ger hög driftsäkerhet och vara utrustad med en lättarbetad administrationsmodul. Support och underhåll ska säkerställas för systemets hela livslängd. Detta ska anges i systemförvaltningsdokumentationen.

Driftsansvarig ska innan driftsättning av nya IT-system/-tjänster godkänna driftsättningen.

7.13 Avveckling av IT-system
En plan både för avvecklingen av IT-systemet samt principer för hur väsentliga data ska sparas ska tas fram redan på *planeringsstadiet*.

8 Drift och underhåll

8.1 Systemadministration

8.1.1 Systemförteckning

KMH:s gemensamma IT-system och -tjänster, ska finnas förtecknade centralt på IT-avdelningen med angivande av:

- Systemnamn
- Informationsägare
- Systemägare
- Systemförvaltare
- Driftsleverantör
- Systemleverantör
- Om systemet innehåller personuppgifter.

8.1.2 Roller

IT-chef samt systemägare ska i den dagliga driften och underhållet av IT-system och IT-infrastruktur stödjas av en för respektive system utsedd operativ systemförvaltare.

Driftsleverantören ska i den dagliga driften och underhållet av IT-system och IT- infrastruktur stödjas av

- en för respektive IT-system och IT-infrastruktur utsedd ansvarig
- en eller flera systemadministratörer.

8.1.4 Ansvarförbindelser för IT-personal

Innan medarbetare ges behörighet att arbeta med drift och underhåll av KMH:s IT- resurser ska hen vidimera att hen tagit del av gällande regelverk för informations- och IT-säkerhet, ansvarsförbindelse för användning av KMH:s IT-resurser vid KMH samt undertecknat sekretessförbindelse för medarbetare med högre teknisk och administrativ behörighet till KMH:s IT-resurser.

8.1.5 Beslut om och dokumentation av systemförändringar

Beslut om systemförändringar fattas av respektive systemägare i samråd med systemleverantör.

Systemförvaltare och systemleverantör ansvarar för att både beslut om systemförändring och genomförd förändring dokumenteras och arkiveras på ett säkert sätt som medger:

- uppföljning av vidtagna systemförändringar

- eventuell överlämning av både systemförvaltning och teknisk förvaltning.

8.1.6 Test före driftsättning

Alla systemförändringar ska före driftsättning testas i särskild testmiljö. Om test i särskild testmiljö inte är möjlig ska andra lämpliga kontroller göras för att undvika driftstörningar eller felaktig funktion när systemförändringen sätts i produktion.

Driftsansvarig vid IT-avdelningen ska vid driftsättning av nya IT-system/-tjänster genomföra en bedömning av om driftsättning kan godkännas utan att det får negativ inverkan på driftsäkerheten i IT-plattformen och för övriga IT-system i denna.

8.2 Behörighetsadministration

8.2.1 Grunder

En fungerande och säker behörighetsadministration är en av de viktigaste grunderna i KMH:s IT-säkerhetsarbete.

Användare får endast tilldelas behörighet till KMH:s IT-resurser i den omfattning som krävs för dennes arbetsuppgifter eller studier.

8.2.2 Allmän behörighet

Innan användare ges behörighet att använda KMH:s IT-resurser ska han/hon informeras om gällande regler för användning genom att verifiera att denna tagit del av Ansvarsförbindelse för användning av KMH:s IT-resurser.

8.2.3 Behörighet till IT-system med särskilda behörighetsregler

Riktlinjer för tilldelning av behörigheter till specifika IT-system beslutas av respektive informationsägare/systemägare.

8.2.4 Roller vid behörighetshantering

Informationsägare

Utifrån regler för informationsklassning och genomförd säkerhetsanalys ansvarar respektive informationsägare för att i samråd med systemförvaltaren utarbeta regler för behörighetstilldelning.

Systemägare

Systemägaren ansvarar för att informationsägarens regler för behörighetstilldelning säkerställs.

Drifts- och systemleverantörer

Drifts- och systemleverantör ansvarar för att informationsägarens och systemägarens säkerhetskrav på behörighetskontroll uppfylls tekniskt samt att loggar säkerhetskopieras, sparas och förvaras på ett säkert sätt under föreskriven tid.

Behörighetsansvarig

Behörighetsansvarig beslutar om tilldelning av behörigheter till högskolans gemensamma och lokala system samt ansvarar för uppföljning av tilldelade behörigheter. Tilldelningen och uppföljningen ska följa regler fastställda av informationsägare, systemägare, system- och driftsleverantör.

Behörighetsansvarig kan vara avdelningschef inom högskoleförvaltningen, bibliotekschef eller akademichef eller motsvarande.

Behörighetsadministratör

Behörighetsadministratören utses av systemägare och ansvarar för inregistrering och avregistrering av behörigheter enligt behörighetsansvarigs beslut. Administratören ansvarar också för att beslut om behörighetstilldelning arkiveras enligt fastställda arkivregler. Systemförvaltaren är oftast densamma som behörighetsadministratör.

8.2.5 Dokumentation och arkivering av behörighetsbeslut

Bekräftelse på att en användare tagit del av ansvarsförbindelse för användning av KMH:s IT-resurser respektive beslut för behörighetstilldelning till IT-system med särskilda behörighetsregler ska bevaras i 1 år efter det att behörigheten har upphört.

Beslut om behörighetstilldelning avseende ekonomiska transaktioner i t.ex. ekonomisystemet och det personaladministrativa systemet ska bevaras i 10 år.

Dokumentation av beslut om behörighetstilldelning ska

- förvaras inlåsta så att obehörig åtkomst förhindras
- förvaras enligt gällande arkivregler så att ofrivillig förstörning genom brand eller liknande förhindras.

8.2.6 Borttagning av behörighet

Behörighetsansvarig ansvarar för att en användares behörigheter omedelbart tas bort när denne lämnar sin anställning, avslutar sina studier eller motsvarande

vid KMH och att behörigheterna anpassas vid förändrade arbetsuppgifter eller studier.

Behörighetsansvarig ansvarar för att det årligen sker en genomgång av tilldelade behörigheter mot

- aktuella användarförteckningar
- av systemägare framtagna listor över tilldelade behörigheter. Utifrån denna genomgång ska behörighetstilldelningen justeras och gallras.

8.3 Skydd av digital information

8.3.1 Säkerhetskopiering

Syfte med säkerhetskopiering är att garantera tillgänglighet till IT-system och lagrad information.

Säkerhetskopiering ska göras regelbundet.

Informationsägare/systemägare ska i samråd med driftsleverantör, utifrån genomförd informationsklassning och förändringsfrekvens i informationen, besluta om och dokumentera

- vilken information som ska omfattas av säkerhetskopiering
- tidsintervall för säkerhetskopiering
- vilka normer för säkerhetskopiering som ska följas
- när och hur kontroll av säkerhetskopiors läsbarhet ska genomföras och dokumenteras.

Alla IT-system ska säkerhetskopieras vid installation samt före och efter större förändring.

Löpande säkerhetskopiering av IT-system där information läggs till och förändras dagligen bör genomföras minst en gång per dygn.

IT-system och lagrad information ska kunna återskapas på annan maskinvara.

8.3.2 Brand- och stöldskydd för säkerhetskopior.

Säkerhetskopior ska förvaras i serverrum eller brandsäkert datamedieskåp med placering i annan brandcell än i vilken original informationen förvaras.

8.3.3 Hantering av driftsincidenter

Förekomna IT-incidenter ska *omgående* rapporteras av systemförvaltare till IT-avdelningen som vidarerapporterar till MSB i enlighet med MSB FS:2020:08.

Det åligger systemägare och driftsleverantören att tillsammans ombesörja att det i respektive systemförvaltningsdokumentation finns dokumenterade rutiner för hantering av driftsincidenter för varje IT-system.

Dokumentationen ska ta upp följande punkter:

- **Riskanalys och kontinuitetsplanering**
  Tänkbara scenarion och vilka åtgärder som ska företas för respektive scenario.
- **Rutiner för incidentrapportering**
  Rutiner för incidentrapportering som innehåller information om vilka som ska informeras vid olika skeden.
- **Leverantörsåtagande**
  Dokumentation om de avtal som finns gällande hårdvarugarantier, inställelsetid, support vid driftsincidenter etc.
- **Dokumentation och analys**
  Incidenter ska alltid dokumenteras och analyseras så att man skaffar sig kunskap om det inträffade och i fortsättningen undviker nya incidenter samt minskar tiden för åtgärd vid liknande incidenter i framtiden.

8.3.4 Hantering av IT-säkerhetsincidenter

Dataintrång

Vid dataintrång där person olovligen skaffat sig behörighet till IT-system ska IT-support kontaktas *omgående*. Intrånget ska analyseras så att det kan vidtas relevanta åtgärder i syfte att likartat intrång inte upprepas. När systemadministratör (motsvarande) kan fastslå att IT-systemet tagits över av obehörig ska systemet återställas genom ominstallation och återläsning av säkerhetskopia tagen före intrånget. Samtliga användare av det drabbade systemet ska förses med nya lösenord och om någon användare nyttjar flera system och använder samma lösenord för dessa ska även dessa lösenord bytas.

Virus/maskar

Vid intrång orsakade av virus/maskar ska systemet åtgärdas med de antivirusprogram som KMH tillhandahåller. I de fall där systemadministratör (motsvarande) bedömer att detta inte är tillräckligt ska systemet installeras om. Orsaken till virus/maskangreppet ska analyseras så att lämpliga åtgärder mot upprepning kan vidtas.

Missbruk

Upptäckt av interna intrång så som utökande av egna befogenheter, manipulering av data, att obehörigt ta del av eller obehörigt hantera digital

information etc. ska anmälas till avdelningschef/akademichef eller motsvarande, som informerar IT-avdelningens IT-säkerhetsansvarig.

8.4 Loggning

8.4.1 Allmänt

IT-system bör ha funktioner och rutiner för loggning av säkerhetsrelaterade händelser i systemet och bör kunna ske automatiskt. Syfte med loggar är att kunna säkerställa spårbarhet, underlätta framtida utredningar av driftstörningar och eventuella oegentligheter.

För att loggar effektivt bör de kunna nyttjas för utredning av säkerhetsincidenter samt som bevismaterial vid en eventuell rättslig prövning. Loggar bör därför vara för respektive IT-system är synkroniserade enligt KMH:s standard och kunna tas ut ur systemet vid behov.

Användarloggar ska sparas under tid som fastställts gälla för systemet av respektive systemägare.

Systemägare och informationsägare ansvarar för att i det systematiska informationssäkerhetsarbetet fastställa om loggar behöver finnas och hur länge de ska sparas.

8.4.2 E-postloggar

Funktioner för bevarande av e-postloggar ska vara påslagna i systemet.

8.5 Säkerhetsskydd i IT-plattformen

Hänvisning görs till MSB:s föreskrifter 2020:07 rörande skyddsåtgärder för informationssystem.

8.5.1 Brandväggar

Konfigurering av brandväggar ska följa KMH:s standard.

Brandväggarna ska vara försedda med IDS som ska vara påslaget för att kunna upptäcka intrångsförsök till KMH:s nätverk.

KMH ska använda DNSSEC.

8.5.2 Nätverk

Digitalt verktyg för hantering av regelverk i nätverk ska finnas för effektiv administration.

KMH ska ha **realtidsövervakning** av nätverkskommunikation.

KMH:s nätverk ska vara indelat i olika **nätverkssegment med filtrering** av trafik.

Vid **nyetablering av trådlösa nätverk** inom högskolan ska KMH:s standardlösning för högskolan användas.

Användare som sköter systemadministrativa uppgifter i känsliga tjänster t.ex. har tillgång till KMH:s driftsmiljö, ska ha ett separat **systemadministrativt individuellt konto** som är avskilt från det vanliga användarkontot samt använda **flerfaktorsautentisering**.

Identitetshantering och autentisering av KMH:s användare ska ske i enlighet med de krav som anges av SUNET för att bli godkänd användare av SWAMID-federationen. All autentisering ska även ske i krypterad form. Krypteringen ska följa av KMH:s standard.

Rutiner ska finnas för ändrings- och incidenthantering, livscykelhantering och för uppdatering av mjukvara.

Det ska finnas en tidsserver för att säkerställa korrekt och spårbar tid i KMH:s IT-plattform i enlighet med svensk standard (NTI).

Återställning från säkerhetskopior för IT-system och data ska testas regelbundet. Säkerhetskopiorna ska vara fysiskt och logiskt åtskilda från den ordinarie produktionsmiljön och bör vara placerade i olika brandceller.

KMH:s datorer ska vara försedda med antivirusskydd.

I de fall där IT-system nyttjar certifikat ska ett av KMH:s IT-avdelning rekommenderat certifikat användas.

8.6 Utformning av IT-utrymmen och serverrum

I syfte att skydda KMH:s IT-infrastruktur, applikationer och lagrade data mot oavsiktlig skada genom brand och vätskeläckage, avsiktlig skadegörelse respektive olovligt användande ska IT-utrymmen och serverrum följa *MSB:s vägledning för fysisk säkerhet i IT-utrymmen*. Reglerna ska ses som minimikrav och nyttjas vid ny- och ombyggnad samt som målbild för successiv höjning av IT-säkerheten i befintliga lokaler.

Datamedieskåp som används för skydd av digital information ska vara godkänt för datamedier enligt svensk standard SS-EN 1047-1. Förvaras sekretessbelagd information i skåpet ska det också uppfylla kravet för säkerhetskåp av klass SS3492.

8.7 Arkivering av information på IT-media

Arkivering av information lagrad på IT-media ska ske i rum eller skåp som uppfyller ”Riksarkivets föreskrifter och allmänna råd om arkivlokaler” (RA-FS 2013:4).

8.8 Fysiskt skydd av stationära och bärbara arbetsdatorer

8.8.1 Stationära arbetsstationer

Stationära arbetsstationer i öppnare miljöer, så som korridorer, datorsalar, receptioner samt i fönsterförsedda lokaler som lätt kan nås utifrån, ska vara fastlåsta. Datorn placeras i av IT-säkerhetsansvarig tillhandahållen säkerhetsanordning.

8.8.2 Bärbara datorer

På ordinarie arbetsplats bör det finnas möjlighet till fastlåsning alternativt inlåsning i skåp för bärbara datorer.

Om det inte finns möjlighet att låsa fast dessa kan en bärbar dator förses med utrustning för temporär fastlåsning.

8.4.3 Stöldskyddsmärkning

All IT-utrustning så som stationära och bärbara arbetsstationer inkl. skärmar, videoprojektorer, skärmar i entréer och dylikt ska stöldskyddsmärkas.

8.5 Omhändertagande av IT-media och utrustning som ska återvinnas

8.5.1 Allmänt

För att förhindra att lagrad information, så som personuppgifter, forskningsdata, sekretessbelagd information och liknande blir tillgänglig för obehöriga, ska alla utrangerade minnesmedier raderas och överskrivas samt eventuellt destrueras mekaniskt på ett säkert sätt..

Till minnesmedium räknas i detta sammanhang all elektronisk utrustning som innehåller en minnesfunktion såsom fasta och lösa hårddiskar, surfplattor, smartphones, mobiltelefoner, USB-minnen, cd, band, och annan elektronisk utrustning som innehåller minnesmedia. Även skrivare med inbyggda minnesfunktioner behöver raderas och överskrivas på ett säkert sätt innan de lämnar högskolan.

Alla utrangerade datorer och minnesmedium ska lämnas till *IT-support* för återvinning.

Avdelningschef/akademichef eller motsvarande ansvarar för att utrangerad IT-utrustning eller när medarbetares äldre dator ersätts av ny, att tidigare dator överlämnas till IT-avdelningen

Minnesmedium som innehåller *sekretessbelagd information eller minnesmedium från forskning* eller motsvarande med särskilda sekretesskrav, ska kontakt tas med KMH:s *IT-säkerhetsansvarig* för beslut om vidare åtgärd.

Inlämnad utrustning till IT-avdelningen ska fram till transport förvaras i låst och övervakat utrymme.

Externt företag som ombesörjer återvinning av datorer och minnesmedium ska kunna uppvisa användning av godkänt överskrivningsprogram enligt standard DoD 5520-22.M.

Överskrivning och eventuell fysisk destruktion ska dokumenteras. Av dokumentationen ska framgå datum för överskrivning rep destruktion, vem som utfört överskrivningen.

Enligt förordningen (2000:208) om producentansvar för elektriska och elektroniska produkter, ska aktuella elektronikleverantörer vid behov kunna återta utrangerad och kasserad IT-utrustning.