HÖGSKOLAN ARCADA

INFORMATIONSSÄKERHETSPOLICY

Fastställd av Högskolestyrelsen 11.3.2011

Innehåll

1. Allmänt

Denna informationssäkerhetspolicy (härefter ”Informationssäkerhetspolicyn” eller ”Policyn”) utgör det övergripande dokumentet för hur informationssäkerheten skall regleras inom högskolan Arcada. Ledningen ansvarar för att högskolan fungerar. Informationssäkerhetspolicyn redovisar ledningens viljeyttring och mål för informationssäkerhetsarbetet.

Arcadas verksamhet är i allt högre grad beroende av en oavbruten och reglerad tillgång till korrekt, aktuell och komplett information. Satsningen på informationssäkerheten är ledningens strategiska beslut som syftar till att märkbart förbättra högskolans konkurrenskraft. Också lagstiftningen ställer krav på hur man garanterar informationssäkerheten.

Informationssäkerhetspolicyn definierar även ansvarsfördelningen och metoderna för genomförandet av skyddet av informationen inom högskolan. Såväl medarbetarna som studerandena bör vara medvetna om Policyn och agera enligt den. Policyn konkretiseras i informationssäkerhetsinstruktioner. Dessa finns som bilagor till denna Policy.

En god administration av informationssäkerheten kräver kontinuerlig uppföljning av all verksamhet, långsiktig planering, beredskap för olika hot, iakttagande av överenskomna funktionssätt, anvisningar, utbildning och informationsspridning om Policyn.

2. Målsättningar

De långsiktiga målen för informationssäkerhetsarbetet är att säkerställa att Arcada kan tillhandahålla information i) som endast delges behöriga personer och kan levereras vid rätt tidpunkt och till skäliga kostnader (sekretess), ii) som är riktig, komplett och aktuell (riktighet), iii) som är relevant och nödvändig och som organisationen har ett ansvar att tillhandahålla (tillgänglighet), (iv), som skapar sådan bevisföring att en som har deltagit i databehandling eller dataöverföring efteråt inte kan förneka det (obestridighet)..

I begreppet informationssäkerhet beaktas som separata delområden enligt statsförvaltningens praxis administrativ säkerhet, personsäkerhet, fysisk säkerhet, datamaterialsäkerhet, kommunikationssäkerhet, utrustningssäkerhet, programsäkerhet och användningssäkerhet.

Med informationssäkerhetsarbetet strävar man efter att förebygga skador som kan orsakas av interna och externa hot eller begränsa dem till en godtagbar nivå samt förbereda sig på att återställa läget efter en problemsituation. Som en del av informationssäkerheten under normaltillstånd förbereder sig högskolan också inför störnings- och problemsituationer, så att verksamheten kan fortsätta under alla förhållanden.

3. Organisation, roller och ansvar

En tydlig ansvarsfördelning är en avgörande förutsättning för att Arcada skall kunna leva upp till de krav som ställs i Informationssäkerhetspolicyn. Säkerhetsansvaret följer organisationsstrukturen på Arcada. Var och en, som är ansvarig för någon del av verksamheten, ansvarar också för informationssäkerheten inom sitt område.

3.1 Roller och ansvar

Fördelningen av ansvaret ska säkerställa att ett IT-system kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stöda verksamheten och uppfylla Informationssäkerhetspolicyns mål. Den interna organisationen för informationssäkerhetsarbetet, roller, fördelning av ansvar och arbetssätt framgår av Säkerhetsinstruktionen ”Förvaltning” (bilaga 1).

3.2 Verksamhetsansvarig och systemförvaltare

Det övergripande ansvaret för att systemen uppfyller verksamhetens krav vilar på IT-styrgruppen. Gruppen har ansvar för att bedöma verksamhetens krav på säkerhet, tillförlitlighet, tillgänglighet, funktionalitet, verifierbarhet och att medarbetarna har tillräckliga kunskaper för att hantera systemen på ett säkert sätt. IT-styrgruppen tar också de beslut som berör systemens vidareutveckling, avveckling och gör förslag till införskaffning av nya system. Gruppen kan utse förvaltare för olika delsystem om så behövs.

3.3 Datasäkerhetschef

Datasäkerhetschefen har i uppdrag att bereda datasäkerhetsfrågor för IT-styrgruppen samt att handha det operativa ansvaret för datasäkerhetsutbildningen. Datasäkerhetschefen skall kontinuerligt följa upp lagstiftning som gäller datasäkerheten samt genomföra datasäkerhetsrelaterade utvecklingsprojekt, övervaka nya interna och externa hot och den datatekniska säkerheten i allmänhet. Datasäkerhetschefen har i samråd med IT-chefen befogenhet att vidta nödvändiga åtgärder då hot mot datasäkerheten uppstår i organisationen (Se bilaga 2.1).

3.4 IT-chef

IT-chefen har det operativa ansvaret för Arcadas IT-infrastruktur och för att de olika datasystemens tekniska delar fungerar tillsammans. IT-chefen är föredragande för IT-styrgruppen. IT-chefen ansvarar också för driften och resursfördelningen för respektive IT-system i Arcada.

3.5 Användare

Var och en som hanterar data ansvarar för sin egen del för informationssäkerheten och är skyldig att iaktta högskolans regler. Alla de personer och samarbetsorgan som hanterar **konfidentiell** information samt datatekniska experter och stöd- och handledningspersonal har ett utökat ansvar för säkerheten. Instruktionerna för användarna finns i Säkerhetsinstruktionen ”Användningsregler” (bilaga 2).

3.6 Informationssäkerhetsansvarig

Informationssäkerhetsansvarig är Arcadas rektor. Rektor bistås av förvaltningsdirektören, som skall säkerställa att målen med Informationssäkerhetspolicyn uppnås. Förvaltningsdirektören fungerar som ordförande för IT-styrgruppen.

4. Metoder för genomförande av informationssäkerheten

Upprätthållandet och utvecklingen av informationssäkerheten är en kontinuerlig process. Användarnas verksamhet styrs med hjälp av inbyggda regler för användningen samt genom

utbildning och information om hur man hanterar information på ett säkert sätt, som framgår av säkerhetsinstruktionen ”Förvaltning” (bilaga 1).

De nyanställda informeras om Informationssäkerhetspolicyn i samband med introduktionen av Arcada som arbetsplats.

Studenterna informeras om informationssäkerheten i samband med att nyttjanderätten emottas. Samtidigt förbinder de sig att följa aktuella regler och anvisningar.

Anvisningarna som behövs gällande informationssäkerheten i arbetet och studierna finns tillgängliga på Arcadas interna webbplats.

5. Information och kommunikation

Information om ärenden som gäller högskolans informationssäkerhet sprids inte aktivt utanför högskolan, eftersom det kan utgöra en säkerhetsrisk.

Högskolans datasäkerhetschef ansvarar i samråd med kommunikationschefen för den interna informationsspridningen som anknyter till högskolans IT-säkerhet. Den externa kommunikationen sköts av kommunikationschefen i samråd med rektorn och datasäkerhetschefen / IT-chefen.

6. Uppföljning av informationssäkerheten och hantering av problemsituationer

Upprätthållandet av informationssäkerheten kräver en kontinuerlig uppföljning, som omfattar övervakning av informationssäkerheten samt rapportering om säkerhetens nivå och eventuella problem. Uppföljningen genomförs både automatiskt och manuellt. För den tekniska uppföljningen finns separata anvisningar. Datasäkerhetschefen koordinerar uppföljningen av datasäkerheten och rapporterar om den till IT-chefen och IT-styrgruppen samt vid behov till rektor.

Datasäkerhetschefen och IT-styrgruppen har fullmakt av Arcadas högsta ledning att göra kartläggningar som anknyter till informationssäkerheten vid högskolan och att vidta åtgärder för att korrigera observerade brister.

Användarna och IT-administratörerna bör anmäla observerade brister i informationssäkerheten, missbruk som utgör hot mot den eller misstänkta brott till sin chef och till datasäkerhetschefen, som vidtar åtgärder enligt separata bestämmelser. Även för påföljderna av datasäkerhetsbrott finns separata regler. (Bilaga 2.1 Praxis och sanktioner vid IT-förseelser)

7. Fastställande och ändring av policyn

Denna policy har på förslag av IT-styrgrupen fastställts av Arcadas högskolestyrelse [11.3.2011]. Policyn tillämpas till den del annat inte bestämts i lag eller förordning. Beslut om ändring i policyn görs av högskolestyrelsen på förslag av IT-styrgruppen.

Bilagor:

Bilaga 1 Förvaltning
Bilaga 2 Användningsregler
Bilaga 2.1 Praxis och sanktioner vid IT-förseelser
Bilaga 2.1.1 Sanktioner

Bilaga 1 Förvaltning

I denna bilaga till Arcadas informationssäkerhetspolicy beskrivs hur Arcada organiserat arbetet för att förvalta informationssäkerheten.

Informationssäkerheten är en väsentlig del av Arcadas verksamhet och kvalitetssystem, den helhetsmässiga säkerheten och den dagliga databehandlingen inom högskolan. En god administration av informationssäkerheten kräver kontinuerlig uppföljning av all verksamhet, långsiktig planering, beredskap för olika hotande situationer, iakttagande av överenskomna funktionssätt, anvisningar, utbildning och information.

Som en del av det totala ansvaret svarar rektorn också för informationssäkerheten, dess genomförande, utveckling och skapandet av nödvändiga förutsättningar (bl.a. allokering av resurser) vid högskolan. För att förverkliga dessa har rektor utsett en IT-styrgrupp.

IT-styrgruppen ansvarar för högskolans IT-verksamhet och för organisering av informationssäkerheten.

Organisering av informationssäkerheten handhas i Arcada av IT-styrgruppen och datasäkerhetschef.

Informationssäkerhetens organisation och ansvarsfördelning vid Arcada

Genomförandet av informationssäkerheten är en kontinuerlig, omfattande verksamhet som inte kan handhas av endast några få ansvariga personer. I stället behövs tätt och konstruktivt samarbete mellan alla personer och grupper inom högskolan. Arcadas personal samt användare av systemen och tjänsterna deltar i genomförandet och övervakningen av informationssäkerheten som en del av sitt eget allmänna verksamhetsansvar.

Informationssäkerhetens ansvarsfördelning bör följa eventuella förändringar i högskolans verksamhet. Många av ansvarsområdena nedan kan höra till samma persons uppgifter och ansvar. Det väsentliga är att dessa uppgifter sköts också för ersättares del.

IT-styrgruppens ansvar

- genomförande av informationssäkerheten som en del av den helhetsmässiga ansvaret för informationssäkerheten på förslag/föredragning av datasäkerhetschefen,
- allokering av resurser och organisering av informationssäkerheten,
- informationssäkerhetens huvudlinjer,
- funktionernas informationssäkerhetsprioritering,
- uppföljning av informationssäkerheten,
- bereda och styra det praktiska genomförandet av högskolans datasäkerhet samt tillhörande utvecklingsåtgärder och riskhantering,
- ansvara för för högskolans kontinuitetsplaner för infrastrukturens och de centrala systemens del inför exceptionella förhållanden,
- ansvara för regelbundna riskanalyser,
- ansvara för att personalens säkerhetskunskap utökas och planera datasäkerhetsutbildningen
- ansvara för för att informationssäkerheten fungerar i anskaffade datatjänster,

- rapportera till den högsta ledningen om informationssäkerheten och
- lämna förslag och initiativ till rektorn och förvaltningsdirektören gällande högskolans informationssäkerhet.

Datasäkerhetschefens uppgift är att i samråd med IT-styrgruppen:

- bereda utvecklingsprojekt för datasäkerheten på Arcada,
- ansvara för genomförandet av utvecklingsprojekt för datasäkerheten,
- ansvara för organisering av datasäkerhetsutbildning
- informera om datasäkerhetsfrågor och – problem i samråd med kommunikationsavdelningen,
- delta i definieringen av datasäkerhetsprinciperna på Arcada,
- assistera ledningen och avdelningarna i att verkställa datasäkerheten,
- utveckla datasäkerhetsförslagen,
- organisera uppföljning av datasäkerheten,
- rapportera till den högsta ledningen om datasäkerheten.

IT-avdelningen uppgift är att:

- ansvara för det tekniska dataskyddet inom högskolan,
- ansvara för säkerheten i högskolans datakommunikationsnät,
- ansvara för för högskolans centrala säkerhets- och skyddskopiering,
- organisera utbildning i teknisk datasäkerhet för it-administratörerna och
- ge råd i frågor som gäller teknisk datasäkerhet.

Avdelningschefens/prefektens uppgift är att:

- rapportera om datasäkerheten och problem i samband med den.

De datatekniska experternas uppgift är att:

- tillämpa och genomföra högskolans datasäkerhetsprinciper med hjälp av sin egen specialexpertis,
- ansvara för datasäkerhetsåtgärder inom sitt eget område i samråd med datasäkerhets- och IT-chefen, och
- rapportera om datasäkerheten och problem i samband med den till datasäkerhets- och IT-chefen

Personerna som ansvarar för information och dokumenthantering har i uppgift att:

- verkställa informationssäkerheten i informationstjänsterna och dokumenthantering enligt god administrations- och datasäkerhetspraxis.

Systemförvaltarens uppgift är att:

- ansvara för personregister- och datasystemrapporterna samt möjliga användningsregler för datasystemets användning i samråd med IT-styrgruppen
- ansvara för skyddet av datasystemet och datamaterialet, användarrättigheter samt säkerhets- och skyddskopiering i samråd med datasäkerhetschefen,
- verkställa säkerhetsåtgärderna som hänför sig till ägarens datasystem och utveckla dem i samråd med datasäkerhetschefen,
- följa upp datasäkerheten i datasystemet och

- rapportera om datasäkerheten och problem i samband med den till datasäkerhets-och IT-chefen samt IT-styrgruppen.

Person med administrationsrättigheter har i uppgift att:

- upprätthålla personregister- och datasystemrapporterna och se till att de är tillgängliga för personerna i registret,
- administrera säkerhetsprocedurerna i datasystemet i samråd med datasäkerhetschefen,
- följa upp systemets funktion ur datasäkerhetens synvinkel i samråd med datasäkerhetschefen,
- förbereda sig på exceptionella händelser och de motåtgärder som dessa kräver och
- rapportera om händelser och störningar som utgör en säkerhetsrisk i samråd med datasäkerhets- och IT-chefen.

- administrera och övervaka datasäkerheten i de system som de ansvarar för enligt de allmänna anvisningarna för Arcadas datasäkerhet

Samtliga användares uppgift är att:

- känna till anvisningarna om informationssäkerheten och iaktta dem,
- delta i datasäkerhetsutbildning som är avsedd för användarna och
- rapportera om observerade problem, hot och beteende som bryter mot anvisningarna till datasäkerhets- och IT-chefen.

Konsulternas och serviceföretagens uppgift är att:

- iaktta god databehandlings- och datasäkerhetspraxis på Arcada,
- i sin verksamhet som anknyter till Arcada upprätthålla och övervaka att datasäkerheten följer statsförvaltningens allmänna anvisningar om datasäkerheten och övriga anvisningar och
- rapportera om datasäkerheten och faktorer som påverkar den till datasäkerhets- och IT-chefen.

Bilaga 2 Användningsregler

Syftet med användningsreglerna för IT-systemen är att trygga informationens konfidentialitet, integritet och användbarhet för alla användargrupper i högskolan samt erbjuda en pålitlig och trygg miljö för databehandlingen. Dessa och övriga regler har utarbetats för att hjälpa användare att känna till sitt ansvar, sina rättigheter och skyldigheter som anknyter till användningsrätten. Även en oavsiktlig försummelse av skyldigheterna kan innebära en risk för andra användares information, dess integritet, konfidentialitet och användbarhet.

Dessa regler tillämpas på alla IT-system som administreras av högskolan eller på annat sätt hör till högskolans ansvarsområde och på användningen av dessa IT-system, samt för användarnas del också på övriga tjänster som är tillgängliga eller för vilka högskolan har beviljat användningsrätt. Reglerna gäller också arbetsstationer som är i allmänt bruk vid högskolan och all utrustning som kopplats till högskolans datanät.

Alla datoranvändare vid högskolan bör iaktta dessa regler liksom också övriga regler och anvisningar som utfärdats för högskolans IT-system, god sed samt finländsk lagstiftning. Användning som bryter mot detta behandlas enligt bilagan praxis och sanktioner vid IT-förseelser.

Gällande version av Arcadas regler finns på Arcadas interna webbplats.

Principer för användningen

De centrala allmänna principerna för all användning och tolkningen av användningsreglerna är följande:

- Alla användare ges möjlighet till rimlig och saklig användning.
- Användningen får inte orsaka övriga användare eller organisationer eller datasystem i datanätet olägenhet eller skada.
- Sekretessen bör respekteras.
- Användningsrätten som beviljats av högskolan är personlig.
- Användaren ansvarar för all användning som sker under sitt användarnamn.

Högskolans IT-system är avsedda som arbetsredskap för uppgifter som anknyter till studier, forskning, undervisning eller förvaltning. Övrig användning förutsätter ett separat avtal.

Privat användning tillåts i ringa grad och endast till den del den inte stör övrig användning av systemet eller strider mot reglerna som getts för användningen. Privat material bör hållas klart avskilt från material som anknyter till arbetet, i syfte att garantera sekretessen.

Kommersiell användning i annat syfte än för högskolans räkning tillåts endast med specialtillstånd. Användning för politisk verksamhet (såsom valreklam) är förbjuden. Ett undantag är högskolans val samt den verksamhet som studentkåren, politiska studentorganisationer/underorganisationer som deltar i verksamheten och personalens fackföreningar eller dylika organisationer idkar.

Alla användare bör för sin del ansvara för åtgärder som anknyter till den allmänna datasäkerheten. Även om användaren själv inte innehar något material som behöver speciellt skydd kan det hända att övriga användare innehar dylikt material. Alla användare är för egen del ansvariga för datasystemens totala säkerhet. Upptäckta eller misstänkta brister och missbruk avseende datasäkerheten bör meddelas till datasäkerhetschefen.

Högskolan strävar efter att skydda alla användare mot sabotageprogram (malware), skräppost och försök till intrång i systemen eller enskilda arbetsstationer. Användarna bör också för egen del bidra till denna strävan enligt anvisningarna.

Användaren ansvarar själv för skyddet av sina datafiler och i sista hand för säkerhetskopieringen av dem. Högskolan säkerhetskopierar de centrala IT-systemen, men ansvarar inte för skador som orsakas av att datafiler eventuellt har förstörts.

Användarna har tystnadsplikt om systemens datainnehåll, användningssätt, säkerhetsnivå och egenskaper ifall datasystemens användningssyfte, bestämmelserna angående systemens användning eller lagstiftningen så kräver.

Till högskolans datanät får endast kopplas utrustning som godkänts och registrerats av nätets administratör. Givna anvisningar bör följas då utrustning kopplas till nätet. Sådana delar av nätet som reserverats för allmänt bruk eller anslutning av användarnas egen utrustning är särskilt märkta.

Användningsrätt och användarnamn

Användaren beviljas användningsrätt till angivna IT-system. Användningsrätten är baserad på användarens roll vid högskolan. Av speciella orsaker kan personer som inte tillhör högskolan beviljas användningsrätt.

En förutsättning för att användningsrätten skall aktiveras är att användaren förbinder sig att iaktta dessa regler samt övriga anvisningar och bestämmelser. Användaren bör på förhand bekanta sig med anvisningar och regler som gäller systemet.

Användningsrätten får inte överlåtas till tredje part. Om det finns orsak att misstänka att en utomstående har kommit i besittning av ett lösenord eller användarnamn bör lösenordet bytas genast eller så skall användningen av användarnamnet förhindras omedelbart. Lösenordet bör bytas med jämna mellanrum och det bör vara svårt att gissa sig till/knäcka samt bör iaktta Arcadas lösenordspolicy.

Användningsrättens giltighet

Användningsrätten upphör automatiskt

- då användaren inte längre har en roll i högskolan,
- då en tidsbunden användningsrätt upphör att gälla eller
- då användarens roll förändras, så att det inte längre finns någon grund för användningsrätten till systemet i fråga.

Dessförinnan bör användaren själv se till att på ett ändamålsenligt sätt överföra eller radera data som sparats under användarnamnet. Användarens datafiler och e-postlåda avlägsnas efter att användningsrätten upphört.

Bilaga 2.1 Praxis och sanktioner vid IT-förseelser

Med IT-förseelser avses sådan verksamhet eller användning av IT-system som strider mot finländsk lag eller andra regler och bestämmelser som gäller för användningen av högskolans IT-system.

I detta dokument beskrivs åtgärder, som vidtas mot en person, när en IT-förseelse har uppdagats eller det finns vägande skäl att misstänka att en sådan skett. Åtgärderna har delats upp i begränsningar av användarrättigheterna *under utredning* av förseelsen, samt i eventuella *sanktioner* som stipulerats för förseelsen.

Dokumentet berör i första hand högskolan examensstudenter och personal. Andra som också kan ha beviljats användarnamn till högskolans system är bl.a.

- forskare och anställda vid externa serviceföretag samt
- studerande vid fortbildningen och öppna högskolan
- utbytesstudenter och -lärare
- gästföreläsare.

På grund av att gruppen andra användare är så heterogen bedöms tillämpningen av praxis och sanktioner för dessa användare separat i varje enskilt fall.

Alla uppdagade IT-förseelser och av dessa förorsakade åtgärder skall rapporteras till högskolans rektor och datasäkerhetschef.

Begränsandet av användningsrättigheterna medan utredningsarbetet pågår

Användningsrättigheterna kan begränsas genom avstängning av användarens användarnamn, eller genom att på annat sätt förhindra användningen av något IT-system (t.ex. genom att avlägsna rätten till att ändra data).

Under utredningsarbetet

- inaktiveras i regel *studentens* användarnamn och personen kallas till ett samtal med datasäkerhetschefen eller IT-chefen.
- begränsas, om användaren hör till *personalen,* användarrättigheterna. Om det gäller ett störningstillstånd i datanätet, kan en begränsning också bestå i att arbetsstationen kopplas från datanätet.

Användarrättigheterna begränsas alltid då det finns skäl att misstänka att användaren gjort sig skyldig till en IT-förseelse, och det är möjligt att användningen försvårar utredningen av förseelsen eller om det är påkallat för att minimera skadorna.

Om begränsning av användarrätten besluter IT-styrgruppen, avdelningens chef eller någon annan person som fått detta till sin uppgift. Begränsningen verkställs av administratören. I brådskande fall

beslutar administratören om begränsning av användningsrätten för högst tre dagar, vilket omedelbart meddelas åt den som ansvarar för begränsningarna.

Sanktioner

I de lindrigaste fallen ges användaren en anmärkning för osakligt beteende.

Som en följd av en IT-förseelse är användaren ersättningsskyldig för både de resurser som missbrukats och de kostnader som förorsakats av utredningsarbetet kring missbruket.

Studerande

Sanktioner som riktas mot en *studerande* kan bestå av att användningsrättigheterna begränsas (användarnamnen inaktiveras), av högskolans interna administrativa åtgärder (skriftlig varning, avstängning för viss tid) och av brottsanmälan (vid handlingar som enligt lag är straffbara).

Om stängning av användarnamn besluter IT-chefen eller datasäkerhetschefen. En avstängning under utredningsarbetet räknas inte in i tiden för avstängningen av användarnamn.

Om skriftlig varning besluter högskolans rektor. Om avstängning från studierna för viss tid besluter högskole styrelsen. Användningsrättigheterna dras in för avstängningstiden. Begränsningen av användningsrättigheterna gäller dock minst för den tid som anges i den bilagda tabellen.

Personalen

Sanktioner som riktas mot *personal* kan bestå av arbets- och tjänstemannarättsliga åtgärder vidtagna av högskolan (skriftlig varning, uppsägning, hävning) och brottsanmälan (handlingar som enligt lag är straffbara). Varning utfärdas av rektor. Användningsrätten till enskilda system kan upphävas för en viss tid eller permanent efter att missbruk gett upphov till förtroendebrist.

Sanktionstabeller (bilaga 2.1.1)

I bifogade tabeller ges rekommendationer angående sanktioner för IT-förseelser för högskolans examensstudenter, personal och övriga användare. I tabellerna finns exempel på typiska förseelser i anknytning till användningen av IT-system. De är klassificerade enligt förseelsens allvarlighetsgrad. Sanktionerna påverkas därtill av handlingens avsiktlighetsgrad.

I tabellernas sanktionsrutor har översta raden reserverats för en eventuell brottsanmälan, på nästa rad finns de administrativa åtgärderna och på den understa de åtgärder som IT-avdelningen verkställer.

Om användaren är såväl anställd som student, tillämpas personalens tabell.

Begrepp

Olaglig behandling av material underlydande strafflagen

- *material underlydande strafflagen* är t.ex. rasistiskt material, dvs. material med hot, förtal eller smädelse av en nationell, raslig, etnisk eller religiös grupp eller med dessa jämställbar folkgrupp, och material med barnpornografi, könsumgänge med djur eller rått våld.
- Behandling är bl.a. innehav, redigering eller spridning av material.

Sådant material underlydande lagen om upphovsrätt är t.ex. musik, video, serier, filmer, spel, bilder, skriftligt material och programvara.

En servicefunktion är en extern tjänst, såsom

- e-postservice (smtp, imaps, …)
- filöverföringsservice (ftp, http, scp,...)
- resursdelningsservice, ”peer-to-peer” program (Kazaa, eDonkey, BitTorrent...)

Överlåtande av användarnamn är t.ex. att delge sitt lösenord åt en annan användare **eller att lämna en datorsession öppen** så att någon annan obevakat kan utnyttja användarnamnet.

Äventyrande av informationens konfidentialitet är t.ex.

- att överlåta information som är icke-offentliga åt en person, som inte har rätt till det (t.ex. överlåtande av en serverdators användardata)
- att försumma informationssäkerheten gällande information som är icke-offentliga (t.ex. bristfälliga skyddsåtgärder i systemet där information behandlas)
- sekretessbrott brott mot personuppgiftslagen

Försummelse av den personliga informationssäkerheten är t.ex. att lämna sitt lösenord synligt för andra eller hantera lösenordet på ett ovarsamt sätt

SANKTIONSSKALA, personal

Förseelse = förbiseende, bristande vaksamhet, förbiseende, misstag, fel (SAOL)

HANDLINGENS AVSIKTLIGHETSGRAD ▶		Ovetskap Okunnighet Vårdslöshet Misstag Oavsiktlighet	Nonchalans Grov vårdslöshet Likgiltighet Skrytsamhet Avsiktlighet Upprepning	Avsikt att begå brott (skadegörelse, olovlig användning , spionage, sekretessbrott, missbruk av ställning m.m.) Avsikt att dra nytta
▲ FÖRSEELSENS ALLVARLIGHETSGRAD				
Allvarlig förseelse (förseelse eller brott som är straffbart enligt lag), t.ex: * Knäckning, intrång * Olaglig behandling av material underlydande strafflagen (pornografi, våld, rasism, m.m.) * Olaglig spridning av material underlydande lagen om upphovsrätt * Avsiktlig obehörig portskanning * Avsiktlig spridning av virus * Överbelastningsattack (DoS-attack)		Brottsanmälan övervägs Anmärkning / Skriftlig varning	Brottsanmälan Skriftlig varning / Uppsägning / Upphävande av arbetsförhållande	Brottsanmälan Upphävande av arbetsförhållande
Förseelse (allvarligt missbruk eller äventyrande av säkerheten), t.ex: * Olovlig kopiering av program och spel * Installation av olovliga program * Knäckning-/olovligt innehav av administratörsverktyg * Olovligt uppsättande av servicefunktion * Överlåtande av användarnamn åt annan * Äventyrande av datas konfidentialitet		Anmärkning / Skriftlig varning	Skriftlig varning / Uppsägning / Upphävande av arbetsförhållande	Brottsanmälan Uppsägning / Upphävande av arbetsförhållande
Lindrig förseelse (missbruk), t.ex: * Försummelse av den personliga informationssäkerheten * Orsakande av förfång för systemet eller för andra användare * Försummelse av virusskyddet eller datasäkerhetsuppdateringar * Olovlig kommersiell eller politisk verksamhet * Brott mot regler för passerkontroll		Anmärkning	Anmärkning / Skriftlig varning	Brottsanmälan övervägs Skriftlig varning / Uppsägning / Upphävande av arbetsförhållande
▲ FÖRSEELSENS ALLVARLIGHETSGRAD				

Användningsrättigheterna till enskilda system upphävs för viss tid eller permanent efter att missbruk givit upphov till förtroendebrist
Utöver ovannämnda sanktioner kan skadeståndsersättning uppstå

SANKTIONSSKALA, examensstuderande

Förseelse = förbiseende, bristande vaksamhet, förbiseende, misstag, fel (SAOL)

HANDLINGENS AVSIKTLIGHETSGRAD ▶		Ovetskap Okunnighet Vårdslöshet Misstag Oavsiktlighet	Nonchalans Grov vårdslöshet Likgiltighet Skrytsamhet Avsiktlighet Upprepning	Avsikt att begå brott (skadegörelse, olovlig användning , spionage, sekretessbrott, missbruk av ställning m.m.) Avsikt att dra nytta
▲ FÖRSEELSENS ALLVARLIGHETSGRAD				
Allvarlig förseelse (förseelse eller brott som är straffbart enligt lag), t.ex: * Knäckning, intrång * Olaglig behandling av material underlydande strafflagen (pornografi, våld, rasism, m.m.) * Olaglig spridning av material underlydande lagen om upphovsrätt * Avsiktlig obehörig portskanning * Avsiktlig spridning av virus * Överbelastningsattack (DoS-attack)		Brottsanmälan övervägs Möjlig skriftlig varning Anmärkning / Begränsning av användningsrätten 1v - 3 mån	Brottsanmälan övervägs Avstängning från studierna för viss tid Begränsning av användningsrätten 3 - 6 mån	Brottsanmälan Avstängning från studierna för viss tid Begränsning av användningsrätten över 6 mån
Förseelse (allvarligt missbruk eller äventyrande av säkerheten), t.ex: * Olovlig kopiering av program och spel * Installation av olovliga program * Knäckning-/olovligt innehav av administratörsverktyg * Olovligt uppsättande av servicefunktion * Överlåtande av användarnamn åt annan * Äventyrande av datas konfidentialitet		 Anmärkning / Begränsning av användningsrätten 1v - 2mån	 Skriftlig varning Begränsning av användningsrätten 1 - 3 mån	Brottsanmälan övervägs Avstängning från studierna för viss tid Begränsning av användningsrätten 3 - 6 mån
Lindrig förseelse (missbruk), t.ex: * Försummelse av den personliga informationssäkerheten * Orsakande av förfång för systemet eller för andra användare * Försummelse av virusskyddet eller datasäkerhetsuppdateringar * Olovlig kommersiell eller politisk verksamhet * Brott mot regler för passerkontroll		 Anmärkning / Begränsning av användningsrätten 1v-1mån	 Begränsning av användningsrätten 1v-2mån	 Brottsanmälan övervägs Begränsning av användningsrätten 1 - 3 mån
▲ FÖRSEELSENS ALLVARLIGHETSGRAD				

Utöver ovannämnda sanktioner kan skadeståndsersättning uppstå

SANKTIONSSKALA, övriga

Förseelse = förbiseende, bristande vaksamhet, förbiseende, misstag, fel (SAOL)

HANDLINGENS AVSIKTLIGHETSGRAD ▶		Ovetskap Okunnighet Vårdslöshet Misstag Oavsiktlighet	Nonchalans Grov vårdslöshet Likgiltighet Skrytsamhet Avsiktlighet Upprepning	Avsikt att begå brott (skadegörelse, olovlig användning , spionage, sekretessbrott, missbruk av ställning m.m.) Avsikt att dra nytta
▲ **FÖRSEELSENS ALLVARLIGHETSGRAD**				
Allvarlig förseelse (förseelse eller brott som är straffbart enligt lag), t.ex: * Knäckning, intrång * Olaglig behandling av material underlydande strafflagen (pornografi, våld, rasism, m.m.) * Olaglig spridning av material underlydande lagen om upphovsrätt * Avsiktlig obehörig portskanning * Avsiktlig spridning av virus * Överbelastningsattack (DoS-attack)		Brottsanmälan övervägs Anmärkning / Begränsning av användningsrätten 1v-3mån (stud.) / Indragning av användningsrätten	Brottsanmälan Indragning av användningsrätten	Brottsanmälan Indragning av användningsrätten
Förseelse (allvarligt missbruk eller äventyrande av säkerheten), t.ex: * Olovlig kopiering av program och spel * Installation av olovliga program * Knäckning-/olovligt innehav av administratörsverktyg * Olovligt uppsättande av servicefunktion * Överlåtande av användarnamn åt annan * Äventyrande av datas konfidentialitet		 Anmärkning / Begränsning av användningsrätten 1v-2mån (stud.)	 Indragning av användningsrätten	Brottsanmälan Indragning av användningsrätten
Lindrig förseelse (missbruk), t.ex: * Försummelse av den personliga informationssäkerheten * Orsakande av förfång för systemet eller för andra användare * Försummelse av virusskyddet eller datasäkerhetsuppdateringar * Olovlig kommersiell eller politisk verksamhet * Brott mot regler för passerkontroll		 Anmärkning / Begränsning av användningsrätten 1v-1mån (stud.)	 Anmärkning / Begränsning av användningsrätten 1v-2mån (stud.) Indragning av användningsrätten	Brottsanmälan övervägs Indragning av användningsrätten
▲ **FÖRSEELSENS ALLVARLIGHETSGRAD**				

Användningsrättigheterna till enskilda system upphävs för viss tid eller permanent efter att missbruk givit upphov till förtroendebrist
Utöver ovannämnda sanktioner kan skadeståndsersättning uppstå

Riktlinjer för lösenord i Arcada

Arcadas IT-säkerhet är inte starkare än den svagaste länken i kedjan. Vanligen är den svagaste länken användaren. Det är av yttersta vikt att användare i Arcada använder starka lösenord, och byter dem tillräckligt ofta.

Innehåll

1 Ansvar

1.1 Användarens ansvar

1.1.1 Användaren ansvarar för lösenordets kvalitet

Användaren ansvarar för att ett lösenord är tillräckligt starkt och bär också konsekvenserna av dåliga lösenord.

1.1.2 Användaren bör byta sitt lösenord ofta

Varje lösenord har en livstid, även de starka. Användaren förbinder sig att byta sitt lösenord minst en gång per halvår.

1.1.3 Användaren bör hålla lösenordet hemligt

Användaren är den enda som känner till lösenordet. Användaren bör aldrig uppge sitt lösenord till annan part. Lösenordet bör endast användas på Arcadas säkra tjänster.

1.2 Arcadas ansvar

1.2.1 Arcada har rätt att övervaka att denna politik följs

Arcada kan, enligt eget omdöme, kontrollera att lösenorden som är i kraft är tillräckligt starka.

1.2.2 Arcada har skyldighet att stänga användarkonton där denna politik inte följts

För att trygga organisationens IT-säkerhet samt individernas rättsskydd har Arcada en skyldighet att trygga användarnas identitet. Om Arcada finner att ett användarkonto har ett svagt lösenord, har IT-avdelningen rätt att stänga kontot för att undvika datasäkerhetsincidenter.

1.2.4 Arcada har rätt att spara information om använda lösenord, så dessa inte återanvänds

Arcada har rätt att spara information om använda lösenord så att dessa inte kan återanvändas. Dessa lösenord skyddas för obehörig åtkomst och används aldrig till något annat ändamål.

1.2.5 Arcada har rätt att skrida till åtgärder om denna politik inte följs

- Åtgärderna Arcada kan ta finns beskrivna i Arcadas informationssäkerhetspolicy. Ett svagt lösenord tolkas som negligering av personlig IT-säkerhet.

- Arcada har rätt att stänga användarkonton, vars lösenord inte bytts inom en rimlig tidsperiod.

1.3 Fastställande och ändring av riktlinjer

Riktlinjerna tillämpas till den del annat inte bestämts i lag eller förordning.
Beslut om ändring i riktlinjerna görs av rektor på förslag av IT-styrgruppen.

Dessa riktlinjer har på förslag av IT-styrgruppen fastställts av Arcadas rektor

9.5.2011

_____
Henrik Wolff
Rektor