Högskolan i Halmstad
IT-RÅDET

PROTOKOLL
fört vid sammanträde 1/2011
2011-03-03

Tid	09.00 – 11.30
Plats	Insikten, B231
Närvarande ledamöter	Lasse Hagestam (Ordförande) Göran Ericson Kenan Ganic KG Hammarlund Ulrika Hällemarker Fredrik Thornberg
Övriga närvarande	Anna Frederiksen (Adj)
Lämnat förhinder	Henrik Barth Elenita Forsberg Johan Nööjd Inger M Johansson
Ej närvarande	Lina Lundgren

§	Ärende	Beslut eller åtgärd
		Ordföranden hälsade välkommen och förklarade mötet öppnat.
1	Fastställande av dagordning	Inga ärenden anmäldes till Övrigt.
2	Val av justeringsperson	Kenan Ganic utses att justera protokollet.
3	Föregående mötes protokoll	Protokollet lades till handlingarna.
4	Rapporter	
	a) ITAN	Man har haft ett möte, där det mest pratades om informationssäkerhetsdokumenten. Dessa synpunkter redovisas under den punkten.
	b) IT-avdelningen	Urkund ska ersätta Genuine text som plagiatverktyg. Urkund kommer att vara i drift från den 1/4, Genuine text slutar att fungera 30/4. CLU ansvarar för systemet, och alla lärare kommer att få information om detta inom kort. VPN är nu på gång, tekniskt sett är det färdigt. VPN är ett säkert sätt att koppla in sig i HHs nätverk över Internet, så att användaren uppfattar sig som sittandes i skolan. Beställningsrutiner och lite dokumentation återstår innan lansering. Installation kommer endast att ske till HH-ägda datorer, efter ansökan. VPN kommer inte att ersätta myfiles, mail och andra webbsystem. Hörsalsdatorer Tillägget av inloggning på datorerna verkar ha fungerat bra och sektionsexpeditionerna har lämnat ut några gästkonton. Mycket få reaktioner. IT-avdelningen kan nu direkt installera program i hörsalarna vid behov.

Studentutskrifter Avtalet går ut snart. När avtalet skrevs beräknades för större volymer än det blev, varför HH har förlorat ekonomiskt på systemet varje år sedan det infördes.
Troligtvis byts systemet under sommaren till ett system med färre skrivare (av ekonomiska skäl). I princip blir det en större svartvit skrivare per hus, med ett par svartvita och en färgskrivare i biblioteket. I det nya systemet kommer studenterna att kunna skriva ut via internet, dvs. från egna bärbara datorer. Bytet bör även lösa utskriftsproblemet som finns från datorer med Windows 7.

Windows 7 Stort jobb med att försöka ta reda på vilka applikationer som inte kommer att fungera under Windows 7, och vem som kan fatta beslut om hur de ska ersättas.

TimeEdit Ny verson är på gång, där planen är att ha en bra integration med Kursinfo, för att hämta t.ex. kursnamn. Integrationen leder också till att studentportalen bättre kan visa scheman. Utbildning i den nya versionen planeras till v 13, inför schemaläggning av höstterminen.

I övrigt arbetar avdelningen vidare med ärenden och projekt.

c) Studentportal

Håkan Fasth arbetar halvtid med pilottestet. De studenter som testat är nöjda, men schemakopplingen fungerar inte alltid. För de administrativa meddelanden är gränssnittet att lägga in dem dåligt, så den funktionen har inte testats i någon större omfattning. Tentaanmälan kommer att testas av en grupp studenter i mars. Planen är nu att Studentportalen ska tas i drift i april. Det är fortfarande vissa rutiner runt portalen som behöver ändras för att den ska fungera optimalt, t.ex. registrering på kurstillfällen för programkurser. Detta behövs även för att ge bra statistik och för den kommande lärplattformen.

Hantering av nya studenter. Mycket av rutiner kring introduktion av nya studenter fungerar dåligt, t.ex. behöver information och organisation i vart de ska vända sig med sina frågor slås fast?

Hittills har inget gjorts för att anpassa portalen

		till telefoner, eller för att skapa appar. Standardgränssnittet är förberett för detta; t.ex. blir flikarna klickbara , men lpw-tjänsterna och schemat fungerar dåligt.
	d) Ny lärplattform	Projektet är inne i en upphandlingsfas, där CLU, HHs upphandlare och IT-avdelningen gemensamt tar fram de underlag som krävs. Tidplanen är att förfrågningsunderlaget ska skickas ut i mars, och avtal skrivas i juni. I så fall bör det gå att komma in i systemet i början av höstterminen. Integration med Ladok (för att hämta kurser och studenter) etc krävs innan kurser kan hållas i plattformen. Senare under hösten bör det gå att börja hålla kurser där. Ett av kraven i upphandlingen är att plattformen ska gå att använda med en smartphone.
5	Inventering IT-system och IT-program inom HH	Listor över IT-system och datorprogram som förekommer på HH delades ut. En diskussion om varför och hur en minskning av programfloran ska göras följde. <u>IT-rådet beslöt</u> att uppmana IT-avdelningen att dels sammanställa en argumentlista för varför en uppstramning ska göras, och dels att gå igenom listorna för att identifiera vilka program som inte används (och planera för en ev avinstallation).
6	Informationssäkerhet	Synpunkterna från ITAN refererades. Informationssäkerhetsarbetet syftar till att varken personer eller verksamheter ska lida skada p.g.a. bristande informationssäkerhet. Några ändringar i dokumentet ”Beskrivning av steget Riskanalys inom informationssäkerhetsarbetet vid Högskolan i Halmstad” och ”Riktlinjer för hantering av allvarliga informationssäkerhetsincidenter” föreslogs. <u>IT-rådet beslöt</u> att efter revidering skicka dokumentförslagen till Högskolans chefer, systemägare och systemadministratörer. Dokumenten ska därefter slås fast av förvaltningschef eller rektor.
7	IT-avdelningens tjänstekatalog	IT-avdelningen har tagit fram ett förslag till tjänstekatalog. Man planerar att presentera den

för cheferna via möten där man i stora drag diskuterar vad de vill ha ut av IT-avdelningen.

Den färdiga tjänstekatalogen publiceras på Insidan, när den är överenskommen.

8 Flytt av nästa möte

Nästa möte flyttas från den 19 maj till den 3 maj kl. 13.00 - 15.30 i Faculty.

Vid protokollet:

Anna Frederiksen

Justeras:

Lasse Hagestam
Ordförande

Kenan Ganic
justerare

Beskrivning av steget Riskanalys inom informationssäkerhetsarbetet vid Högskolan i Halmstad

Detta dokument är en förkortning och anpassning av dokumentet Riskanalys, version 0.2, från informationssäkerhet.se.

Genomförandet av en riskanalys är en viktig grund för att kunna utforma ett väl anpassat skydd för verksamhetens informationssäkerhet. Omvänt, om man inte känner till vilka risker man har, så är det omöjligt att utforma ett säkert och kostnadseffektivt skydd.

Riskanalyser för informationssäkerhet kan göras i många olika situationer och på många olika nivåer – för verksamheten som helhet, för ett specifikt IT-system, för en serverhall, för en verksamhetsprocess, etc. I första skedet utgår arbetet vid Högskolan i Halmstad från olika IT-system, kompletterade med hantering av information i närliggande verksamhet.

Det primära resultatet av en riskanalys är en förteckning av risker, deras potentiella skadeverkning och tänkbara sätt att hantera riskerna. Utöver resultatet genererar själva arbetsprocessen ytterligare ett antal positiva bieffekter. Till exempel:

- Vi lär oss hantera risker.
- Vi får fram en realistisk bild av verkligheten.
- Vi blir medvetna om hoten.
- Vi gör en realistisk och trovärdig värdering av riskerna.
- Vi tar fram beslutsunderlag för att kunna fatta rätt beslut.

Riskanalysens innehåll

Steg 1: Välj och beskriv analysobjekt

Med utgångspunkt i listan på informationstillgångar från tidigare informationsklassificering väljs analysobjekten ut. Normalt görs riskanalysen på de tillgångar där klassificeringen resulterat i klassningen Allvarlig eller Betydande för något av kriterierna Konfidentialitet, Riktighet, Tillgänglighet eller Spårbarhet.

I Steg 1 kompletteras beskrivningen av de informationstillgångar som ska analyseras på ett sådant sätt att alla deltagare är överens om vad som ingår i analysen och vad som ligger utanför.

Resultat av arbetsuppgiften:

- Analysobjekt är valda och beskrivna.
- Avgränsningar är tydligt dokumenterade.
- Alla i gruppen är överens om vad som ska analyseras.

Steg 2: Identifiera hoten

I steg 2 tas hot fram som rör analysobjektet. Analysdeltagarna tar fram, diskuterar och dokumenterar hot de ser mot respektive analysobjekt.

- Vilka är hoten mot de valda informationstillgångarna?
- Vad kan inträffa?

Anna Frederiksen • anna.frederiksen@hh.se • Tel 035-16 73 73 •

Det är viktigt att försöka beskriva hoten så att alla förstår, exempelvis "en extern angripare hackar sig in i systemet x för att ta del av uppgifterna y". Många gånger försöker man sammanfatta flera hot till ett problemområde, exempelvis "hacker", men då är det svårt att verkligen förstå vad det är som är hotet. Det är även svårt att bedöma risken i kommande steg. Viktigt i detta steg är att alla förstår och är överens om innebörden i hoten.

Resultat av arbetsuppgiften:

- Tänkbara hot mot varje utvalt analysobjekt dokumenteras.
- Varje hot ska vara tydligt dokumenterat och satt i sitt sammanhang.

Steg 3: Sammanställa och gruppera hoten

Detta steg har till uppgift att ta bort dubbletter, gruppera hot, ta bort hot som bedöms ligga utanför avgränsningen och eventuellt förtydliga hoten. Vissa hot kan rikta sig mot flera informationstillgångar. Använd mallen för dokumentation av hot/scenario för att dokumentera hoten i detta skede.

Resultat av arbetsuppgiften:

- En hanterbar mängd hot som är numrerade och tydligt beskrivna.
- Hoten finns också nedskrivna och tillgängliga för deltagarna.

Steg 4: Riskbedömning – konsekvens och sannolikhet

I Steg 4 bedöms vilka konsekvenserna blir om hotet inträffar och vilken sannolikheten är för att detta ska ske.

Varje enskilt hot bedöms av gruppen och sätts in på sin plats i en konsekvens- och sannolikhetsmatris (se nedan). Med matrisens hjälp kan analysgruppen bedöma risken (konsekvens och sannolikhet) för ett hot.

Konsekvens					
	Katastrofal				
	Allvarlig				
	Måttlig				
	Försumbar				
		Mycket sällan	Sällan	Regelbundet	Ofta
		Sannolikhet			

Anna Frederiksen • anna.frederiksen@hh.se • Tel 035-16 73 73

Sannolikheten anger hur troligt det är att hotet kommer att inträffa:

- Mycket sällan – en gång på 100 år
- Sällan – en gång på 10 år
- Regelbundet – en gång på ett år
- Ofta – mer än en gång per år

Konsekvensen är ett mått på den skada ett hot skulle ha på verksamheten om det inträffade. Påverkan kan exempelvis vara direkt eller indirekt, ekonomisk eller medmänsklig. I modellen använder vi oss av nivåerna Försumbar, Måttlig, Allvarlig och Katastrofal:

- Försumbar – mycket små konsekvenser för enstaka personer, risk för smärre ekonomiska eller andra konsekvenser för Högskolan.
- Måttlig – negativa konsekvenser för enstaka personer, ekonomiska eller andra tillgångar för Högskolan
- Allvarlig – risk för skada på personer, risk för betydande ekonomiska eller andra konsekvenser för Högskolan.
- Katastrofal – verklig fara för personer, stora ekonomiska eller andra konsekvenser för Högskolan.

Definitionerna av konsekvens och sannolikhet är ett riktmärke och kan förändras. Eventuella förändringar ska dokumenteras och tas med i slutrapporten. Konsekvenserna dokumenteras med fördel i samma dokument som hoten. När sannolikheter och konsekvenser är bestämda kan varje hot placeras in i matrisen.

Resultat av arbetsuppgiften

- En överblick över vilka risker som finns,
- vilka konsekvenserna är om de inträffar, och
- hur sannolikt det är att de inträffar.

Detta visualiseras i en konsekvens- och sannolikhetsmatris.

Steg 5: Framtagning av åtgärdsförslag

I steg 5 går man igenom de identifierade riskerna och tar fram förslag på hur riskerna kan hanteras. För detta finns två alternativ – hantera riskerna senare, eller hantera riskerna direkt. Även om riskerna ska hanteras senare kan bra idéer på åtgärder dokumenteras redan nu. Risker med stor sannolikhet och konsekvens kanske inte kan vänta på grund av den påtagliga risken för verksamheten. De riskerna ska i så fall åtgärdas direkt.

Den framtagna matrisen visar vilka hot som är allvarligast – de med högst sannolikhet och konsekvens. Med den informationen som utgångspunkt är det dags att diskutera eventuella åtgärdsförslag och prioritetsordning. Detta steg ska leda till en rekommendation med förslag på åtgärder och förbättringar för att eliminera, reducera eller acceptera riskerna.

Diskutera också behovet av sekretess - riskanalysen är troligtvis känslig.

Resultat av arbetsuppgiften

- Förslag till åtgärder och rekommendationer som mottagaren kan ta ställning till.

Sammanställning och rapport

Resultatet ska sammanställas till en slutgiltig rapport. Förutom själva resultatet av analysen är det viktigt att all tänkbar information, alla avsteg som gjorts och eventuellt nya definitioner sammanställs och inkluderas i slutresultatet. I rapporten kan också annan viktig information inkluderas, till exempel

Anna Frederiksen • anna.frederiksen@hh.se • Tel 035-16 73 73

styrande dokument eller annan dokumentation som är av värde för resultatet. Det är viktigt att skriva en sammanfattning som på ett enkelt sätt beskriver de risker analysgruppen funnit. Att ta med matrisen är ett bra sätt att illustrera riskanalysens resultat. Sammanställningen bör även innehålla eventuella förslag till åtgärder och rekommendationer till den som ska fatta beslut.

Anna Frederiksen • anna.frederiksen@hh.se • Tel 035-16 73 73

Mall för dokumentation av hot/scenario för [informationstillgång]

Namn	[Ange namn på hot/scenario]
Beskrivning	[Beskriv vad som inträffar]

Konsekvenser

Konsekvensen är ett mått på den skada ett hot skulle ha på verksamheten om det inträffade. Påverkan kan exempelvis vara direkt eller indirekt, ekonomisk eller medmänsklig. Konsekvenser kan vara exempelvis verksamhetskonsekvenser, goodwillkonsekvenser och ekonomiska konsekvenser.

Beskriv konsekvenser av det inträffade:

Riskbedömning

Markera den bedömda risken i matrisen

Konsekvens					
	Katastrofal				
	Allvarlig				
	Måttlig				
	Försumbar				
		Mycket sällan (1gång/100 år)	Sällan (1gång/10 år)	Regelbundet (1gång/1 år)	Ofta (mer än 1gång/år)

Sannolikhet

Åtgärder

Nuvarande skydd

[beskriv nuvarande skydd]

Bedömning av nuvarande skydd

Bedömning	Nivå
Ja/Nej	Det nuvarande skyddet bedöms tillräckligt
Ja/Nej	Det nuvarande skyddet bedöms inte tillräckligt men kvarvarande risker accepteras av verksamheten
Ja/Nej	Det nuvarande skyddet bedöms inte tillräckligt, ytterligare åtgärder krävs

Ytterligare skydd

[ange behov av ytterligare skydd]

Mall för prioriterad handlingsplan

PRIORITET	ÅTGÄRD	ANSVARIG	DATUM	UTFÖRT
1				
2				
3				
4				
5				

Riktlinjer för hantering av allvarliga informationssäkerhetsincidenter

Nedanstående riktlinjer tydliggör rutiner som syftar till att motverka effekten av allvarliga informationssäkerhetsincidenter.

Med allvarlig informationssäkerhetsincident avses en händelse som kan ge katastrofal konsekvens på en informationstillgångs konfidentialitet, riktighet, tillgänglighet eller spårbarhet.

Informationssäkerhetsansvarig bör även informeras om mindre allvarliga informationssäkerhetsincidenter för att möjliggöra upptäckt och motverkande av upprepade, snarlika, incidenter. Denna information bör, om möjligt, innehålla svaren på frågorna i punkt 4 nedan.

Vid en allvarlig informationssäkerhetsincident ska följande snarast utföras:

1. Sätt stopp för händelsen och minimera skadan

Den som upptäcker incidenten ska omedelbart informera informationssäkerhetsansvarig om händelsen. Är incidenten IT-baserad ansvarar IT-chefen för att IT-personalen agerar skyndsamt för att i första hand stoppa incidenten, och i andra hand avhjälpa eller lindra effekterna av det inträffade. I annat fall ansvarar informationssäkerhetsansvarig för att avhjälpa och lindra effekterna av det inträffade.

2. Larma ansvariga om incidenten

Informationssäkerhetsansvarig ansvarar för att sprida korrekt, aktuell information och för att samordna nödvändiga åtgärder. När en allvarlig informationssäkerhetsincident sker ska rektor, förvaltningschef samt ev. berörd systemägare och systemadministratör (nedan kallas dessa samlat för nyckelgrupper) direkt informeras om detta.

3. Sprid information till alla berörda

Ovan nämnda nyckelgrupper ansvarar för att relevant information om incidenten skyndsamt sprids i den egna organisationen och till externa berörda.

4. Dokumentera vad som sker

Alla allvarliga informationssäkerhetsincidenter ska dokumenteras, för att man ska kunna analysera vad som hänt och förebygga att de upprepas. Informationssäkerhetsansvarig ansvarar för denna dokumentation som ska inkludera hur problemet upptäcktes och vidtagna åtgärder i kronologisk ordning. Följande frågor ska besvaras i rapporten: VAD, VAR, NÄR, VEM, HUR och VARFÖR.

5. Samla in konsekvensanalyser

Ovan nämnda nyckelgrupper ansvarar för att konsekvensanalyser, som beskriver vilka störningar som informationssäkerhetsincidenten orsakat, sammanställs vid berörda sektioner/avdelningar. Dessa sänds till informationssäkerhetsansvarig och förvaltningschef och används som underlag i arbetet med att följa upp och utreda det inträffade.

6. Förebygg att incidenten upprepas

För att undvika och hantera informationssäkerhetsincidenter är det viktigt med förebyggande åtgärder och att dra nytta av kunskapen från tidigare incidenter. Efter varje allvarlig informationssäkerhets-incident bör berörda dokument gås igenom och vid behov justeras av ansvariga.

Anna Frederiksen • anna.frederiksen@hh.se • Tel 035-16 73 73 •

7. Återrapportera till verksamheten och ledningen

När hela händelsen är dokumenterad från start till slut ska en analys göras över förloppet. Återrapportering ska göras i första hand till nyckelgrupperna. I återrapporteringen bör ett förslag ingå som specificerar nödvändiga åtgärder och om möjligt uppskattade kostnader för dessa. Information om rapporten görs tillgänglig för all personal via Insidan. Personuppgifter om vem som ev. har, medvetet eller omedvetet, orsakat incidenten, såväl som tekniska detaljer om vad som hänt och planerade tekniska åtgärder, ska spridas med stor försiktighet.

Anna Frederiksen • anna.frederiksen@hh.se • Tel 035-16 73 73

Incidentrapport för [informationstillgång]

Tidpunkt för incidenten:	När den inträffade
Tidpunkt för upptäckt:	När den upptäcktes (om den inte upptäcktes direkt)
Beskrivning av incident/orsak:	Beskriv incidentens innehåll, och om möjligt vad den beror på.
Konsekvens och påverkade tjänster pga incidenten:	Fyll i vad/vem som påverkas och hur.
Genomförda åtgärder:	Fyll i vad som testats eller planeras för att hitta orsaken till incidenten. Om incidenten beror på en IT-säkerhetsincident, fyll i hur den incidenten löstes.
Tidpunkt för lösning:	När incidenten är löst (om incidenten beror på en IT-säkerhetsincident)
Erfarenheter, nya åtgärder:	Erfarenheter och åtgärder som behöver göras på andra system, processer eller rutiner för att undvika snarlika incidenter i framtiden.

Anna Frederiksen • anna.frederiksen@hh.se • Tel 035-16 73 73

Hantering av behörighet i IT-system

Varje användare i ett IT-system ska ha personlig behörighet, anpassad efter sina arbetsuppgifter. Detta innebär att begränsningar kan ske, såväl avseende funktionalitet som avseende tillgång till information (uppgifterna i systemet).

Förändring av en användares behörighet (och även beställning av nya behörigheter) kan ske löpande, eller vid en anställnings början och slut.

Behörigheter ska vara dokumenterade så att det i efterhand går att undersöka vem som haft tillgång till vilka uppgifter vid en specifik tidpunkt. Respektive systemägare ansvarar för att detta sker.

Förändringar av behörigheter skall beställas skriftligen, helst på bifogad blankett, till systemadministratör antingen av verksamhetsansvarig eller av annan, känd, anställd som har delegerat ansvar inom området. För vissa system kan en anställd själv begära behörighet efter beslut av systemägaren (t.ex. webuser).

Behörigheter som gäller generellt för alla (eller en större grupp) anställda eller studenter behöver inte beställas separat (t.ex. tillgång till Helpdesk, konferensrumsbokningssystemet och HHs trådlösa nätverk).

För de IT-system där systemadministratören kan dela ut möjligheten att skapa eller ändra behörigheter till en gruppansvarig, ansvarar respektive gruppansvarig för att behörigheterna är dokumenterade.

Systemadministratör/systemägare ska minst en gång per år stämma av samtliga användare och deras tilldelade behörigheter i systemet.

I dokumentet Elektroniska identiteter vid Högskolan i Halmstad, dnr 2009-01135, beskrivs hur Högskolans datoridentiteter fördelas.

Anna Frederiksen • anna.frederiksen@hh.se • Tel 035-16 73 73

Blankett för beställning av behörighet

Avser IT-system:

Avser användare (namn och användarnamn/personnummer):

Ny behörighet ☐ Ändrad behörighet ☐

Önskad behörighet (såväl funktionalitet som omfång[1]):

Beställare:

Underskrift Datum
Namnförtydligande
Roll/titel

Registrerat Datum

Systemadministratörs signatur

1 Med omfång avses mängden uppgifter personen ska ha tillgång till, t.ex. avseende en viss sektion eller en viss informationstyp.

Anna Frederiksen • anna.frederiksen@hh.se • Tel 035-16 73 73