Högskolan i Halmstad
IT-RÅDET

PROTOKOLL
fört vid sammanträde 2/2011
2011-05-03

Tid	13.00 -
Plats	Faculty Club, styrelserummet
Närvarande ledamöter	Lasse Hagestam (Ordförande) Henrik Barth Göran Ericson Kenan Ganic KG Hammarlund Ulrika Hällemarker Lina Lundgren Johan Nööjd
Övriga närvarande	Anna Frederiksen (Adj)
Lämnat förhinder	Elenita Forsberg Inger M Johansson Fredrik Thornberg
Ej närvarande	

§	Ärende	Beslut eller åtgärd
		Ordföranden hälsade välkommen och förklarade mötet öppnat.
1	Fastställande av dagordning	Följande ärenden anmäldes till Övrigt: a. Policy för sociala medier b. Studentrepresentant c. Info om W3D3
2	Val av justeringsperson	Göran Ericson utses att justera protokollet.
3	Föregående mötes protokoll	Protokollet läggs till handlingarna
4	Rapporter a) ITAN	ITAN har haft ett möte där man fick lägesrapporter kring ny lärplattform, nytt diaresystem, förändringar i Primula och kort om nya krav på e-beställningar.
	b) IT-avdelningen	Informationen sammanfaller i stort med IT-avdelningens kommande nyhetsbrev. Därutöver kommer IT-avdelningen att undersöka framtida alternativ för hantering av studenternas e-postkonton (om HH ska fortsätta hantera det själva eller i stället använda Google eller Microsoft som leverantör framöver). En extern leverantör ger studenterna t.ex. större hemkatalog och andra samarbetsmöjligheter kring dokument och i projekt. Det är viktigt att också se till de juridiska aspekterna – t.ex. gäller naturligtvis personuppgiftslagen, men kan vi tvinga studenterna till att nyttja en specifik kommersiell aktör på samma sätt som vi tvingar dem att läsa sin e-post idag?

5	Informationssäkerhet	Dokumentation av behörigheter kan ske i ett IT-system, men det är viktigt att inte bara dokumentera vilken person som tillhör vilken användargrupp, utan även vilka behörigheter den aktuella gruppen har. Beslut: IT-rådet beslöt lämna dokumenten vidare till förvaltningschef/rektor för godkännande.
6	IT-system och IT-program inom HH	Diskussion uppkom kring första punkten under Förslag till beslut. ITAN hade föreslagit att samordningen skulle ske på sektionsnivå istället för på arbetsgruppsnivå. IT-rådet kom fram till att processen blir enklare om texten kvarstår. Samordningspunkten gäller program i datorsalar i första hand. Beslut: Dokumentet förtydligas i enlighet med diskussionens resultat. Därefter skickas förslaget på remiss till chefer/gruppledare i organisationen.
7	Höstens möten	Höstens möten blir tisdagarna 13/9 och 1/11. Båda gångerna kl. 13-15.30 i styrelserummet i Faculty.
8	Övriga frågor	
	a) Policy för sociala medier	Policyn ska kompletteras med praktiska råd och tips. Syftet med policyn är att stärka HHs varumärke genom att visa upp en likartad bild av HH i de olika sammanhangen på nätet. Att Informationsavdelningen dessutom vet t.ex. vilka bloggar som finns underlättar också vid sökning/länkning och marknadsföring. Beslut: Dokumentet förtydligas i enlighet med diskussionens resultat. Därefter skickas policyförslaget på remiss till chefer och de anställda som informationsavdelningen vet är aktiva inom sociala medier i tjänsten.
	b) Studentrepresentant	Två nya representanter är valda till IT-rådet. Det finns önskemål om att i studentportalen lägga in en länk eller på annat sätt visa vilka som är studentrepresentanter för de olika organen.
	c) Info om W3D3	W3D3 är det ärendehanteringssystem som HH använder för diarieföring och hantering av

myndighetsärenden. Leverantören kräver att vi byter till en nyare molntjänst (eller tar hem driften av systemet).

I samband med detta vill HH utveckla användningen av systemet, t.ex. genom att hantera ärenden (som tillgodoräknanden) i systemet och även använda det för möteshantering med kallelser och protokoll.

Det kommer att behövas många olika arbetsgrupper och referensgrupper för att skapa rutiner kring den utvecklade användningen av systemet.

Vid protokollet:

Anna Frederiksen

Justeras:

Lasse Hagestam
ordförande

Göran Ericson
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 •

Försök att beskriva hoten så detaljerat att alla förstår vad som menas, exempelvis "någon hackar sig in i systemet x med avsikt att ta del av uppgifterna y". Det är lätt att sammanfatta flera hot till ett problemområde, exempelvis "en hacker tar sig in i systemet", men utan att specificera vad den är ute efter är det svårt att gå vidare med riskbedömning kring och åtgärder mot ett hot. I detta steg är det är viktigt 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

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

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 till systemadministratör antingen av verksamhetsansvarig eller av annan, känd, anställd som har delegerat ansvar inom området. En blankett finns framtagen för detta ändamål, och kan användas för IT-system som inte har andra inarbetade rutiner för anskaffning och förändring av behörigheter. 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

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

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				

Förslag till förnyad programhantering

Inom HH används många olika IT-system och datorprogram. Så ska det också vara, eftersom vi är många anställda, och vi har många olika berättigade behov. Däremot finns det behov av att minska floran av program.

Anskaffning och installation av ett helt nytt program eller ny version av befintligt program tar arbetstid i anspråk, såväl administrativt som praktiskt. IT-avdelningen har väl utbyggda rutiner för hur installationer ska ske, och för de flesta program krävs betydligt mindre arbetstid för att installera ett program ”den andra gången”. För varje nytt program som installeras måste också ev. säkerhetsuppdateringar från leverantören hanteras.

Även om Högskolan som lärosäte ofta kan utnyttja stora rabatter vid programvaruköp är det dock inte ovanligt att rabatterna ökar ju fler licenser man köper av ett program.

Olika programvaror (eller olika versioner av samma program) kan kräva olika stödprogram som inte fungerar i samma dator. Detta kan leda till problem i t.ex. datorsalar där vissa program inte kan vara installerade samtidigt (eller där användningen av vart och ett av programmen blir onödigt komplicerad). När många program är installerade i samma dator kan det också leda till att datorn går väldigt långsamt.

Användningen av olika program som gör ”samma sak” ställer också krav på support och användarnas kunskaper i programmet. Detta påverkar naturligtvis även studenternas undervisningsmiljö. Det finns exempel när studenterna måste lära sig nya IT-verktyg flera gånger under ett utbildningsprogram enkom för att lösa sina uppgifter, istället för att fokusera på metodik och utbildningens innehåll. Det är också lättare att utforma mallar och HH-specifikt användarstöd i ett program eller att hitta en kollega som har löst en programspecifik uppgift man behöver hjälp med när fler använder samma version och programvara.

Vissa program kräver också ständiga uppdateringar på grund av säkerhetsproblem. T.ex. Acrobat, QuickTime, Java etc. I vissa fall finns ersättare som ger liknande funktionalitet utan att ständiga säkerhetsuppdateringar behöver göras, t.ex. QTLite som ersätter QuickTime. I dessa fall kan IT-avdelningen ställa krav på att ersättningsprogrammet används.

Att ett program är freeware (utan licenskostnad) innebär inte att hanteringen av detta är gratis. Ett sådant program kan, ur installationssynvinkel, vara dyrare än ett "köpeprogram", eftersom det oftast inte finns support på freeware medan köpeprogram har support.

Förslag till beslut: Att varje enhet (ämnesgrupp/labb etc) tillsammans med IT-avdelningen i god tid inför varje termin diskuterar och kommer överens om vilka programvaror som ska användas i labb och datorsalar. IT-avdelningen kan bistå med t.ex. information om HHs avtal och priser, innehåll i programpaket, och vilka program som används inom övriga delar av HH.

Anna Frederiksen • anna.frederiksen@hh.se • •

Att det normalt inte bör finnas installerat mer än två olika versioner av samma produkt inom HH vid samma tidpunkt. Detta kan dels innebära kostnadsökningar eftersom det kan kräva tätare uppdateringar av programversioner än vad som i många fall skett idag, dels att inte uppgraderingar ”per automatik” omedelbart görs när en ny version finns tillgänglig att köpa.

Att varje gång en ny version av en programvara installeras på en dator avinstalleras den äldre versionen.

Att otillåtna program, t.ex. poker-program, kan komma att avinstalleras.

Anna Frederiksen • anna.frederiksen@hh.se

IT-rådet 2/2011
Bilaga 3

Policy för Högskolan i Halmstads närvaro i sociala medier

Policyn gäller för Högskolans i Halmstads närvaro inom samtliga kanaler för sociala medier. Den är skapad för arbetet med att skapa dialog med Högskolans omvärld samt förmedla information till olika målgrupper med myndigheten Högskolan som avsändare. Policyn bygger på E-delegationens riktlinjer för sociala medier.

Inledning

Sociala medier är ett samlingsbegrepp för olika webbplatser och teknologier som används för att dela med sig av information och åsikter. Högskolans närvaro inom de sociala medierna ska effektivt stödja och väcka intresse för Högskolans olika verksamhetsområden. Närvaron ska sprida och belysa viktiga nyheter, händelser och områden inom Högskolan. Genom de sociala medierna, exempelvis bloggar, mikrobloggar, sociala nätverkswebbplatser, forum och artikelkommentarer, finns det möjlighet till social interaktion med olika målgrupper. För att denna kommunikation ska vara effektiv behöver Högskolan en gemensam policy för hur varumärket ska framställas och presenteras i sociala medier. Högskolan i Halmstad är en myndighet och måste uppträda som en sådan. Därför är det viktigt att ha en sammanhållen och tydlig profil för de sociala kanalerna. Det är viktigt att fundera noga på vad konsekvenserna kan bli av olika inlägg för att kunna förebygga negativ uppmärksamhet kring varumärket.

Mål

Målet är att ytterligare stärka Högskolans varumärke genom att interagera med olika målgrupper – att genom konversationsmarknadsföring berätta om Högskolans verksamhet och vad vi kan. Högskolan kan, genom att skapa närvaro inom olika sociala mediekanaler, agera varumärkesbyggande då Högskolans namn och logotyp visas för besökarna. Det ökar kännedomen om att vi finns och att vi finns närvarande på andra virtuella platser än webbplatsen, hh.se. Det är viktigt att inse att kanalerna kommer att skifta, men att det nya kommunikationssättet kommer att bestå. För att vara trovärdig ska Högskolan i Halmstads medverkan i sociala medier därför följa gällande grafiska profil.

Målgrupper

Eftersom sociala medier är nästan hundraprocentigt efterfrågestyrt kan inte målgrupperna definieras enkelt. Sociala medier handlar om relationer, att bygga upp diskussionsklimat och möjligheter för att möta varje individ i målgruppen. I dagsläget använder Högskolan två typer av kanaler, den direktkonverserande som marknadsför sig till sin målgrupp och den som fungerar som startpunkt för att skapa en viral process för att påverka sina bekanta genom egna nätverk. Högskolan, som myndighet, kan inte längre välja om och när man vill stå i centrum. Användarna styr kommunikationen.

Ansvar

Det ska tydligt framgå att Högskolan i Halmstad är avsändaren och därigenom har ett ansvar för all information, såväl text, bild som ljud, som sprids via sociala mediekanaler. Rektor är ansvarig utgivare för Högskolans medverkan i olika sociala medier. Informationschefen är ansvarig för att verkställa Högskolan i Halmstads medverkan i sociala medier. Spridning av information från dessa kanaler ska alltid följa gällande lagar och förordningar som exempelvis E-delegationens Riktlinjer för sociala medier, SUNET:s etiska regler och policyer, nätetikett samt regelverk från Högskolan i Halmstad.

Rutiner för konto

Informationsavdelningen är ansvarig för att skapa officiella konton inom sociala medier. Dessa kanaler ska innehålla Högskolans logotyp och framföra lärosätets åsikter i egenskap av myndighet. Önskar enskilda sektioner, avdelningar eller enheter ett konto ska det beställas via helpdesk och ”SiteVision/webbfrågor”. Dessa kanaler ska skapas efter principen ”tillhörighet_hogskolan”, ”tillhörighet_hogskolanihalmstad” eller ”hogskolanihalmstad.blogg.se/namn/” beroende på vilken kanal som avses. Exempel: bibliotek_hogskolan eller forskning_hogskolanihalmstad. När det gäller dessa kanaler är det viktigt att de som medverkar i sociala medier uttrycker åsikter som ligger inom ramen för deras ansvarsområde. Enskilda medarbetare, i sin roll som lärare, forskare eller teknisk administrativ personal har givetvis rätt att uttrycka sig i sociala medier, men då i rollen som privatpersoner och under rådande yttrandefrihet.

Rutiner för bevakning

Högskolans olika sociala mediekanaler kräver både underhåll och resurser. Eftersom det finns ett antal funktioner inom kanalerna, bland annat diskussionsforum, krävs en hög grad av delaktighet och moderering. Det är av yttersta vikt att Högskolan bevakar sina sociala mediekanaler för en stringent kommunikation kring Högskolan i Halmstads varumärke. Det är viktigt att våga bemöta och uppskatta både missnöjda och nöjda användare. Ansvarig för bevakningen av kanalen ligger hos respektive avdelnings- eller sektionschef. Kontroll av att ansvaret efterlevs utförs av informationsavdelningen som också kan besluta om kanalen bör stängas till följd av bristfällig bevakning eller missbruk.

Rutiner för hantering av ärenden och personuppgifter

Sociala medier är en bra kanal för att kommunicera med allmänheten i allmänna frågor. Kommunikationen bör sträva efter att vara allmän och informerande, därför ska Högskolan i Halmstad inte hantera enskilda ärenden, särskilt om de innehåller uppgifter om personliga eller ekonomiska förhållanden i sociala medier utan hänvisa till andra kommunikationskanaler.

Rutiner för arkivering

Högskolan i Halmstads medverkan i sociala medier ska arkiveras enligt gällande arkivlagstiftning och Högskolan i Halmstads lokala regler avseende arkivering. Likaså ska skärmdumpar av mediet tas två gånger per år och vid större förändringar av mediet. Informationsavdelningen ansvarar för att dessa skärmdumpar tas. Vid avveckling av mediet ska så mycket som möjligt av materialet bevaras genom skärmdumpar. Inlägg, kommentarer eller övrig aktivitet i Högskolans sociala medier som föranleder start eller del i ärende ska diarieföras.

Brytande mot policy

Rektor eller av rektor utsedd person får omgående kontakta enskild medarbetare som skapat ett konto som använder Högskolans logotyp. Respektive chef ansvarar för att policyn efterföljs.

Om webbkoordinator upptäcker eller får rapport om agerande som strider mot policyn ska i första hand den som äger kontot kontaktas. I andra hand ska chef kontaktas. Om ägaren till kontot vägrar ändra eller radera aktuell information eller inte kan nås inom rimlig tid har chef rätt att anmäla ärendet till rektor. Uppnås inte samförstånd ska ärendet anmälas till rektor.

Om chef är tveksam i sin bedömning kan ärendet tas upp med förvaltningschef eller informationschef för diskussion. Om innehållsansvarig är missnöjd med chefens beslut kan denne vända sig till rektor för att få saken prövad.

Informera

Informera i det sociala mediet om följande:

- Att det är Högskolan i Halmstad som ansvarar för kontot i det sociala mediet.
- Vad syftet är och vad Högskolan i Halmstad avser med användningen av mediet.
- I vilken utsträckning inlägg blir tillgängliga för andra användare.
- Att inlägg blir allmänna handlingar.
- Vilka uppgifter som inte får publiceras.
- Vad Högskolan i Halmstad gör om användaren inte följer rekommendationerna (blockera, ta bort etc.).

Om Högskolan i Halmstad använder cookies ska dessutom följande information lämnas:

- Att webbplatsen innehåller cookies.
- Varför cookies används.
- Hur användaren kan hindra cookies.

Mer information

Kommunikationsrummet på Insidan, Högskolan i Halmstads intranät (länk)
E-delegationen Riktlinjer för sociala medier (länk)
Datainspektionen Personuppgiftslagen (länk)
Offentlighetsprincipen på Wikipedia (länk)