Doumenttyp	Rapport Slutrapport Säkerhetssöversyn	Datum	2007-11-30
Document ID	Mittuniversitetet Fas 2 - 4	Område	
Utarbetad av	Robert Hagelin / 063-157244	Version	RevA
Godkänns av/signatur	Anders Nordlander/ 060-149523		

Slutrapport
Projekt Säkerhetsöversyn av Mittuniversitetet Fas 2 - 4

Sammanfattning

Säkerhet är i allra högst grad en arbetsmiljöfråga. Personal och studenter skall kunna känna sig trygga på sin arbetsplats. Men säkerhetsnivån får inte bli så hög att det skapar problem för personal och studenter att utföra sitt arbete. Endast i ett krisläge av någon form får säkerheten sätta gränser för tjänsteutövning. Det är vår uppfattning och med det i minnet har vi försökt kartlägga verksamhetens behov och hitta de risker som upplevs hos personal och studenter vid Mittuniversitetet idag för att kunna formulera de krav som vi i framtiden vill ställa på ett säkerhetssystem.

Innehåll

Bilagor

nr	Titel	sidor
1	Informationssäkerhetspolicy Mittuniversitetet 2006-2008	6
2	Identifierade risker vid intervjuer	2
3	Frågemall vid Intervju med verksamhetsrepresentanter	4
4	Minnesanteckningar från ECCA möte 2007-10-18 --19	4
5	Krav och kostnader	2

1 Inledning

Säkerhetstjänsten vid Mittuniversitetet verkar idag inom ett stort område. Brandskydd, hot mot personal/studenter, skydd mot tillgrepp av vår materiel/information, sabotage och spioneri är exempel på arbetsområden för säkerhetsarbetet. För att begränsa att dessa hot realiseras krävs policys och regelverk men också rutiner och kunskap hos såväl personal/studenter som den personal som arbetar aktiv med frågorna.

Mittuniversitetet har idag ett tekniskt säkerhetssystem som börjar närma sig sin slutstation avseende teknisk funktionalitet och anpassning till verksamhetens förändrade behov. Systemet började installeras under slutet av 90-talet och bygger på den IT-teknologi som då var gångbar. Systemet börjar dessutom uppvisa mer och mer behov av underhåll med tanke på sin ålder vilket ökar den årliga driftkostnaden såväl i ekonomiska medel som i personella resurser. Många funktioner är ålderdomliga sett till moderna systems möjligheter vilket medför att säkerhetsanpassningar till verksamhetens krav och behov inte alltid kan efterlevas eller att anpassningarna kommer för sen och blir orimligt kostsamma. Dagens tekniska säkerhetssystem möjliggör ej en uppgradering eftersom det är konstruerat på ett sätt att i stort sett måste alla komponenter ersättas för att en uppgradering skall kunna ske.

Ett nytt säkerhetssystem kräver en ordentlig analys av Mittuniversitetet behov. Systemet kommer att kunna tillgodose olika behov som verksamheten kräver. Det är dock viktigt att kunna införa ett flexibelt system och som kan möta framtidens krav. Befintliga policys och riktlinjer finns inom många av de områden som nämndes inledningsvis. Nya krav på säkerheten kräver att dessa policys, riktlinjer och handlingsplaner ses över och anpassas till rådande förutsättningar och krav.

Säkerhetsarbetet är en viktig del av Mittuniversitetets trygga arbetsmiljö varför dessa frågor i högsta grad är en del av verksamhetens arbetsmiljöansvar och är en fråga för alla såväl anställda som studenter.

2 Projektmodell

2.1 ANALYSPROJEKTET

Projektet är en fortsättning på förstudieprojektet som avslutades före sommaren. Arbetet startade med en detaljplanering av det fortsatta arbetets olika steg. Det innefattar metoder som skall användas, vilka personer som bör fungera som informationskällor för projektet och i detta fall ett intervjuunderlag då intervju på arbetsplats valdes som informationsinhämtningsmetod. Detta för att skapa en trygghet för den intervjuade och för att få en möjlighet att se den arbetsmiljö som vi talar om i intervjun. I de flesta fall har frågemallen (bilaga 3) har använts som utgångspunkt för intervjun som kompletterats med diskussion kring huvudområdet och specifika krav för den egna verksamheten. I de fall mallen inte använts har det handlat om specifika frågor från projektet. Det handlar om intervju angående möjligheten att sända larm från säkerhetssystemet till Nilex och vad som behövs för att få det att fungera och säkerhetsproblem och krav i Mittuniversitetets datasalar; samt en diskussion ang. Mittuniversitetets lokalstrategi .

2.2 GENOMFÖRANDE

Arbetet har utförts av Robert Hagelin genom intervjuer med representanter som pekats ut av Bo Ekwärn. Personerna har intervjuats en och en. Intervju med enskild person valdes som arbetssätt istället för Workshops då det tidigt framkom att det var omöjligt att samla de som skulle delta på en plats under en dag.
Intervjuer har skett i tre steg, först i Östersund sedan i Sundsvall och sist Härnösand, vilket har inneburit många resor framför allt mellan Sundsvall och Östersund. Målet var att hitta representativa personer som belyser verksamhetens säkerhetsbehov.
Ganska snabbt kunde fyra huvud grupper av arbetsuppgifter identifieras:

- Normalverksamhet som inte har några specifika säkerhetsbehov utöver det normala.
- Verksamhet som möter många studenter i vardagen t ex bibliotekspersonal, receptionister, studievägledare och institutionssekreterare som i en servicefunktion får möta frustrerade personer med olika problem. Detta har i enstaka fall lett till hot från person mot personalen. Viss del av studentkårens arbete är även det utsatt ur samma säkerhetssynpunkt.
- Verksamhetsområden som kräver en högre nivå av säkerhet pga hantering av sekretessbelagd information. Detta sker ofta i forskningssammanhang eller på institutions expeditionen.
- Vid de institutioner som hanterar känsliga ämnen och miljöer krävs en högre nivå av tillträdeskontroll som skall hanteras.

Nästa steg är att ta fram det sammanställda resultat som finns beskrivet nedan under punkten 3 och att analysera intervjusvaren samt värdera risker och hot. Sammanställningen av risker som framkommit vid intervjuer finns i "Identifierade risker" (bilaga 2). Detta kopplas sedan till de erfarenheter Bo Ekwärn har samlat vid möten med säkerhetsföreträdare vid andra universitet och vi söker lösningar som går att återanvända i vårt arbete med Mittuniversitetets framtida säkerhetslösning. Dock kan det vara svårt att ta någon annan myndighets lösning och implementera den direkt hos Mittuniversitetet då förutsättningarna oftast skiljer sig åt, men goda idéer kan tas tillvara när en plan för utveckling av säkerheten vid Mittuniversitetet skapas.

Slutligen dokumenteras resultaten och sammanställs i denna rapport och även kompletteras med en kravlista med skall- och eventuella börkrav som kan användas av Mittuniversitetet i nästa steg vid skapandet av en Offertförfrågan till leverantörer av en ny säkerhetslösning

2.3 ÖVRIGA MÖTEN

Två samlade möten har genomförts med andra än de deltagare som är beskrivna under punkten 2.4.

2.3.1 IT-avdelningen i Östersund (20070917)

Möte med delar av IT-avdelning där projektets avgränsningar beskrevs. Resultatet av mötet visade att det föreligger ett stort behov av en genomgång av IT-avdelningens styrdokument. Det styrdokument som finns idag är en framtagen IT-policy som inte är heltäckande eller styrande på alla nivåer.(bilaga 1)
Detta kommer inte att hanteras i det pågående projektet, men rekommendationen är att ett arbete startas omgående för att hantera problematiken.

2.3.2 Internt Säkerhetsmöte i Sundsvall (20071008)

Möte med alla intendenter vid Mittuniversitetet, säkerhetschefen och representanter från G4S, SOS och larminstallatör i Sundsvall. Upplevda nulägesproblem diskuteras och vilka möjligheter till förbättring som finns. SOS och G4S kan erbjuda ett antal tjänster som kan vara aktuella för Mittuniversitetet som hantering av larm, ärendehantering och vidareförmedling. Utvecklingen har också gjort att även IP-kommunikation skall kunna hanteras nu.

2.4 DELTAGARE

Följande personer har aktivt arbetat med projektet:

Bo Ekwärn	Projektledare
Robert Hagelin	Projektdeltagare

Följande personer har bidragit till resultatet i utvärderingen genom intervjuer:

Susanna Öhman	Prefekt SHV
Maria Nyberg Ståhl	Akademisk sekreterare
John Wold	Bibliotekschef Östersund
Torbjörn Engh	Säkerhetssamordnare
Per-Erik Östhling	Intendent Östersund
Lena Andersson	Receptionen i Östersund
Bert Persson	IT-avd Ansvarig för datasalar
Per-Ove Forss	ITM
Bengt Jonsson	Studentkåren Östersund
Annika Spånning	Institutionssekreterare
Maria Torstensson	Prefekt NAT
Mikael Marklund	Lektor TFM Designutbildningen
Håkan Norberg	Adjunkt NAT Kemist (skyddsombud)
Viktoria Engman	Bibliotekarie (skyddsombud)
Åsa Granberg	Studentkåren Sundsvall
Jenny Bergfors	IT-avd Ansvarig för ärendehantering
Lena Jadekrans	EKO
Hans Beijar	Intendent Härnösand
Per Olof Björner	Lokalansvarig Mittuniversitetet

3 Resultat av intervjuer

Nedan beskrivs resultatet som framkommit i arbetet med informationsinhämtning i projektet.

3.1 VERKSAMHET

Varje intervjuperson beskriver den verksamhet som bedrivs på respektive enhet. Av praktiska själ har verksamheten grovt delats upp i fyra områden:

- Ledning
- Utbildning
- Forskning
- Service

Alla tillfrågade har en uppfattning om Mittuniversitetets visioner och mål och hur dessa styr och påverkar den egna verksamheten.

3.2 TILLGÅNGAR

Alla tillfrågade ser personal som en stor tillgång och har svårt att enkelt ersätta personal vid längre tids frånvaro. För vissa institutioner är lokaler viktiga tillgångar, ex då undervisningen kräver speciella förutsättningar eller då stora ytor behövs för verksamheten.
Samtliga är beroende av ett väl fungerande IT-stöd och det är främst e-post, webb med intranät, LADOK och för vissa även ATLAS. Vidare finns ett antal andra system och applikationer som är verksamhetskritiska för vissa institutioner och funktioner. I många fall behöver rutiner ses över för att erhålla säker hantering av dokument. Endast en Institution har en handlingsplan för krishantering med reservrutiner.

3.3 HOT

Det finns en viss oro i verksamheten för effekterna av ett vikande studentunderlag och många ser det som det primära hotet. Därför är det viktigt att det säkerhetsarbete som bedrivs och kommer att bedrivas i framtiden inte uppfattas som en belastning, utan tvärt om ger en trygg arbetsmiljö för både studenter och anställda.

För bibliotekspersonal, vaktmästeri, receptionist och institutions-sekreterare är det största hotet direkt person hot. De är utsatta i och med att de utgör ansiktet utåt mot studenter. Här finns behov av en larmknapp så att hjälp kan tillkallas snabbt. Larmknappen kan exempelvis tillkalla kollegor eller väktare beroende tid på dygnet
För biblioteken är brand och vattenskador stora hot som skulle skada verksamheten mycket och göra det omöjligt att fortsätta. Här finns

dock möjlighet att hänvisa studenter till övriga campusorter om hotet blev verklighet.

Stölder beskrivs även det som ett hot, både mot enskilda och mot hela verksamheter. Det faktum att all kontor är låsta, men att alla har samma nyckel bedöms som ett stort problem i sammanhanget. Det räcker med att en nyckel kommer på avvägar så har förövaren tillträde till samtliga kontor. I forskningshänseende där känsligt materiel hanteras bör möjlighet ges att effektivt säkerställa säkerhet. Det kan vara så att en unik låscylinder monteras till kontoret eller att ett säkerhetsskåp installeras på kontoret vid behov.

Alla bedömer IT-stödet som väsentligt och även det utgör ett hot mot samtliga. Kortare avbrott går att hantera, men man har oftast ingen uthållighet över tiden med framtagna reservrutiner. En tillfrågad institution har utarbetade reservrutiner för att kunna fortsätta verksamheten om katastrofen skulle inträffa.

3.4 INFORMATION

Information sprids oftast via e-post, muntligen eller vid interna möten inom enheten och utanför enheten används oftast Mittuniversitetet intranät och portal. Man är beroende av att IT-stödsystemen fungerar. Säkerhet bör ha en egen, självklar plats i portalen som är lätt att hitta och som är uppdaterad med aktuell information om den normala säkerhetsnivån inom mittuniversitet och snabbt uppdateras om den skulle förändras tillföljd av någon oväntad händelse. I vissa fall används externa leverantörer av hosting för hemsidor vilket kan innebära en säkerhetsrisk för hela Mittuniversitetets webb.

3.5 INFORMATIONSSÄKERHET

Hanteringen av information som inte klassas som öppen enligt offentlighetsprincipen kan inte skötas på ett tillfredsställande sätt. Då samtliga kontorsnycklar fungerar i alla kontorsdörrar på institutionerna finns möjlighet till informationsläckage d v s att obehöriga kan få tillgång till informationen. Det kan räcka med att en nyckel kommer på avvägar och hamnar i händerna på fel person. Därför bör säkerhetsskåp installeras för den personal som behöver hantera det material som kan klassas som hemligt eller internt, exempelvis oskrivna tentor, forskningsresultat, modeller och prototyper. All dokumentation skall klassas enligt en informationsklassningspolicy som skall tas fram för att höja informationssäkerhetsnivån. Policyn bör tas fram i samråd med arkivarie vid Mittuniversitetet för att en gemensam syn på informations-klassning skall erhållas.

Vid informationsmöte med delar av IT-avdelningen beskrevs det arbete som skulle genomförs inom projektet. Det framkom att uppenbara brister finns inom informationssäkerhets området. Avsaknaden av

fastställda policys, riktlinjer och rutiner för IT-avdelningens arbete gör att informationssäkerhet inte kan erhållas.
Det föreligger ett stort behov av fortsatt studie av detta område.

3.6 UTBILDNING

Samtliga har behov av utbildning i olika former. Förmedlad utbildning i seminarieform bör kompletteras med andra former av utbildning. I portalen bör generell och specifik information om Mittuniversitets säkerhetsregler finnas. Vidare bör man kunna hitta hur olika larmsignaler låter i olika byggnader och hur man skall agera i olika situationer. För dom som inte har möjlighet att närvara vid ett seminarietillfälle, kan videoupptagningar från seminariet läggas ut på intranätet och på så sätt erbjuda en möjlighet att personal, gäster och studenter kan tillgodogöra sig utbildningen i efterhand, samt även gå tillbaka till seminariet för att komma ihåg vad som sades. Lättillgänglig information gör det möjligt att sprida kunskap och medvetenhet på ett bättre sätt i den form som tilltalar varje enskild individ.

Interaktiv utbildning med efterföljande kontrollfrågor ger kvitto på att personal och studenter tagit del av och förstått den utbildning som förmedlats. Möjligheten till kontrollfrågor är även ett bra sätt att se att kontrollera att personal, gäster och studenter har tagit del av de krav som finns och måste följas på Mittuniversitetets verksamhetsområde.

Övning är också en viktig del i utbildningen när det handlar om säkerhet. Det är en sak att veta hur ett brandlarm låter och hur man skall agera när larmet ringer, men en annan sak att göra det när korridoren är rökfylld och all belysning har slocknat. Därför är det viktigt med övningar och i de fall det är möjligt realistiska sådana. Därför ar det viktigt att tid läggs på att planera och genomföra övningar med regelbundenhet och efteråt kommunicera resultatet av övningen. Därefter kan planer revideras och uppdateras.

3.7 TRYGGHET

Alla tillfrågade känner en grundtrygghet på sin arbetsplats. Dock känns det i vissa fall olustigt att under vara kvar på jobbet efter 17.00 den mörka årstiden. Oro finns för att personer dröjer kvar i lokaler efter låsning. Genom införande av en "Mittuniversitetslegitimation" för anställda, gäster och studenter finns möjligheten att göra en kontroll av lokaler efter låsning och avvisa de som inte kan styrka sin rätt att vistas i Mittuniversitetets lokaler.

3.8 HÄNDELSEHANTERING

Idag rapporteras händelser direkt till säkerhetschefen eller intendenter via e-post eller telefon. Detta förfarande ökar risken för informations- och ärende förluster och att uppföljningen inte kan kvalitetssäkras. Förslaget är att alla ärenden rapporteras in i Nilex, det ärende-hanteringsverktyg som Mittuniversitetet redan använder för IT-stöds ärenden. Det gör att ärenden inte kan falla mellan stolarna och att fler rapport vägar finns med telefon till helpdesk, webanmälan och e-post till helpdesk. Detta ger även en möjlighet för anmälaren att följa hanteringen av egna anmälda ärendet. Det kommer även att förändra viljan att rapportera även de händelser som inte direkt är incidenter, exempelvis en olycka eller stöld, utan även upplevda avvikelser t ex då man är osäker på om den person man sett i korridoren på institutionen verkligen är behörig att vara där, men inte vågat fråga. Om fler ärenden rapporteras med samma innehåll ger en Statistik som kan visa på trender och ett proaktivt arbete blir möjligt.

3.9 KRISHANTERING

Hantering av stora krissituationer har nyligen övats. I och med tak-incidenten på campus i Östersund prövades de krisplaner som finns. Situationen hanterades på ett bra sätt och har fått god kritik från alla inblandade och utomstående observatörer. Dock hittades ett antal brister eller saker som kunde hanterats annorlunda. Den plan som finns idag är inte heltäckande, utan behöver utvecklas och övas så att inga tveksamheter råder om något liknande skulle inträffa igen. Dagens plan är personberoende och måste göras rollbaserad så att den kan utföras även om en person saknas.
Det är lätt att se behovet av planer när stora kriser avhandlas, men det är även mycket viktigt att planen är användbar aven vid små kriser. Ett kontorsinbrott kan leda till en personlig kris hos den som blivit utsatt och detta får inte glömmas bort. Möjlighet till hjälp att hantera situationer och känslor måste kunna hanteras.

3.10 STUDENTLEGITIMATION FÖR MITTUNIVERSITETET

Frågan om "en student – ett kort" diskuterades med samtliga och alla ser de positiva effekter en legitimation för samtliga på Mittuniversitetet ger. Kortet kommer att bli mer personligt än dagens kort och gemene man kommer att förändra sitt beteende vid hantering av sitt passerkort. Införandet av en Mittuniversitetslegitimation ger även möjlighet att avvisa personer som inte är behöriga att vistas i de lokaler som har begränsat tillträde för personal, gäster och studenter vid Mittuniversitetet. Ett "smart kort" ger även möjligheten att utföra andra funktioner, ex hantera kopiering och utskrifter, fungera som lånekort vid Mittuniversitetets bibliotek. Om man väljer att hantera utsrifter via kortet minskar belastningen på receptionens personal och dom slipper

även att hantera kontanter, som i sig kan leda till ökade risker. En ny kortstandard och ett nytt system för korthantering kommer även att underlätta utlämningen av kort vid terminsstart. För att ta hänsyn till framtida studentutbyte mellan universitet och andra länder så är rekommendationen att anamma den kortstandard som beskrivas av European Campus Card Association (ECCA). Sören Sollén, Torbjörn Engh och Anders Lundgren från Mittuniversitetet har deltagit i en konferens i frågorna omkring kort anordnad av ECCA:s svenska underorganisation i Göteborg 18-19 oktober 2007.
Minnes anteckningar från mötet finns bifogat till rapporten i bilaga 4.

Vidare behöver rutiner ses över vid avslut, både när studenter avslutar utbildning och när anställda slutar sitt uppdrag vid Mittuniversitet. Ett nytt, personligt kort är en av grundstenarna för att stärka säkerheten på Mittuniversitetet samtliga utbildningsorter.

3.11 FRAMTIDSKONTROLL

Efter intervju med Maria Nyberg-Ståhl konstateras att ingen större utveckling av kärnverksamheten är planerad hos Mittuniversitet som påverkar säkerhetsutvecklingen negativt. Viss lokalutveckling kommer att ske i Sundsvall, men det kommer inte att påverka behovsgrunden i ett nytt säkerhetssystem. En lokalöversyn pågår av Mittuniversitetets alla campus, där även säkerhet tas i beaktande.

4 Omvärldsanalys

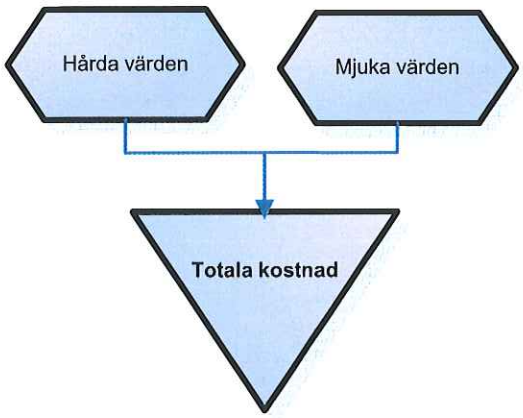
4.1 ERFARENHETER FRÅN ANDRA UNIVERSITET.

Varje universitet har sin egen lösning på säkerhetsområdet. Vissa har tagit fram ett personligt flerfunktionskort med gott resultat, medan andra har tagit in ett säkerhetsbolag på hel entreprenad för att få en bra säkerhetslösning. Det är omöjligt att kopiera någon annans lösning fullt ut då förutsättningarna är olika. Om jämförelsen görs med ett universitet med lika många studenter, så kanske spridningen av verksamheten skiljer eller om jämförelsen görs mot ett campus med liknande spridning så skiljer det förmodligen på budgetnivå. Vissa lägger upp till 5% av totala verksamhetsbudgeten på säkerhet, medan Mittuniversitetet lägger betydligt mindre. Därför är det viktigt att lyssna på vad andra gjort och sedan utvärdera om någon del är applicerbart för Mittuniversitetet.

5 TCO och ROI

5.1 TOTAL COST OF OWNERSHIP (TCO)

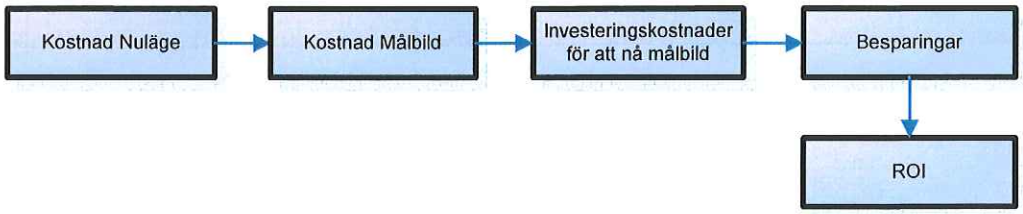
TCO beräknas ur flera faktorer. Dels finns de synliga kostnader som går att koppla till hårdvara, installationskostnad, löner för supportpersonal och dels finns dolda kostnader som alltid är tidsestimat.



De löpande kostnaderna för den tekniska lösningen kommer förmodligen inte bli förändrade, då Mittuniversitet kommer att behöva ett servicekontrakt även med en framtida teknikleverantör, men den utökade funktionaliteten i en ny lösning medger att mer detaljerade larm kan skickas, vilket ger ett bättre beslutsunderlag för om väktarinsats är nödvändig. Någon form av investering kommer att bli nödvändig oavsett om det handlar om en uppgradering eller en nyanskaffning. Kostnaden för detta går i dagsläget inte att bedöma, men det är troligt att investeringsbehovet är avsevärd mindre om en uppgradering sker då redan befintlig kringutrustning i form av dörrmiljöer och larmsensorer kan återanvändas. Om valet faller på en uppgradering av systemet så innebär det trots allt införande av ny teknik som samtidigt bör följas av en översyn av befintlig installation med larmsändare och dörrmiljöer som kontrolleras och trimmas för att mängden falsklarm minimeras, vilket också minskar den totala kostnaden över tiden.

5.2 RETURN OF INVERSTMENT (ROI)

ROI räknas fram på ett liknande sätt som TCO:



ROI definieras dels med ekonomiska och kvantitativa vinster men vinsterna är även kvalitativa.

För projektets vidkommande så är vinsterna till största del av kvalitetshöjande art. Att införa ett mer flexibelt, modernt system borgar för en säkrare arbetsmiljö, som kan anpassas efter den rådande hotbilden som kan förändras över tiden

En konkret ekonomisk vinst är att sammanföra kortkostnader för tre kort till ett kort. Beroende av vilken teknik Mittuniversitetet beslutar att införa blir besparingen större eller mindre. En investering på c:a 300.000 Sek fördelat på tre orter behövs för att klara de krav som ställs på utrustning för framtagandet av unika, personbundna kort vid införandet av ett nytt Multifunktions kort hos Mittuniversitetet. Dagens kostnader för Mittuniversitetets kort specificeras i bilaga 5.

Kostnaden för hantering av kopieringsfunktionen ligger idag på Studentkåren och innebär ingen ekonomisk vinst för Mittuniversitetet, men det är viktigt att denna funktion kan hanteras av ett nytt multifunktionskort, då det skapar ett ekonomiskt mervärde för studenten.

Besparingen på fysiska kort och hantering vid utlämning bedöms vara 57.60 Sek/kort med ett multifunktionskort.

En ytterligare direkt konsekvens av att ett nytt arbetssätt införs är att de larm som genereras av det nya larmsystemet kommer att hanteras på ett strukturerat och spårbart sätt. Detta gör att kostnader kan vidarefaktureras internt så att kostnadsmassan för säkerhet kan spridas över samtliga verksamheter på ett riktigt sätt. Genom att larmen i målbilden registreras direkt i Nilex kan även trender uppfattas och hanteras så att upprepade falsklarmsutryckningar på sikt kan minimeras och därmed sänka utryckningskostnaderna. Vidare minimeras risken för att ärenden faller mellan stolarna eller inte hanteras i tid. Detta ger en synbar kvalitetshöjning som är väldigt viktig när det handlar om säkerhet

6 Slutsats

Kraven på ett nytt säkerhetssystem är något högre än de krav vi ställer idag, men kommer förmodligen inte leda till att en helt ny installation behövs. Kontakter som har tagits med dagens leverantör av säkerhets lösning gör gällande att de krav Mittuniversitet ställer på ett system för framtiden kan hanteras med en uppgradering av befintlig plattform och kringutrustning såsom kortläsare och detektorer kan återanvändas. Ett möte med leverantören är planerat till början av nästa år då den kravlista som detta projekt genererat kommer att gås igenom med leverantören. Om kraven kan tillgodoses så är projektets rekommendation att en uppgradering sker istället för en investering i ett helt nytt system.

En viktig del är även administrationsgränssnittet. Flera tillfrågade ser det som positivt att kunna tillfälligt förändra säkerhetsnivån i sin egen miljö, exempelvis att låsa sin institution när ingen personal finns i lokalerna även inom kontorstid. Därför behövs ett användarvänlig, konfigurerbart gränssnitt eller liknande alternativ lösning. Den kan fungera så att några personer per institution får utökad behörighet på sitt passerkort som gör att de kan låsa och larma egna lokaler med sitt passerkort.

En ny säkerhetslösning måste vara flexibelt och det måste finnas möjlighet att dela in lokaler och byggnader i zoner. Plattformen bör även vara utbyggbar för eventuella framtida behov, ex. med kameror för övervakning av riskutsatta utrymmen. Kortläsare i systemet måste kunna hantera den kortstandard som beslutas av Mittuniversitetet i och med framtagandet av ett multifunktionskort.

För att kunna hantera de larm som kommer från systemet är rekommendationen att det nuvarande ärendehanteringssystemet Nilex används, varför larmen måste vara i den form som Nilex kan hantera så att ärenden kan skapas automatiskt. Vidare kan då larmen följas upp och hanteras direkt i Nilex enligt fastslagna rutiner som tas fram i samband med införande av en ny lösning. Riktlinjer och rutiner måste granskas så att de är aktuella och fungerar i den nya säkerhetsmiljön.

Tekniklösningen är ena delen av systemet och den andra delen är instruktioner för hur säkerhet skall hanteras. Detta behandlas i Mittuniversitetets säkerhetspolicy, riktlinjer för säkerhet och i anvisningar för olika områden inom säkerhet. En handlingsplan för varje institution bör även utarbetas av den enskilda institutionen för att öka förståelsen för behovet av delaktighet för skapandet av ett säkert arbetsklimat på Mittuniversitetets alla verksamhetsområden.

7 Rekommendationer

7.1 FÖRSLAG TILL FORTSATT ARBETE

Flera punkter inom säkerhetsområdet har belysts tidigare i rapporten med förslag till fortsatt arbete. Ett fortsatt arbete kommer att behövas för att nå upp till en önskad, kvalitetssäkrad säkerhetsnivå som är hållbar och flexibel över tiden. Det är mycket svårt att i dagsläget ge ett riktigt tidsestimat för mycket tid som kommer att gå åt för de listade rekommendationerna nedan. Hur mycket tid och resurser som går åt beror på behovet av förändring.

- Utvärdering av den uppgraderade teknikplattformen Torgard kommer att genomföras av Mittuniversitetets säkerhetspersonal i början av 2008. Om alla krav kan tillfredställas med en uppgradering är den lösningen att föredra ur ett ekonomiskt perspektiv. Annars behövs en upphandling under 2008 av ett nytt system som kan tillgodose de skallkrav som framkommit.

- Planering och införande av nytt larmflöde i ärendehanterings-systemet Nilex för att hantera larm, incidenter och övriga händelser. Nya rapportvägar införs och kontrolleras. Det är möjligt att använda den helpdesk som idag endast hanterar IT-support ärenden för mottagning av rapporter om händelser och incidenter kopplat till säkerhet under kontorstid. Efter kontorstid kan dagen webbanmälan även innefatta säkerhetsärenden. Målet är att inga incidenter eller larm skall kunna ramla mellan stolarna eller få en onödigt långsam hantering.

- Mittuniversitetets säkerhetsprocess bör utvärderas efter införandet av uppgraderad/ny teknik och nya rutiner för hantering. En processanalys bör genomföras varefter processen anpassas efter de nya förutsättningar som en ny säkerhetsmiljö ger.

- Fortsatt utvärdering av ett multifunktionskort för Mittuniversitetets personal, gäster och studenter enlig ECCA:s specifikation. Även detta ger ytterligare förutsättningar som blir till krav till kravställningen på en uppgraderad/ny systemteknik.

- Revidera och utveckla säkerhetsutbildning. Utbildningen bör vara tillgänglig i olika former för att passa så många som möjligt. Planera, genomför och utvärdera övningar som bygger på utbildningar.

- Kommunikationsvägar för att nå ut med säkerhetsinformation skall vara definierade. Rekommendationen är att Mittuniversitetets portal används för informationsspridning och att en ny sida för säkerhet utformats.

- Genomgång och avstämning av framtidens riktlinjer och planer för säkerhetsarbete vid Mittuniversitetets med ledningen. Det är mycket viktigt att riktlinjer är förankrade från ledningsnivå och nedåt i organisationen.

- Genomgång och utveckling av policys, riktlinjer och anvisningar för informationssäkerhet. Detta arbete skall ske tillsammans med IT-avdelningen. Samtidigt bör aven en organisatorisk översyn göras så att ansvaret för alla delar av säkerhetsarbetet hamnar på rätt nivå i organisationen. Samspelet mellan fysiska säkerheten, informationssäkerheten och IT-säkerheten är mycket viktig och processerna för hanteringen av enskilt område skall ha klara, definierade kopplingar.

- En genomgång och identifiering av rollerna i säkerhetsorganisationen bör genomföras för att se att alla områden är besatta med tillräckliga resurser för att genomföra verksamheten och att rätt kompens finns för att lösa tilldelade uppgifter.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Informationssäkerhetspolicy
Mittuniversitetet 2006-2008

Informationssäkerhetspolicy
version 1.0, 2006-05-30
Upprättad av: Styrgruppen EffIT
Dokumentansvarig: Ronny Lundberg

Mittuniversitetet
MID SWEDEN UNIVERSITY

Inledning

Inom Mittuniversitetet är informationen en nyckelresurs. All informationshantering ska vara kostnadseffektiv och stödja våra övergripande mål och vår särart. Det är därför grundläggande att vi hanterar vår egen, våra partners och övriga intressenters information på ett säkert och effektivt sätt. Informationssäkerhet innebär för oss att:

- Våra medarbetare, studenter, partners och övriga intressenter har tillgång till den information och de informationsresurser i den utsträckning de behöver för att klara sina arbetsuppgifter och åtaganden *(tillgänglighet)*.
- Vår information vid varje tillfälle är korrekt och att våra informationsresurser säkerställer att informationen inte kan förvanskas genom obehörig och felaktig hantering *(riktighet)*.
- Vi i efterhand kan visa vad som har hänt och vem som har gjort vad vid användande av vår information och våra informationsresurser *(spårbarhet/oavvislighet)*.
- Vår information och våra informationsresurser alltid är skyddade mot obehörig åtkomst *(sekretess)*.

Informationssäkerhetspolicyn är det styrande dokumentet för informationssäkerhetsarbete inom Mittuniversitetet. Policyn omfattar all information inklusive det stöd som finns för att tillhandhålla informationen, såsom IT-system, datornät, servrar och arbetsstationer. Policyn gäller för samtliga anställda, studenter och övriga kontraktsbundna intressenter inom Mittuniversitetet.

Roller och ansvar

Ytterst ansvarig för informationssäkerheten inom Mittuniversitetet är säkerhetschefen som tillsammans med systemägare och systemleverantör ska säkerställa att Mittuniversitetets system kan skydda informationen på ett tillfredställande sätt. Varje individ inom Mittuniversitetet har sedan ett individuellt ansvar för att hantera informationen på ett korrekt sätt med hjälp av de systemstöd som erbjuds. Mer information om systemägare och systemleverantör återfinns i Mittuniversitetets systemförvaltningsmodell, se systemförvaltningsmodell.

Informationssäkerhet är alltså ett verksamhetsansvar som inom Mittuniversitetet innebär att medarbetare, studenter och samarbetspartners ansvarar för att skydda informationen. Beroende på vilken roll man har i organisationen ser ansvaret lite olika ut. Grundläggande för alla roller är dock att efterleva de punkter som återfinns under rubriken "Checklista för individen" i denna informationssäkerhetspolicy.

Strategiska och långsiktiga informationssäkerhetsfrågor ska behandlas av Mittuniversitetets IT-råd och säkerhetschef.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Typ av information

Merparten av den information som hanteras inom Mittuniversitetet är att betrakta som öppen, då vi som statlig instans lyder under offentlighetsprincipen och ska vara tillgänglig för alla.

Inom våra olika verksamhetsgrenar finns dock viss information som inte kan göras tillgänglig för alla och därför måste hållas sekretesskyddad enligt sekretesslagen. För Mittuniversitetet förekommer detta bland annat i följande exempel:

- Tentamensfrågor, 4 kap, 3 §
- Anbud vid offentlig upphandling, 6 kap, 2 §
- Uppgift som rör facklig förhandling eller stridsåtgärd, kap 6, 5§ och 6§
- Uppgift och enskilds förhållanden hos psykolog, kurator, personalkonsulent eller liknande, kap 7, 9§ och 11§.
- Uppgift om psykologisk undersökning för forskningsändamål, kap 7, 13 §
- Uppgifter avseende avskiljande av studenter, kap 7, 27 §
- Uppgift om uppdragsforskning, kap 8, 9 §, samt övrig extern finansierad forskning som kan omfattas av sekretess enlig kap 8, 10 § (affärs- eller driftförhållanden)

Arbetssätt

Individen har ett ansvar att ta ställning till om en informationsmängd är sekretesskyddad. Utifrån detta ställningsstagande ska informationsmängden hanteras enligt nedanstående riktlinjer.

Gemensamt för all information, oavsett om informationen bedöms som öppen eller sekretesskyddad, är att nedanstående delar ska beaktas;

- Information ska vara tillgänglig för de individer som ska ta del av informationen. Detta innefattar aspekter av både lämplighet och rättslig karaktär (t.ex. offentliggörande av myndighetens lokala föreskrifter).
- Information ska arkiveras i enlighet med gällande författningar. Generellt ska allmänna handlingar arkiveras. Undantag ges om det finns någon särskild gallringsbestämmelse (t.ex. tentor, spam etc.).
- Det ska framgå vem som är ansvarig för en viss information samt informationsmängdens utfärdande och aktualitet.
- Information ska vara korrekt.
- Information som berör personuppgifter kan omfattas av PuL (personuppgiftslagen) och ska hanteras i särskild ordning.
- För att uppfylla kraven på tillgänglighet ska alla handlingar i form av dokument, filer, e-brev och liknande lagras på våra centrala servrar. Filer som från myndigheten inte betraktas som handling, programvaror och liknande kan lagras lokalt på datorn.
- För att uppfylla kraven på spårbarhet och oavvislighet ska våra system, så långt det är möjligt, vara uppsatta så att vi i efterhand kan påvisa vad som har hänt och vem som har gjort vad.

Mittuniversitetet
MID SWEDEN UNIVERSITY

För sekretesskyddad information gäller dessutom att:

- Informationen får inte lämnas ut. Finns det ändå ett behov av att skicka sekretesskyddad information till en annan myndighet, eller till någon utanför universitetet, ska man vara medveten om att e-post kan läsas på alla ställen den passerar och kan jämföras med att skicka ett vykort.
- Informationen bör lagras på ett sätt så att det utifrån filnamn eller katalognamn är enkelt att avgöra om informationen är sekretesskyddad. Detta eftersom en handling kan begäras ut enligt offentlighetsprincipen även när den som ansvarar för handlingen ej är i tjänst, och det kan vara svårt för andra medarbetare att avgöra om handlingen är sekretesskyddad.
- Om informationen är sparad på en bärbar dator bör hela eller delar av hårddisken krypteras.

Om det råder osäkerhet kring informationen och vad som räknas till öppen respektive sekretesskyddad information kontaktas Mittuniversitetets jurist, arkivarie eller registrator. Vid frågor kring teknik kontaktas Mittuniversitetets IT-avdelning.

Checklista för individen

Etiska regler

- För användandet av MittNet och universitetets datorresurser finns ett antal etiska regler, se etiska regler

Skydda åtkomst till din dator; Användaridentitet

- Använd alltid "Lås Arbetsstation" (WinLogo + L) när du lämnar din dator obevakad, se till att du har en skärmsläckare och att denna är lösenordsskyddad.
- Försäkra dig om att du loggat av/låst din dator när du lämnar arbetet.
- Ditt användarnamn är personligt men ej hemligt.
- Ditt lösenord är både personligt och hemligt.
- Du får aldrig "låna" ut din användaridentitet/lösenord till någon annan.
- Avslöja inte ditt lösenord för andra och byt lösenord direkt om du misstänker att det kan ha blivit känt.
- Dina lösenord måste följa universitetets lösenordsregler, se regler för lösenord

Bärbar Dator

- Lämna inte din bärbara dator obevakad på allmän plats.
- Vid resa, bär din bärbara dator som handbagage.
- Kontrollera att din bärbara dator tydligt är märkt för att underlätta identifiering och återlämnande vid stöld.
- För att minimera risken för diskkrasch bör du inte utsätta din bärbara dator för extrema miljöförhållanden.
- Din dator är arbetsgivarens egendom och får inte lånas ut till övriga familjemedlemmar, släkt, vänner eller bekanta.

- Tänk på att om du synkroniserar och sparar din e-post och ditt hembibliotek så sparas detta lokalt och okrypterat på din dator.
- Har du mycket känslig information på din dator kan du få din hårddisk (delar av) krypterad. Kontakta IT-avdelningen för mer information.

Trådlösa nät

- Mittuniversitetets trådlösa nät har två olika ingångar, en för studenter (ssid=Student) och en för personal (ssid=Personal). Som personal ska du alltid använda dig av personalnätet där all trafik är krypterad för att förhindra avlyssning.
- Om du som personal kopplar upp dig på andra trådlösa nät måste detta **alltid** ske över universitetets VPN-tunnel, se VPN-tunnel.

Virus

- Agera med försiktighet när du hanterar nya eller okända filer. Detta för att minska risken att bli smittad av virus.
- Du är skyldig att rapportera varje förekomst eller misstänkt förekomst av virus till IT-avdelningen.
- Du får ej försöka avlägsna misstänkta virus själv.
- Du måste säkerställa att din dator har senaste versionen av Antivirusskydd. Har IT-avdelningen installerat din dator sker detta med automatik under förutsättning att du inte ändrar inställningarna.
- Stäng inte under några omständigheter av ditt antivirusskydd.

Skydda din information

- Lämna inte din dator obevakad eller åtkomlig för obehöriga när du arbetar med känslig information eller när du är uppkopplad till system som innehåller känslig information.
- Kasta aldrig dokument som kan anses vara känsliga i papperskorgen. Använd dokumentförstörare.
- Lämna inte dokument som kan anses vara känsliga på allmänna platser eller i centrala skrivare/fax- och kopieringsmaskiner.
- Vill du ha backup på en informationsmängd måste den lagras på ditt hembibliotek (vanligtvis H:\) och inte på exempelvis din lokala hårddisk (C-disk). Det är ditt ansvar att avgöra var information ska lagras och behovet av backup.
- Tänk på att ha kontroll över dina "rörliga medier" som t.ex. usb-minnen, disketter och cd/dvd-skivor etc. och lämna dem inte obevakade om de innehåller känslig information.
- Vid lagring av sekretesskyddade filer kan det underlätta om du t.ex. skapar en katalog som heter "Sekretesskyddade handlingar" och/eller namnger berörda filer med "filnamn.sekretesskyddad.doc". Samma hantering gäller för sekretesskyddad e-post där du t.ex. kan skapa en mapp för "Sekretesskyddad e-post" där alla sekretesskyddade e-brev placeras.

E-post

- Avslöja aldrig ditt lösenord. Vid frånvaro finns speciella regler för hur e-posten ska skötas. För mer information, se mer om e-post.

- Var vaksam när du öppnar meddelanden i vilka ämnet är tvivelaktigt eller om det finns en bifogad fil du inte bett att få. E-post adresser är lätta att förfalska och e-brev som innehåller virus, trojaner eller liknande problem kommer ofta från en avsändare som du "känner".
- Var vaksam på brev skrivna på engelska där avsändaren normalt inte skriver på engelska.
- Öppna aldrig bifogade filer som du inte bett om att få eller där du känner minsta osäkerhet inför dess innehåll. Konsultera istället IT-avdelningen om hur du ska hantera denna typen av filer.
- Var restriktiv med att lämna ut din e-post adress. Man blir ofta uppmanad att ange sin e-postadress på webbsidor, men gör inte detta om du inte verkligen litar på företaget som har webbsidan.

Hantering av Incidenter

- Incidenter måste omedelbart rapporteras till din närmaste chef eller säkerhetschef.
- Notera allt som kan vara av vikt. Skriv ner så mycket som möjligt så att du kan besvara frågor om vad som hänt och när det hände.
- Avslöja detaljer endast till de personer som behöver dessa för att fullfölja sitt arbete.

Installation av hård- och mjukvara

- Installera inte hård- eller mjukvara själv. All hård- och mjukvara ska installeras av IT-avdelningen.
- För all installerad mjukvara ska erforderlig licens finnas.
- Gratis programvara kan ibland innehålla så kallad adware eller spyware. Kontrollera därför alltid med IT-avdelningen om du är osäker på programvarans innehåll.

Hot mot Informationstillgångar

	Hot	Beskrivning	Hot mot	Sannolikhet	Påverkan	Åtgärd
1a	Skyddsidentitet uppdagas	Om information om skyddad identitet inte hanteras på ett säkert och genomtänkt sätt så är det lätt att skilja ut de personer som har en skyddad identitet. Oaktsamhet är straffbart	Sekretess	Låg	Mycket allvarlig	Genomgång av rutin som hanterar skyddade personer
1b	Spridning av resultat av annan än Forskargruppen	Om någon annan än de behöriga forskarna får del av resultatet som forskningen producerat kan detta användas av den enskilde för egna syften.	Sekretess Riktighet Spårbarhet	Måttlig	Allvarlig	Det skall vara möjligt att hantera resultat och material på ett säkert sätt så att sekretessen kan bevaras.
1c	Avslöjad design i förtid	Vid samarbete med externa partners är det extremt viktigt att designresultat hålls inom arbetsgruppen som har avtalet med den externa patrnern. Information som foton och resultat av tester måste hanteras på ett säkert sätt.	Sekretess Riktighet Spårbarhet	Låg	Allvarlig	Information och utbildning kring ämnet. Kontroll av tillträde till designlabb och prototyper.
1d	Olovlig läsning av Tentamen	En tenta hanteras av flera personer i flera steg. Det ger en förrövare tillfällen att ta del av innehållet i förväg. Detta är primärt ett hot mot sekretessen.	Sekretess Spårbarhet	Måttlig	Allvarlig	Strikta regler för hur en tenta får skickas mellan inblandade personer och hur den skall förvaras innan före skrivningstillfället.
1e	Oklara rutiner vid händelse rapportering	Om kontaktvägar, vad som bör anmälas, och hanteringsprocess är oklara så kan inte kvaliteten i ärendehanteringen garanteras.	Riktighet Spårbarhet	Måttlig	Allvarlig	Skapa rutin som beskriver hur en anmälan sker och hur den hanteras. Använd ärendehanteringssystem för att säkra kvalitet i hanteringen. Det ger möjlighet till statistik, eskalering och pro-aktivt arbete

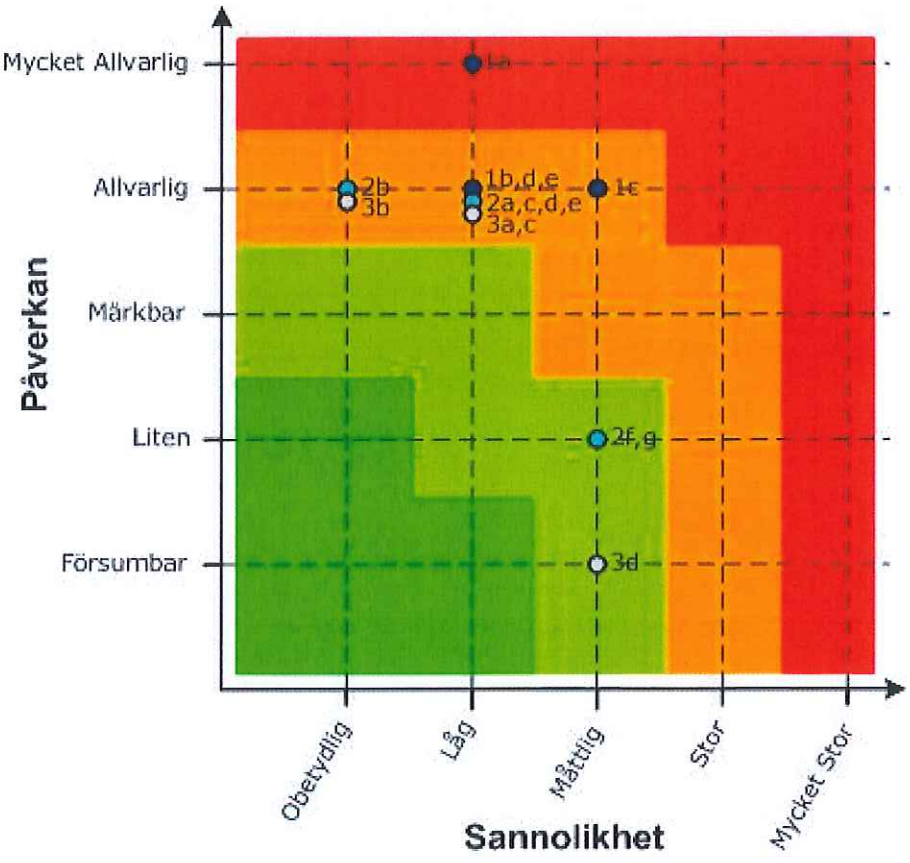
Hot mot Anläggningstillgångar

	Hot	Beskrivning	Hot mot	Sannolikhet	Påverkan	Åtgärd
2a	Oanvändbara Utbildningssalar		Tillgänglighet	Låg	Allvarlig	
2b	Personhot (bibliotek)	Personer (kunder) till biblioteket kan uppträda hotfullt mot personalen och då lokalen är en allmän area dit alla har tillträde under öppettid	Tillgänglighet	Obetydlig	Märkbar	Utbildning i att hantera situationen. Aldrig ensamarbete. Larm till hjälp i någon form (kollegor, väktare)
2c	Brand	Brand i lokeler	Tillgänglighet	Låg	Allvarlig	Utbildning Plan Övning
2d	Vatten	Biblioteket drabbas av fukt, ex genom översvämning, det regnar in genom takfönster.	Tillgänglighet	Låg	Allvarlig	Utbildning Plan Övning
2e	Icke ändamålsenliga Labb	Lokalerna är anpassade till den verksamhet som skall bedrivas. Det innebär att man inte kan välja en annan sal om det aktuella labbet inte är tillgängligt.	Tillgänglighet	Låg	Märkbar	
2f	Stöld av personliga tillhörigheter	Tillgrepp mot enskilda personer och där personliga tillhörigheter eller den utrusning som Mittuniversitetet tillhandahåller.	Tillgänglighet Spårbarhet	Måttlig	Liten	En generisk identifikationshandling för Mittuniversitetets anställda, gäster och studenter som skall bäras synligt eller visas upp på anmodan. Vana att alltid låsa kontor när man lämnar rummet.
2g	Inbrott	Samma nyckel används till alla rum i en korridor. Det räcker med att en nyckel kopieras eller kommer på avvägar så har en förrövare tillträde till alla rum.	Tillgänglighet Spårbarhet	Måttlig	Liten	Unika låscylindrar eller möjlighet till inlåsning/fastlåsning av stöldbegärligt gods. Rutiner för lås och larm av institutionen

Hot mot applikationer och system

	Hot	Beskrivning	Hot mot	Sannolikhet	Påverkan	Åtgärd
3a	Virusangrepp i LADOK server	LADOK server blir smittad av Virus vilket kan göra informationen otillgänglig eller korrupt.	Tillgänglighet Riktighet Spårbarhet	Låg	Allvarlig	Väl inarbetade rutiner för hur skyddet skall hållas på rätt nivå. En katastrofplan för hur en smittad server på snabbaste sätt återställs till normal status igen.
3b	Kommunikations bortfall till LADOK server	Om information inte kan hämtas från LADOK kan inte studentstatus kontrolleras och inpasseringssystemet kan inte uppdateras med uppgifter.	Tillgänglighet	Obetydlig	Allvarlig	
3c	e-post Server går ner	Om e-post server inte är tillgänglig kan ingen e-post skickas eller tas emot. Detta hämmar verksamheten i stor utsträckning och arbetet stannar av.	Tillgänglighet Riktighet Spårbarhet	Låg	Allvarlig	Katastrofplan bör upprättas och övas för att återställa tjänsten så fort som möjlighet. En reservrutin bör även skapas.
3d	Felaktig information	Studenter ha nu möjlighet att uppdatera vissa fält på egen hand. Påverkar dock inpasseringssystemet, men bara den enskilde	Riktighet	Måttlig	Försumbar	Stickprovskontroll av uppgifter kan ske med jämna mellanrum

Grafisk tabell över Sannolikhet - Påverkan



Mittuniversitetets Säkerhetsöversyn

Intervju underlag, nuläges- och riskanalys

1. Verksamhet

1.1 Övergripande

Verksamheten kan se olika ut inom olika enheter och Campus.

Fråga:
Beskriv den verksamhet som din enhet bedriver här.

Svar:

1.2 Visioner / Mål

Mittuniversitetet har en Vision och ett antal verksamhetsmål

Fråga:
Känner du till Mittuniversitetets Vision och mål?

Svar:

1.3 Problem

Fråga:
Har ni några direkta problem som härrör till säkerhet idag?

Svar:

---

2. Tillgångar

2.1 Kritiska tillgångar

Varje verksamhet har ett antal kritiska tillgångar, d v s tillgångar som gör att verksamheten flyter. Om en eller flera tillgångar försvinner eller på annat sätt blir obrukbara kommer verksamheten fungera väsentligt sämre eller stanna av.

Fråga:
Nämn några tillgångar som är viktiga för er verksamhet.

Svar:

2.2 Effekter

Fråga:
Vilken effekt skulle ett tillgångsbortfall få för er verksamhet?

Svar:

---

3. Hot

3.1 Potentiella hot

Mot varje verksamhet finns en hotbild. De kan vara av karaktären att nyckelpersoner försvinner, utrusning blir stulen, IT-systemen slutar att fungera.

Fråga:
Kan du se några hot som är troliga mot er verksamhet.

Svar:

3.2 Trygghet

Fråga:
Upplever du din arbetssituation som trygg?

Svar:

3.3 Direkta / Upplevda hot

Mot varje verksamhet finns en hotbild. De kan vara av karaktären att nyckelpersoner försvinner, utrusning blir stulen, IT-systemen slutar att fungera.

Fråga:
Ha du eller någon annan upplevt något hot om er verksamhet?

Svar:

---

4. IT-Stöd

4.1 Typ av stöd

I stort sett all verksamhet är idag beroende av ett väl fungerande IT-stöd för att arbetet skall bedrivas effektivt.

Fråga:
Vilka IT-funktioner används som stöd i er verksamhet?

Svar:

4.2 Effekter av bortfall

I stort sett all verksamhet är idag beroende av ett väl fungerande IT-stöd för att arbetet skall bedrivas effektivt.

Fråga:
Hur länge skulle verksamheten kunna fortgå om IT-stödet försvann?

Svar:

4.3 Reservrutiner

I stort sett all verksamhet är idag beroende av ett väl fungerande IT-stöd för att arbetet skall bedrivas effektivt.

Fråga:
Vilka reservrutiner finns om IT-stödet skulle försvinna.

Svar:

---

5. Information

5.1 Spridning av information

Fråga:
Hur sprids information inom er enhet

Svar:

5.2 Inhämtande av information

Fråga:
Hur får ni information om mittuniversitetets övriga verksamhet?

Svar:

5.3 Portal

Fråga:
Använder ni Mittuniversitetets portal för att sprida information om er verksamhet till andra.

Svar:

---

6. Utbildning

6.1 Idag

Personal och studenter behöver besitta kunskaper dels om verksamheten på den enhet där man är aktiv, dels och 'sitt' campus och om Mittuniversitetet generellt. Det innefattar bl a regler för in/utpassering, inskrivning, IT-säk utb, rutiner vid brand, etc

Fråga:
Hur utbildas personal och studenter idag.

Svar:

6.2 Framtiden

Personal och studenter behöver besitta kunskaper dels om verksamheten på den enhet där man är aktiv, dels och 'sitt' campus och om Mittuniversitetet generellt. Det innefattar bl a regler för in/utpassering, inskrivning, IT-säk utbildning, rutiner vid brand, etc

Fråga:
Hur skulle du vilja att utbildning kring detta bedrevs?

Svar:

---

7. Händelsehantering

7.1 Rapportering

Fråga:
Hur rapporteras en säkerhetsincident idag?

Svar:

7.2 Uppföljning

Fråga:
Vill du som anmälare bli uppdaterad på händelseutvecklingen i ett rapporterat säkerhetsärende?

Svar:

---

8. Övriga frågor

8.1 Specifika behov

Fråga:
Finns det några speciella behov som er verksamhet har som vi inte diskuterat under andra punkter?

Svar:

Minnesanteckningar förda vid ECCA-möte 2007-10-18 – 10-19, Ågrenska villan Göteborg

Närvarande: Se bilaga

1. Inledning och välkommen

Tommy Wallhult, värd för konferensen, inledde med att hälsa alla välkomna till Göteborg och Ågrenska villan.

2. Tor Fridell – ECCA-president

Tor Fridell informerade om ECCA (European Campus Card Association) och dess verksamhet. Organisationen växer fort och har i dagsläget ca 50 medlemmar. Varje sommar genomförs en internationell konferens (nästa blir i Lodz, Polen 16 – 17 juni 2008). ECCA Sverige – och förhoppningsvis snart ECCA Skandinavien – är en underavdelning till "stora" ECCA. ECCA driver vissa landspecifika frågor och dess huvudsyfte är erfarenhetsutbyte.

3. Presentationsrunda – olika lärosäten i Sverige

Göteborgs universitet
Arbetet med att införa ett GU-kort har genererats ur ett delprojekt i det s k NEKST-projektet vid Göteborgs universitet. Ett projekt som till huvuduppgift hade att ta bort kontanthanteringen inom GU. Första steget var att ta bort handkassorna och införa ett s k inköpskort. Det projektet är avslutat och i dagsläget har ca 500 inköpskort i princip ersatt handkassorna.

I arbetet med att kartlägga kontanthanteringen framkom att en stor del av den sker mellan GU och dess studenter och mellan GU och allmänheten. Vårt uppdrag inom NEKST-prjektet har nu övergått till att införa ett GU-kort för studenter (och anställda på sikt). Målet är en enhetlig kortlösning för hela GU med passage, bilbiotek, copy/print, betalfunktion osv. Pilotprojekt startas i dec 2007 – jan 2008 då i första hand passage, copy/print kopplat till någon form av betalfunktion testas. Utvärdering sker och sedan tar upphandling och implementering i liten skala vid för att successivt omfatta hela GU.

Karolinska institutet
Idag har man passerfunktion, biblioteks- och copy/print-funktionen på en del ställen. Målet är att man skall kunna koppla på både betalfunktion och kårleg på samma kort.

Chalmers
Idag finns det många olika kort inom Chalmers. Utskrifter osv betalas kontant i ett system. Man för f n inga diskussioner om att samla alla funktioner på ett och samma kort.

Umeå
Här jobbar man med ett campusprojekt vars syfte är att införa ett kort med många funktioner. Bakgrunden är liknande den i Göteborg. Projketplanen är klar och driftstart är beräknad till den 1 jan 2008 med fyra serviceställen för distribution av korten.

SLU
SLU finns på fyra orter i landet och det finns idag många olika kort. Målet är att samsas om ett system. Samarbete sker med Mälardalens högskolor betr Ladokbiten och man ser även över andra funktioner. I dagsläget diskuteras ej så mycket kontanthantering.

Lunds universitet
Campus finns på 3 – 4 ställen varav ett är universitetssjukhus. För närvarande diskuteras hur man kan förenkla copy/printbiten. Man testar ett system via Carl Lamm där ett virtuellt kort skapas (alltså inget platskort). Man avser också att i framtiden endast ta emot konferensavgifter och betalning för trycksaker via nätet.

Lunds tekniska universitet
Här finns sedan 2005 ett studentkort med id-, passer-, biblioteks-, inloggnings- och labredovisningsfunktioner. På sikt vill man införa betalkort med rabatter inlagda.

Kalmar
Här finns idag många olika lösningar som man försöker samordna. Ett gemensamt kort beräknas införas under 2008.

Stockholms universitet
Här samarbetar man inte med studentkåren, vilket innebär att kårleg inte blir aktuellt. Fr o m den 1 jan 2008 kommer ett kort att finnas med biblioteks- och passerfunktion. Man har i dagsläget inte funderat på någon form av betalfunktion i kortet.

Jönköping
Här finns idag två olika passersystem till vilka basdata importeras från en intern databas över personal och studenter. Data tankas ned två gånger per dygn till kortet. Från databasen hämtas även den giltighet som skall sättas ut på kortet.

Mälardalen
Här finns ett kort med id-, passer-, biblioteks- och färdbevisfunktion (buss mellan två campus) Kortet förnyas varje termin genom att man sätter på ett klistermärke som tas ut vid en läsare. Betalfunktion för copy/print finns på kortet som laddas med pengar. Kortet körs mot Ladok och passagefunktionen knyts till det. Kan ändras manuellt vid behov. Kompendier m m säljs via Akademibokhandeln så ingen kontanthantering sker ute vid institutionerna.

Linköping
Här finns ett fungerande kortsystem – LIU-kortet – som omfattar:

- id
- passer
- studenbevis
- busskort mellan campus
- lånekort
- medlemsbevis för kåren

Kortet har blivit ett varumärke som bygger identitet och trygghet.

Mittuniversitetet
Under 2008 startas ett projekt "Allkort" som är planerat att starta under 2009. De tittar mycket på Linköpings kortsystem.

4. Info från PasCard

Vi fick information om PasCard och dess tjänster. Här nedan följer en kort sammanfattning. (PP-presentation bifogas också minnesanteckningarna.)

Det kort som gäller på marknaden nu är ett s k RFID plastkort (RFID = Radio Frekvent IDentifikation), som innehåller:

- magnetremsa för t ex tidredovisning, passerfunktion, lånekort, betalkort, copy/print
- streckkod för t ex lånekort, tidredovisning

RFID innebär ett beröringsfritt kort och Mifare är namn på en produkt. När det gäller säkerhet kan konstateras att bankerna går i allt högre utsträckning över till RFID-systemet. Vad kortet i övrigt innebär och erbjuder framgår av den bifogade pp-presentationen, men i korthet kan sägas att om fler funktioner samlas i ett kort ger det fler möjligheter och sparar miljö, sparar pengar, effektiviserar administrationen och tar bort onödig kontanthantering.

5. Outsourcad copy/print - LIU

Linköpings universitet har efter att ha inventerat behov av skrivare/kopiatorer och analyserat kostnaderna för utskrifter och kopiering beslutat att man skall köpa hela tjänsten – utom påfyllning av toner och papper – från leverantören. Detta innebär en helhetslösning för utskrifter och allt sköts centralt. I princip alla skrivare och kopiatorer byts ut och betalning för utskrifter kommer att ske via klick-kostnad.

Förslag på lösning ser ut enligt nedan:
- en extern totalleverantör
- ett utskriftsystem
- ett betalsystem
- en driftorganisation
- en förvaltning

Upphandlingen är inne i slutskedet och det skall bli spännande att se hur det går med de tre pilotprogrammen som kommer att startas inom kort.

6. Chalmers

Från Chalmers rapporterades att man satsar på en central IT-förvaltning och med ett upplägg som lite liknar Linköpings, dock inte outsourcat.

7. Mecenat

Mecenat är ett rabattkort som riktar sig till studenter och finansieras via verifierade partners som ger studenterna rabatt mot uppvisande av ett giltigt kort. En gemensam layout-del avseende rabatter är viktigt för att kunna uppvisa ett enat kort gentemot rabattgivarna.

Vilka studentrabatter är viktiga?
- För universitet och högskolor
- För andra myndigheter
- För rabattkortsföretagen

… och för studenten?

SJ är navet, hamburgaren är viktig…

När det gäller SJ är det de som sätter normen:
- man måste vara heltidsstudent
- man måste vara inskriven kårmedlem (kravet på att uppbära studiemedel är släppt, men manuell verifiering via kåren krävs)
- man måste studera minst 75% under 20 veckor eller 100% under 15 veckor

Mecenat förhandlar fortfarande med SJ om själva "studentbegreppet". När det gäller lay-outen är SJ bekymrad över att loggan ser litet hemmagjord ut i den överskrivningsbara ytan på kortet.

En gemensam plattform är vägen att gå för att nå en totallösning med SJ.

8. Studentkortet - Cosmos

Studentkortet – Cosmos är också ett kort som riktar sig till studenter med ungefär samma upplägg som Mecenat. Inom företaget finns:
- Chili (en tidning)
- Reklambyrå
- Ungdomsbarometer som speglar ungdomar mellan 16 – 30 år
- Studentkortet

De erbjuder rabatter i mängder till studenterna och gör regelbundet undersökningar om vilka rabatter som studenterna vill ha.

9. Vad kan ECCA göra för dig?

Inledningsvis informerades om ECCA och då även om konferensen som hålls den 16 - 17 juni 2008. Maila gärna till Tor Fridell om vad som bör tas upp under konferensen.

Svenska ECCA
Det finns mängder med medel att söka och Svenska ECCA bör göra det, men då måste vi ha ett verkligt fall. Beslutades att jobba vidare med den frågan.

Beslutades också att Svenska ECCA skall genomföra en konferens per termin från lunch till lunch. Nästa gång ses vi i Lund den 23 – 24 april 2008. Punkter att ta upp då:
- Print on demand
- Moms på utskrifter
- Passersystem – elektroniska nycklar
- Banker
- Mecenat/Studentkort/Membit

Vid pennan

Kerstin Gidsäter
2007-10-23

1 Krav på nya systemet

Nr	KRAV	JA/NEJ	KOMMENTAR
1	Bra, fuktionellt administrations gränssnitt som eventuellt kan användas av verksamhets-personal för att hantera larm och dörrmiljöer på den egna institutionen		
2	Fullt fungerande SIM modul som täcker MIUN:s behov		
3	Kortläsare som klarar ECCA-standard för kort		
4	Larm kan skickas till NILEX-ärendehanterings system		
5	Detaljerad presentation av vilken detektor som genererat larmet		
6	Almanacksfunktion i Administrationsgränssnittet är ett krav.		
7			
8			
9			
10			

2 Kostnader för Flerfunktionskort

Ett flerfunktionskort fyller ett flertal syften. Grunden är ett passerkort som blir personligt i och med att personuppgifter och foto trycks på varje kort. Designen på kortet visar också att bäraren tillhör Mittuniversitetet och tre kategorier kort tas fram: Personal, student och gäst. Kortet skall alltid bäras och uppvisas på anmodan.
Sedan kan ytterligare funktionalitet knytas till kortet. Lånefunktionen i biblioteket hanteras idag via en streckkod på ett anonymt kort som kopplas till personuppgifter. I framtiden kan streckkoden skrivas på passerkortet och kostnaden för kort i biblioteket kan minskas väsentligt.
Utskrift och kopiering kan även den knytas till det nya kortet och nu har kortet fått ett ekonomiskt värde som gör bäraren mindre benägen att låna ut kortet.

2.1 KORTKOSTNADER, NULÄGE

Passerkort
Dagens kort är förhållandevis dyra för den begränsade funktionaliteten. Vidare gör korthanteringsrutinen att många kort låses upp till studenter som sedan inte hämtar ut kortet. I och med att man väljer ett nytt kort som kan få utökad funktionalitet och skapar en ny rutin så att kortet produceras vid utlämningstillfället kommer man inte att binda ner kapital i kort som inte används. Vi beräkningen nedan används en genomsnittlig timlönekostnad på 167 Sek (inkl. soc. avg)

Fysiskt kort:	21 Sek
Kostnad för utlämning:	5.60 Sek (2 min)
TOTAL:	26.60 Sek

Lånekort på bibliotek

Fysiskt kort:	10 Sek
Tid vid utlämning:	2.80 sek (1 min)
TOTAL	22.80 Sek

Kopierings/utskriftskort

Fysiskt kort:	20 Sek
Tid vid nyutlämning:	2.80 Sek
TOTAL:	22.80 Sek

2.2 KORTKOSTNADER, FRAMTID

Fysiskt kort:	2 Sek för samma teknik som används idag.
Hanteringskostnad:	5.60 Sek (2 min produktionstid)
TOTAL:	7.60 Sek