

POLICY FÖR DATA- OCH INFORMATIONSSÄKERHET VID BMC I LUND

Oktober 2005

Innehåll

Introduktion	1
Avsikten med denna policy	1
Ansvar	1
Allmän policy.....	2
Klassificering av data	2
Accesskontroll	3
Policy för viruskydd.....	4
Policy för användning av nätverk och andra dataresurser	4
Policy för internetsäkerhet.....	5
Intrångsövervakning.....	5
Undantag.....	6

INTRODUKTION

Denna data- och informationssäkerhetspolicy är utformad med hänsyn tagen till att BMC består av ett stort antal olika enheter med skilda behov och användningssätt av datorer, datahantering och datanätverket. Policyn är inte avsedd att inkräkta på eller inskränka den akademiska friheten. Denna policy gäller för samtliga nätverksanvändare inom BMC.

Datanätverket i BMC är anslutet till LUNET, Lunds Universitets datanätverk, och därigenom till SUNET – det svenska universitetsnätverket. Detta policydokument grundar sig på LUNETs säkerhetspolicy, på Lunds Universitets regler för användning av datanätverk (Dnr: I D9 2218/2001) och SUNETs säkerhetspolicy. Det är till alla delar en tillämpning av dessa regler men inte nödvändigtvis en tillämpning av samtliga regler. Detta innebär att grunddokumenten är överordnade denna policy, och att samtliga deras regler gäller. Vid tvetsamheter har SUNETs säkerhetspolicy tolkningsföreträde

AVSIKTEN MED DENNA POLICY

Avsikten med denna policy är:

- Att fastställa en uppsättning regler för att skydda BMCs data, programvaror, nätverk och datasystem från intrång, obehöriga förändringar eller förstörelse.
- Att föreskriva verktyg och metoder för att identifiera och förhindra försök till intrång, obehöriga förändringar eller förstörelse av BMCs och Lunds Universitets data, programvaror, nätverk och datasystem.
- Att föreskriva verktyg och metoder för att skydda Lunds Universitets och BMCs goda renommé samt för att möjliggöra för Lunds Universitet att leva upp till det legala och etiska ansvar som följer av nätverkets och datasystemens förbindelse med Internet.
- Att föreskriva effektiva metoder för att hantera utifrån kommande klagomål och förfrågningar rörande verkligt eller upplevt missbruk av BMCs datanätverk och datasystem.

ANSVAR

- BMCs styrelse ansvarar för att reglerna i denna policy genomföres och upprätthålls.
- BMCs styrelse skall försäkra sig om att:
 - föreliggande data- och informationssäkerhetspolicy regelbundet revideras och hålls aktuell samt publiceras på lämpligt sätt;

- nätverks- och systemadministratörer, serveransvariga och användare har tillräckliga kunskaper och resurser för att fullgöra sina uppdrag på ett tillfredsställande sätt. Lunds Universitets datasäkerhetsgrupp definierar erforderlig kompetens för att installera, konfigurera och bruka system och programvaror anslutna till LUNET (Dnr: I A9 6461/2001)
- BMCs styrelse skall utse en person som ansvarar för att säkerhetsreglerna upprätthålls, att incidentuppföljning och regelbunden revidering av användarregister genomförs samt att verksamheten informeras och utbildas rörande data- och informations-säkerhetspolicy, inkluderande information om aktuella risker för datavirusangrepp.
- Användarna ansvarar för att tilldelade anordningar för accesskontroll (t.ex. magnetkort) samt inloggningsinformation hanteras och förvaras på ett säkert sätt – inte i närheten av en dator där de kan användas för att skapa förbindelse med BMCs nätverk. Förlust av sådan anordning skall omedelbart anmälas så att den kan göras oanvändbar.

ALLMÄN POLICY

- Utvärdering av nätverkets sårbarhet och de risker som följer av externa förbindelser skall regelbundet genomföras (minst årligen).
- Säkerhetskontroll av servrar, brandväggar, routers och enheter för systemkontroll och systemadministration skall regelbundet genomföras. Detta omfattar kontroll av innehållet i accessloggarna och loggar från intrångsdetektering.
- Utbildning och information utformas så att användare av nätverket förstår vad datasäkerhet, säkerhetsnivåkrav och dataskyddsåtgärder innebär. Denna utbildning och information anpassas till målgrupperna nätverksadministratörer, systemadministratörer, serveransvariga och nätverksanvändare.
- Brott mot denna policy kan resultera i disciplinära åtgärder i enlighet med Lunds Universitets regelverk.

KLASSIFICERING AV DATA

- Det är av yttersta vikt att Lunds Universitets och BMCs data och information skyddas. Med jämna mellanrum skall data och information inventeras med avseende på dess användning, riskklass och betydelse för verksamheten. Nedan följer en förenklad klassificering:
 - Känsliga data – information som allvarligt skulle skada Lunds Universitet, BMC, enskilda individer, grupper eller organisationer om den skulle röjas eller förändras. Hit hör data som omfattas av lagstiftning (t.ex Datalagen och Personuppgiftslagen) liksom lösenord. Även vissa data om anställda och vissa ekonomidata hör av integritetsskäl till denna klass.

- Viktiga data – källkoder, loggar, resultat från vetenskapliga experiment, tentamensresultat etc. som inte skulle medföra någon större skada om de röjs, men som måste skyddas mot varje form av obehörig modifiering och förstörelse.
- Publika data – data som får distribueras fritt.
- SUNETs säkerhetspolicy (securityinfo 2 och 5) innehåller detaljerade anvisningar för korrekt skyddsnivå relaterad till klassificeringen av data och information.
- Alla informationsresurser bör klassificeras och skyddas i enlighet med de kriterier som följer av klassificeringen, och samma/motsvarande skyddsnivå och åtgärder skall tillämpas när data kopieras, förflyttas eller bearbetas.
- Serveransvariga skall tillse att data som lagras hålls intakta och har rätt skyddsnivå. Användare av sådana data ansvarar för att skyddet bibehålls på rätt nivå.
- Alla data bör säkerhetskopieras, och kopiorna skall regelbundet kontrolleras. Såväl säkerhetskopiering som kontroll skall loggas och/eller dokumenteras.
- Säkerhetskopior av känsliga och viktiga data skall hanteras med samma säkerhetsnivå som originaldata. När system och/eller datamedia skrotas eller återanvänds skall känsliga och viktiga data förstöras på ett sätt som är förenligt med dess skyddsklass.
- Vid överföring av särskilt känsliga data bör kryptering övervägas. SUNET säkerhetspolicy ger vägledning.
- Inget system inom BMC får ha förbindelse med Internet utan att vara försett med anordningar för att skydda dess information i enlighet med säkerhetsklassificeringen.

ACCESSKONTROLL

- Åtkomst till nätverket, servrar och andra datasystem får endast ske via egen, personlig inloggningsidentitet, och skall vara verifierad. Detta kan ske genom lösenord, smartkort, biometri (fingeravtryck etc.) eller någon annan vedertagen metod för verifiering.
 - Användare får inte delge någon annan sina användaridentiteter eller lösenord. Inte heller får sådana skrivas ner eller lagras i okrypterad form i datafiler eller dokument. Alla användare är skyldiga att försäkra sig om att användarnamn, kontobeteckningar och lösenord inte kan användas av obehöriga.
 - Alla användare av system som innehåller känsliga data skall ha tillräckligt säkra lösenord i enlighet med definitionen i SUNETs säkerhetspolicy (securityinfo 4) eller enligt beslut av BMCs styrelse. Lösenord till konton med hög behörighetsnivå (som systemadministratör, rootbehörighet eller supervisor) skall bytas ofta i enlighet med anvisningar eller beslut från nyssnämnda. .
 - Användaridentiteter eller lösenord får inte vara lagrade i program eller datafiler.
 - Lösenord får inte delges via epost, som inte krypteras. Är detta inte möjligt måste lösenord delges på något annat, tillräckligt säkert sätt.

- Alla standardlösenord måste ändras efter systemets installation. Alla administratörskonton och rootbehörigheter skall ges lösenord i enlighet med denna policy så snart ett system har installerats, ominstallerats eller omkonfigurerats.
- Alla servrar skall förses med system för upptäckt av intrång och intrångsförsök. Konton skall spärras efter ett förutbestämt antal misslyckade inloggningsförsök, och skall förbli spärrade så länge som bedöms lämpligt med hänsyn till dess säkerhetsnivå.
- Konton som tillhör användare som slutar sin anställning eller verksamhet skall avslutas eller spärras. Eftersom det ofta förekommer långa fördröjningar vid rapporteringen av sådana fall, skall den data- och informationssäkerhetsansvarige vid BMC regelbundet inventera användarkonton.
- Konton som tillhör personer som byter arbetsuppgifter eller organisationstillhörighet skall revideras med avseende på behörigheter.
- Loggning skall genomföras på alla känsliga system (där denna möjlighet finns) för att registrera lyckade och misslyckade inloggningsförsök (datum och tid för in- och utloggning).
- Personal med hög behörighetsnivå (administratörer mm) skall använda ett konto med lägre behörighet för arbetsuppgifter där detta är tillräckligt. Alla aktiviteter som utförs med högre behörigheter skall loggas om detta är möjligt. Det skall finnas en förutbestämd, dokumenterad procedur för att granska sådana systemloggar.

POLICY FÖR VIRUSSKYDD

- Alla servrar och arbetsstationer som ansluts till BMCs nätverk skall vara skyddade med ett adekvat, licensierat antivirusprogram som skall hållas uppdaterat till den nivå som distributören av programvaran rekommenderar.
- Inkommande data, inklusive epost, skall kontrolleras med avseende på virus. Även utgående epost skall kontrolleras.
- System- och/eller nätverksadministratörer skall informera användarna om upptäckta virus.
- Om epost kontrolleras centralt med avseende på virus, skall denna verksamhet loggas.
- Avsiktligt införande av datavirus och/eller annan destruktiv programkod i BMCs eller Lunds Universitets nätverk är förbjuden, och kan leda till allmänt åtal.

POLICY FÖR ANVÄNDNING AV NÄTVERKET OCH ANDRA DATARESURSER

- BMCs och Lunds Universitets dataresurser skall användas på ett sätt som överensstämmer med gällande regel- och policydokument samt svenska lagar och regler. Det är ett brott mot Lunds Universitets regler att installera programvara som

inte är försedd med gällande licens på någon av universitetet ägd eller i LUNET brukad dator.

- All användning av BMCs och Lunds Universitets dataresurser och nätverk som inte är relaterad till verksamheten på BMC eller vid universitetet skall begränsas i tid och resursanvändning så att den egna eller andras ordinarie verksamhet inte påverkas. Om användaren är tveksam om vad som kan vara tillåtet skall närmaste chef alltid tillfrågas
- All användning som inverkar menligt på nätverk, datasystem, program och andra dataresurser eller som förhindrar eller försvårar för andra att använda dessa resurser för att utföra sina arbetsuppgifter är otillåten. Exempel på sådan användning kan vara överföring av stora datamängder för privat bruk – t.ex. nedladdning av film och stora ljudfiler.
- Det är inte tillåtet att använda BMCs eller Lunds Universitets dataresurser för egen vinning, t.ex. genom affärsverksamhet eller genom att distribuera material mot personligt arvode.
- Avkodning eller försök till avkodning av lösenord är förbjuden, utom för särskilt utsedd personal som utför kontroll av säkerhet eller genomför säkerhetsrelaterade utredningar. Nätverksavlyssning får utföras av nätverks- eller systemadministratörer för felsökningsändamål. Säkerhetsansvariga får också utföra nätverksavlyssning inom ramen för sina uppdrag. Nätverksavlyssning får inte användas för att kontrollera eller spåra enskilda användares aktiviteter, utan särskilt tillstånd av Lunds Universitets datasäkerhetsgrupp i varje enskilt fall.
- Universitetets datasäkerhetsgrupp och BMCs datasäkerhetsansvarige har rätt att ta del av data- och loggfiler i varje utrustning som är eller har varit ansluten till LUNET (eller delnät) för att genomföra utredningar om misstänkt missbruk eller andra incidenter. Detta innefattar rätten att tillfälligt beslagta sådan utrustning för undersökning.

POLICY FÖR INTERNETSÄKERHET

- All anslutning till Internet skall ske via en säker anslutningspunkt för att garantera nätverkets integritet. Publika servrar med information och data som skall kunna nå från Internet utanför BMC, skall anslutas till särskilda nätverksuttag, anvisade av BMCs datasäkerhetsansvarige.

INTRÅNGSÖVERVAKNING

- Operativsystem och i förekommande fall program skall ha loggning aktiverad i alla servrar och arbetsstationer som medger detta. Om det är möjligt skall dessutom loggarnas larmfunktioner vara aktiverade.
- I alla servrar och arbetsstationer som hanterar känsliga och viktiga data skall systemens integritet kontrolleras. Loggar i servrar, brandväggar och viktiga system skall

kontrolleras ofta. Där det är möjligt skall automatisk loggkontroll användas så att den säkerhetsansvarige omedelbart meddelas när allvarliga säkerhetsintrång sker.

- Intrångsdetektering skall installeras där det bedöms vara av värde, och skall kontrolleras med jämna mellanrum.
- System- och nätverksadministratörer skall hålla sig underrättade om aktuell säkerhetsrelaterad information, hotbilder, sårbarheter, incidenter, system- och programkompletteringar, uppgraderingar och uppdateringar samt se till att all utrustning inom hans/hennes ansvarsområde förses med alla säkerhetsrelaterade uppdateringar.

UNDANTAG

Det finns tillfällen när det inte är möjligt att omedelbart följa alla anvisningar och regler i de gällande policydokumenten. Orsaken kan t.ex. vara:

- Den programvara som används kan för närvarande inte konfigureras för att uppfylla alla krav.
- Gamla system som ännu är i bruk kan inte uppfylla kraven, men förväntas ersättas inom en nära framtid.
- Kostnaden för att i tillräcklig grad uppfylla kraven är orimligt hög.

I sådana fall skall användaren ifråga skriftligen förklara varför kraven inte kan uppfyllas, redovisa en plan för hur detta kan ske inom rimlig tid och förelägga denna för BMCs styrelse för godkännande.