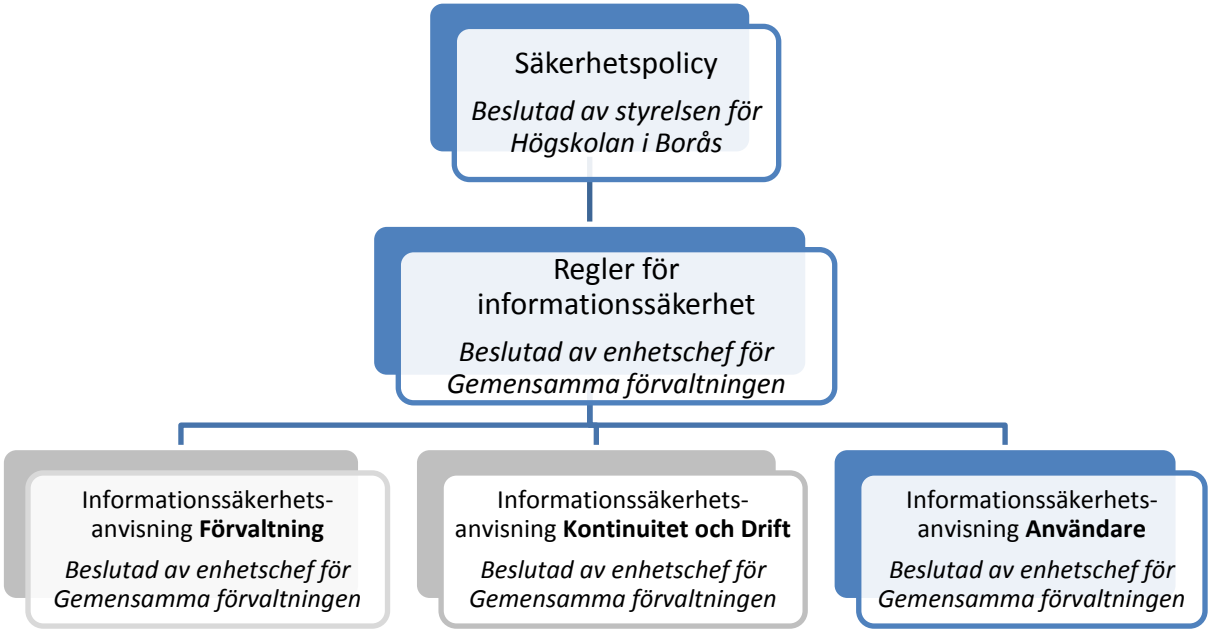
Informationssäkerhetsanvisningar – Användare

Beslutad av enhetschef för Gemensamma förvaltningen i enlighet med rektors beslut fattat den 16 februari 2010 (dnr 020-09-101). Gäller från och med den 12 december 2012 tillsvidare.

Ansvarig funktion för dokumentet: Högskolekansliet

Styrande dokument för informationssäkerhetsarbetet vid Högskolan i Borås:



Innehåll

1. Anvisningens roll i informationssäkerhetsarbetet

Säkerhetspolicyn redovisar högskolans viljeinriktning och mål för det övergripande säkerhetsarbetet, vari informationssäkerheten är en del.

Regler för informationssäkerhet redovisar roller och övergripande struktur för informationssäkerheten.

Informationssäkerhetsanvisning **Användare** redovisar hur en användare ska verka för att upprätthålla en god informationssäkerhet. Här framgår också högskolans regler för informationsklassning.

2. Användarens ansvar

Information är en viktig tillgång för högskolan. För att skydda denna krävs ett säkerhetsmedvetande hos alla medarbetare. Som användare har du därmed en del i ansvaret för säkerheten i informationshanteringen.

För stöd och hjälp när det gäller användningen av enskilda program avseende säkerhet ska du kontakta aktuell systemägare. Användaren bedömer själv när stöd och hjälp behöver inhämtas, men vid osäkerhet bör som huvudregel alltid kontakt tas med systemägaren.

3. Åtkomst till information

3.1 Behörighet

Högskolans informationssystem är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information. De behörigheter du blir tilldelad beror på dina arbetsuppgifter och avgörs i vissa fall av systemägare och i vissa fall av närmaste chef.

3.2 Inloggning

Innan du loggar in första gången får du ett lösenord för åtkomst till högskolans IT-miljö. Lösenordet ska bytas till ett personligt lösenord efter första inloggningen. Samma förfarande gäller för enskilda informationssystem som kräver lösenord för åtkomst.

Lösenord är strängt personliga och ska hanteras därefter. När du är inloggad och arbetar i systemen loggas dina aktiviteter. Detta görs för att vid behov kunna spåra obehörig åtkomst och skydda information samt undvika att oegentligheter inträffar.

Efter ett antal misslyckade försök att logga in spärras ditt konto. Ta då kontakt med IT-avdelningen.

3.3 Val av lösenord

För lösenord gäller att det ska:

- Vara minst åtta tecken långt
- Inte innehålla tecknen å, ä eller ö
- Inte vara egennamn eller enkla ord
- Bestå av en blandning av stora och små bokstäver, siffror och specialtecken

- Inte återanvändas
- Inte vara samma i olika system

3.4 Byte av lösenord
Lösenord ska bytas:

- Efter visst tidsintervall som bestäms av respektive systemägare
- Omedelbart om du misstänker att någon annan känner till det

4. Din arbetsplats

4.1 Utrustning
För den tekniska utrustning som du förfogar över – dator, smartphone etc. gäller:

- Fysiska ingrepp får endast utföras av IT-avdelningen
- Fel ska omedelbart anmälas till IT-avdelningen
- All installation och konfiguration får endast utföras av IT-avdelningen eller efter överenskommelse med IT-avdelning, exempel *Administratörsavtal.*

4.2 Programvaror
Programvaror ska godkännas och installeras av IT-avdelningen eller av IT-avdelningen anvisad/godkänd person.

Egna program får inte installeras i högskolans datorer utan tillstånd från IT-avdelningen.

Det är inte tillåtet att kopiera eller använda högskolans program utanför högskolans verksamhet, undantaget programvaror där hemanvändning reglerats i avtal med leverantör.

4.3 Avveckling av utrustning
Avveckling av utrustning ska alltid göras av eller i samråd med IT-avdelningen.

4.4 När du lämnar arbetsplatsen
När du tillfälligt lämnar utrustningen utan uppsikt ska du låsa den så att den inte kan nyttjas av obehörig.

När du lämnar utrustningen för längre perioder bör du logga ut och stänga av.

4.5 Lagring
Om du lagrar lokalt på din utrustning är du själv ansvarig för att säkerhetskopiera, i annat fall riskerar du att förlora informationen.

Om du använder datorer eller annan IT-utrustning utanför högskolan ska du tänka på att den kan utgöra en säkerhetsrisk, du får därför inte lagra sekretessbelagd eller för verksamheten känslig information på den.

5. Klassning och hantering av information

5.1 Allmänt

Informationssystem inom högskolan klassas utifrån den information som hanteras i respektive system. Klassning av ett informationssystem dokumenteras i det aktuella systemets förvaltnings-plan, vilken systemägaren ansvarar för. Klassning görs från aspekterna sekretess (konfidentialitet), riktighet och tillgänglighet. Med detta menas:

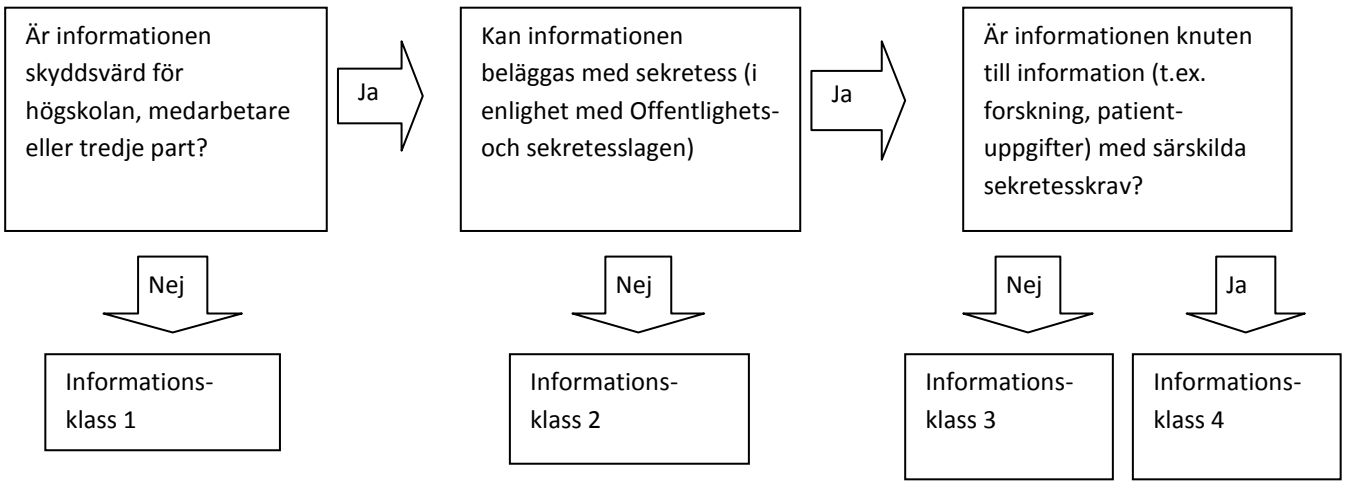
Sekretess	Att informationen skyddas från obehörig insyn
Riktighet:	Att informationen inte ändras på ett obehörigt sätt
Tillgänglighet:	Att informationen finns tillgänglig för rätt person vid rätt tillfälle

Tas information ut ur ett system och lagras på andra media eller används i annat sammanhang måste den klassas där den används och hanteras därefter.

När du ska hantera och spara information i IT-system ska du kontinuerligt klassa den utifrån ovan angivna aspekter. Det resultat du kommer fram till styr därefter din hantering av informationen.

Kravet på tillgänglighet beaktas huvudsakligen av systemägaren i samband med att förvaltningsplan för det enskilda systemet upprättas. Enskilda användare av systemet ska främst beakta kraven på riktighet och sekretess vad gäller det enskilda dokument denne upprättar.

5.2 Sekretess



5.2.1 Informationsklass 1

Informationen får lagras på lokal hårddisk. Informationen få även lagras på flyttbart medium utan restriktioner. Informationen får överföras elektroniskt utan kryptering.

Informationen får faxas samt sändas med post, såväl internt som externt.

5.2.2 Informationsklass 2

Informationen ska i första hand lagras på personlig hemkatalog och inte på arbetsstationens lokala hårddisk. Informationen får lagras på flyttbart medium utan restriktioner. Informationen får överföras elektroniskt utan kryptering.

Informationen får faxas under förutsättning av mottagarkontroll genomförs. Informationen får sändas via intern post under förutsättning att förslutet kuvert används i internpostkuvertet. Informationen få sändas externt via post.

5.2.3 Informationsklass 3

Informationen ska lagras på personlig hemkatalog.

Informationen får i undantagsfall lagras på lokal hårddisk under förutsättning att hela lagrings-mediet är krypterat samt att IT-systemet inte delar ut resurser. Informationen får lagras på flyttbart medium under förutsättning att det är krypterat samt att det hålls inlåst när det inte är under behörig uppsikt. Dessa medium får inte förflyttas utanför högskolans lokaler såvida det inte skickas till annan behörig mottagare. All elektronisk överföring av informationen ska vara krypterad.

Informationen får inte faxas och om det ska skickas med extern post ska postbefordran med REK och mottagningsbevis alternativt bud användas. Vid intern post ska förslutet kuvert i internpostkuvert användas.

Vid byte av hårddisk och/eller radering av informationen ska IT-avdelningen alltid kontaktas.

5.2.4 Informationsklass 4

Informationen ska lagras på en fristående server i isolerat nät och inte på lokal hårddisk. Servern ska vara placerad, separat inlåst, i ett godkänt serverrum. I det fall detta inte är möjligt ska informationen förvaras på en krypterad hårddisk samt förvaras inlåst i säkerhetsskåp när den inte är under behörig uppsikt. Bärbar dator låses in på motsvarande vis och särskilda rutiner för säkerhetskopiering upprättas.

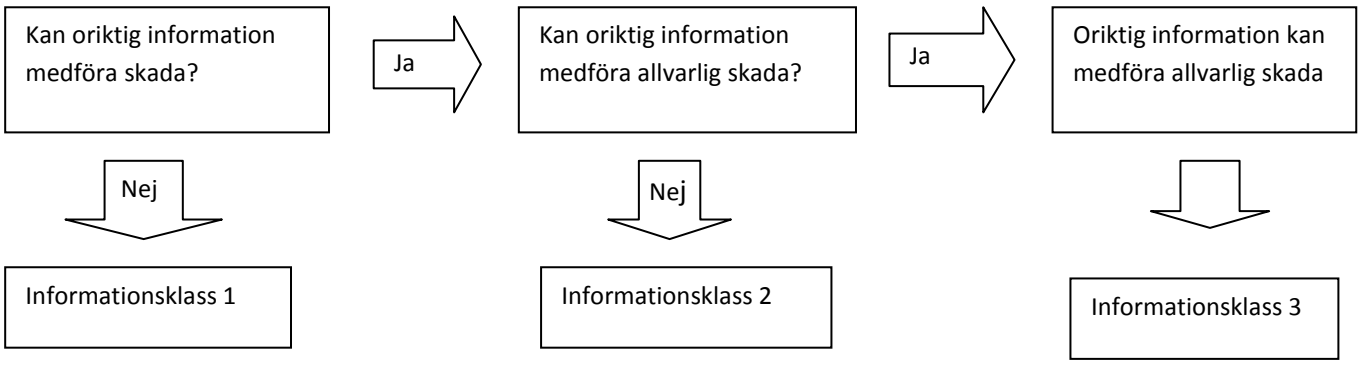
Informationen får förvaras på annat flyttbart medium under förutsättning att hela lagrings-mediet är krypterat samt att det förvaras inlåst i säkerhetsskåp när det inte är under behörig uppsikt. Dessa medium får inte förflyttas utanför högskolans lokaler såvida det inte skickas till annan behörig mottagare. All elektronisk överföring av informationen ska vara krypterad.

Informationen får inte faxas och om det ska skickas med extern post ska postbefordran med REK och mottagningsbevis alternativt bud användas. Informationen får inte sändas via intern post.

Vid byte av hårddisk och/eller radering av informationen ska IT-avdelningen alltid kontaktas.

5.3 Riktighet

Informationen ska vid informationsklassning även bedömas utifrån kravet på riktighet. Kravet på riktighet klassificeras mot nedanstående informationsklasser.



5.3.1 Informationsklass 1

Inga krav ställs på verifiering av riktigheten i informationen eller skydd mot förvanskning av informationen.

5.3.2 Informationsklass 2

Informationen ska vara spårbar och riktigheten ska kunna verifieras t.ex. genom signering eller logg.

5.3.3 Informationsklass 3

Varje inmatning eller förändring av informationen ska vara spårbar och riktigheten ska kunna verifieras t.ex. genom signering eller logg. Informationen ska förses med ett högt skydd mot oavsiktlig eller avsiktlig förändring och får endast hanteras i ett skyddat nät med ett anpassat behörighetskontrollsystem.

5.4 Tillgänglighet

Kravet på tillgänglighet ska uttryckas i tidstermer och i vilken utsträckning avbrott kan accepteras utifrån följande frågeställningar:

- Hur länge ska informationen finnas tillgänglig?
- Hur många timmar per dygn ska informationen vara tillgänglig?
- Vad är längsta acceptabla avbrott?
- Vilket antal avbrott per tidsenhet kan accepteras?
- Varifrån ska informationen vara tillgänglig?

6. Internet

När du använder Internet kan säkerheten i högskolans lokala nätverk påverkas i mycket hög grad beroende på ditt beteende. Högskolan förutsätter att den som surfar på internet endast besöker välrenommerade webbplatser. Tänk på att när du surfar på internet representerar du högskolan och lämnar spår efter dig i form av högskolans IP-adress.

Det är inte tillåtet att via internet titta eller lyssna på material av pornografiskt eller rasistisk karaktär. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning etc.) eller har anknytning till kriminell verksamhet.

I det fall det är motiverat för arbetet, t.ex. omvärldsanalyser, forskning m.m. att besöka sidor som normalt är förbjudna ska beslut om detta tas av närmaste chef. Du som användare ansvarar själv för att tillse att beslut om detta fattas innan du besöker dessa sidor.

7. E-post

Följande gäller avseende användning av e-post:

- Sekretessbelagd information får endast skickas i e-postsystemet under förutsättning att det krypteras
- E-postsystemet är ett arbetsverktyg och privat användning bör endast ske i begränsad omfattning (e-postmeddelanden av privat karaktär inkomna i högskolans e-postsystem är att betrakta som allmän handling och kan komma att lämnas ut om någon begär det)
- Samma regler för diarieföring gäller för e-post som för vanliga brev
- Om du misstänker att det kommit in virus via e-postsystemet ska du agera såsom beskrivs i avsnittet *Incidenter, virus m.m.*
- Det är inte tillåtet med automatisk vidarekoppling till annan e-postadress
- Ange alltid ämne i ämnesraden för meddelandet att klargöra för mottagaren vad denne kan förvänta sig för innehåll i e-posten
- Skriv inte någon känslig information i ämnesraden
- Kontrollera vilka som är medlemmar i sändlistor innan du använder dem annars finns risk för att känslig information når fel mottagare)
- Om du får hotelsebrev ska du spara brevet och omedelbart kontakta din chef
- Lämna aldrig ut kontouppgifter via e-post
- Öppna ej okända bilagor, tänk på virusrisken

8. Incidenter, virus m.m.

8.1 Allmänt

Högskolan rapporterar IT-incidenter till Sunet Cert.

Om du misstänker att du har drabbats av en IT-säkerhetsincident som t.ex. intrång på ditt konto, din dator eller motsvarande ska du:

- Notera när du senast var inne i IT-systemet
- Notera när du upptäckte incidenten
- Omedelbart anmäla förhållandet till IRT-funktionen (Incident Response Team) vid IT-avdelningen – www.hb.se/irt
- Dokumentera alla iakttagelser i samband med upptäckten och försöka fastställa om informationen har påverkats

Om du upptäcker andra fel och brister i de system du använder ska du rapportera dessa till IT-avdelningen.

8.2 Virus

Högskolan har programvaror för viruskontroll både i klienterna och i nätverket men kan ändå drabbas av effekter av s.k. skadlig kod. Om du misstänker att din dator innehåller virus ska du:

- Dra ur nätverkskabeln, men låta datorn stå på
- Omedelbart kontakta IT-avdelningen (OBS! anmälan måste ske per telefon eller besök, inte per e-post)

Om du får e-postmeddelanden med virusvarning kontakta omedelbart IT-avdelningen.

Var noga med att den kringutrustning du ansluter till din dator inte är smittat av virus och, i de fall det är möjligt, har ett uppdaterat antivirusprogram.

9. Avslutning av anställning

När du slutar din anställning ansvarar du för att:

- Rådgöra med din chef om vilket arbetsmaterial som ska sparas. Notera att det arbetsmaterial du framställt kan vara allmän handling och ska då bevaras hos högskolan
- Privat material (ej tjänsterelaterat) tas bort
- Informera din chef om vilka informationssystem du har behörighet till, denne ansvarar sedan för att behörigheterna tas bort