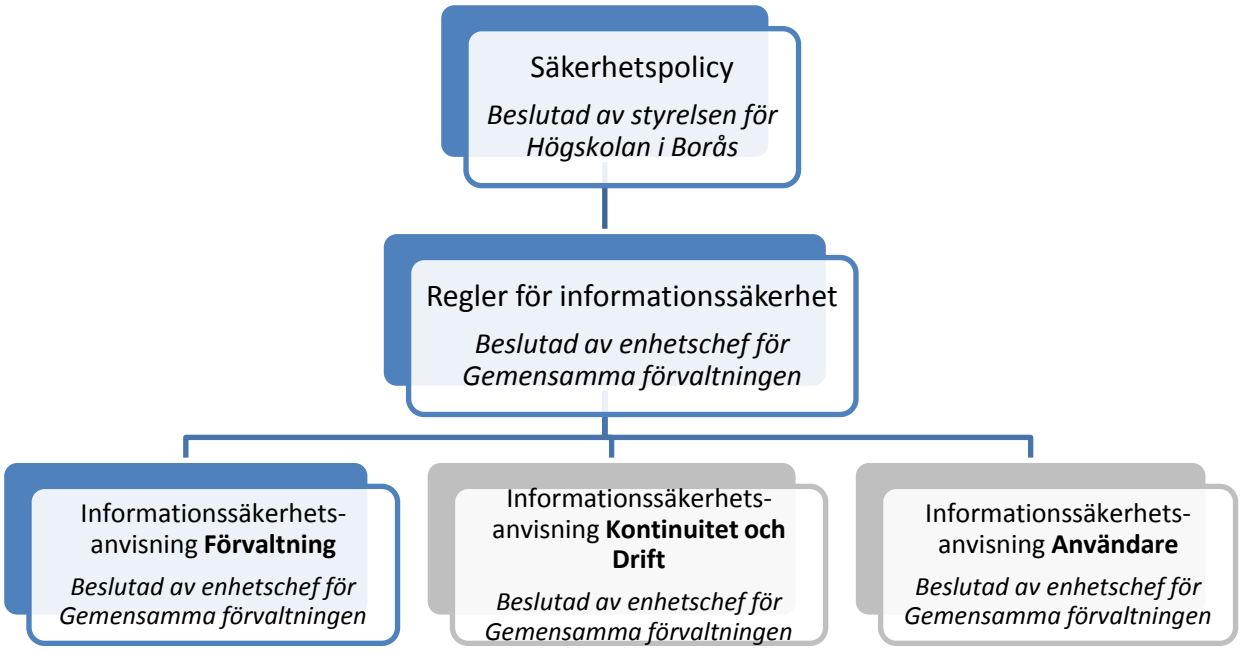
Informationssäkerhetsanvisningar – Förvaltning

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: IT-avdelningen

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. I *Informationssäkerhetsanvisning - Användare* framgår högskolans regler för informationsklassning.

Informationssäkerhetsanvisning **Förvaltning** redovisar:

- Det ansvar som ingår i de olika rollerna
- De regler som gäller för områden av särskild betydelse
- Regler för nyanskaffning, underhåll, förändrings- och incidenthantering

2. Organisation och ansvar

2.1 Ledningen

Ledningen fattar de avgörande besluten hur informationssäkerhetsarbetet ska bedrivas. Besluten ska framgå av den årliga verksamhetsplaneringen.

2.2 Informationssäkerhetssamordnaren

Informationssäkerhetssamordnaren stödjer arbetet med att uppnå säkerhetspolicyns mål avseende informationssäkerhet samt ansvara för analyser för de delar av IT-stödet som är gemensamma för hela verksamheten. Informationssäkerhetssamordnaren initierar och stödjer systemägarnas arbete med att genomföra enskilda systemsäkerhetsanalyser.

2.3 Systemförvaltningsmodell

Modellen styr generella frågor avseende anskaffning, drift, förvaltning och avveckling av informationshanteringsresurser. Inom ramen för detta ingår frågor som avser informationssäkerhet. Ansvar och roller såsom systemägare, systemförvaltare, driftsansvarig definieras i Högskolan i Borås systemförvaltningsmodell (dnr XX).

2.4 IT-chef

IT- chef är systemägare för det interna IT-nätverket och ansvarar för dess funktion. IT-chef ansvarar för att identifiera och analysera de delar som ingår i det interna IT-nätverket.

IT-chef ansvarar också för att *Informationssäkerhetsanvisning Kontinuitet och Drift* upprättas.

3. Regler och rutiner

3.1 Ansvar för tillgångar

Varje fysisk informationsbehandlingstillgång ska vara förtecknad och märkt med ett unikt nummer. Av en förteckning ska framgå var tillgångarna är placerade samt vem som ansvarar för tillgången. Omflyttning och överlåtelse av tillgång får inte ske utan samråd med den ansvarige.

3.2 Klassificering av information

Regler för klassning av information framgår av *Informationssäkerhetsanvisning Användare.*

3.3 Under anställningen

Information och utbildning av anställda ska omfatta:

- Informationssäkerhetens betydelse för verksamheten
- Innehållet i säkerhetspolicyn
- Informationssäkerhetsanvisning Användare

Nya användare ska informeras om högskolans regler för informationssäkerhet i samband med tilldelning av behörighet i nätverket.

Respektive systemägare ansvarar för att de användare som skall nyttja systemet har tillräckliga kunskaper avseende systemets säkerhetsregler.

3.4 Säkrade utrymmen

Känslig information från informationssystem ska lagras på resurser i datorhallar som ska vara försedda med kontrollsystem för in- och utpassering. Utrymmen med konsolutrustning ska vara låsta när de är obemannade. Utrymmen med kopplingspunkter ska vara låsta. Känslig information som inte hanteras i informationssystem ska förvaras i brandklassade säkerhetsskåp. Beslut ska tas av IT-chefen om och när tillträde till säkrade utrymmen tillåts.

3.5 Kontroll av utomstående tjänsteleverantör

Beställare av utomstående leverantörers tjänster ska följa upp och granska att säkerhets-överenskommelser följs.

3.6 Hantering av datamedia

Datamedia med sekretessbelagd information som ska avvecklas överlämnas till IT-enheten som hanterar avvecklingen.

3.7 Utbyte av information

Om media som innehåller känslig information måste transporteras fysiskt ska systemägare kontaktas för beslut om tillvägagångssätt.

3.8 Övervakning

Systemägaren beslutar om regler för användning och övervakning av systemets loggar.

3.9 Styrning av användares åtkomst

Systemägaren ansvarar för behörighet till respektive system enligt behörighetsrutiner som definierats i förvaltningsplanen.

3.10 Styrning av åtkomst till nätverk

IT-chefen ansvarar för att reglera åtkomst till högskolans fasta och trådlösa nätverk.

IT-chefen ska ansvara för

- att en översikt av säkerhetsarkitekturer för interna nätverket och kommunikations-anslutningar upprättas,
- administrationen av brandväggen samt besluta om vad som ska loggas i den, vem som ansvarar för uppföljningen av loggarna, hur ofta uppföljning ska ske och hur länge loggarna ska sparas.

3.11 Styrning av åtkomst till operativsystem

IT-chefen beslutar i vilken utsträckning användning av administrationsverktyg eller system-hjälpmedel som kan förbigå system- och tillämpningsspärrar ska användas. För att erhålla administratörsrättigheter krävs undertecknat administratörsavtal.

3.12 Mobil datoranvändning och distansarbete

Systemägare beslutar om hur och på vilket sätt ett informationssystems information ska vara åtkomligt på distans.

3.13 Säkerhetskrav vid nyanskaffning av informationssystem

Inför nyanskaffning och införande av ett informationssystem ansvarar verksamhetsansvarig chef för att en införandeplan upprättas.

Denna plan ska minst omfatta:

- beskrivning av behov och mål med anskaffningen
- en systemsäkerhetsanalys som syftar till att klarlägga säkerhetskraven på det system som planeras införas
- integrationskrav med andra system
- krav på test
- tidplan
- personella och ekonomiska resurser
- klarlägga behov av användarutbildning
- krav på acceptans mot leverantören

Ansvarig för nyanskaffningsprojekt förbereder överlämnandet från test och utveckling till drift och förvaltning tillsammans med den tilltänkte systemägaren i samråd med IT-chef.

3.14 Säkerhet i utvecklings- och underhållsprocesser

Förslag om önskemål på förändringar i systemet hanteras enligt rutiner beskrivna i förvaltningsobjektets förvaltningsplan.

3.15 Hantering av informationssäkerhetsincidenter och förbättringar

Vid misstanke om intrång eller andra incidenter ska användare agera enligt *Informationssäkerhetsanvisning Användare*.

Informationssäkerhetssamordnaren ska sammanställa och rapportera till ledningen:

- intrång och försök till intrång,
- brott mot lagstiftning och internt regelverk,
- incidenter som orsakar eller skulle kunna orsaka betydande avbrott och störningar,
- konsekvenser och förslag till åtgärder efter intrång.

3.16 Efterlevnad av rättsliga krav

Anvisningar för skydd av register och handlingar ska följas, se *Informationssäkerhetsanvisning Användare.*