ANVISNING **Gäller från och med**
2015-01-01

Informationsklassificering för KTH

Riktlinje

Gäller fr.o.m. 2015-01-01

Riktlinjen grundar sig på:

- Rektors beslut Dnr **V-2014-0090**

Riktlinjen beskriver hur information skall klassificeras vid KTH.

Ändamål och inriktning

KTH:s verksamhetsinformation är en värdefull resurs såväl för allmänheten som för den egna verksamheten. Klassificeringen är ett hjälpmedel för att korrekt bedöma informationens värde och känslighet så att varje informationstillgång kan omges med rätt skydd.

Anvisningar och hanteringsregler

Anvisningar för hur information tillhörig olika klasser ska hanteras finns i de hanteringsregler som hör till denna riktlinje. Anvisningar kan också finnas i andra dokument som behandlar särskilda hanteringsregler för information, till exempel anvisningar för kontinuitetsplanering.

Regelbunden revidering

Denna riktlinje och de hanteringsregler och andra anvisningar som hör till riktlinjen skall revideras årligen. Ansvaret för att revidera detta dokument åvilar informationssäkerhetssamordnaren. Ansvaret för revidering av hanteringsreglerna åligger respektive dokumentägare, men stöd kan fås av informationssäkerhetssamordnaren samt arkivfunktionen.

Klassificering av information

Vad som klassificeras

Det är i första hand information som ska klassificeras. I normalfallet klassificeras "information som hör samman" som en enhet.

"Information som hör samman" kan till exempel vara information i ett visst dokument eller skrift. I många fall är det den tekniska lagringen av informationen som avgör vad som "hör samman". Klassificeringen kan till exempel avse en enskild post, ett IT-system eller ett arbetssätt som innefattar både administrativa rutiner och stödsystem.

För en samling av information är det den högsta klassificeringen för någon av de ingående delarna som tillämpas. När det gäller informationsbärare såsom tekniska system och liknande så styrs klassificeringen normalt av den information som hanteras.

Det är av vikt att klassningen sker i ett tidigt skede och omfattar både informationen och dess bärare så att den inte hanteras felaktigt. Ett exempel är att man vid framtagande av ett konfidentiellt dokument även måste skydda arbetsmaterial, möten, telefonsamtal etc. så att inte obehöriga kan ta del av informationen.

Kategorier

Information klassificeras i följande kategorier, dvs. avseende följande egenskaper hos informationen:

S: Åtkomstskydd (Sekretess, eng. Confidentiality), behov av skydd mot oavsiktlig eller otillåten/obehörig åtkomst.

R: Riktighet (eng. Integrity), behov av skydd mot oavsiktlig eller otillåten/obehörig förändring eller förstöring.

T: Tillgänglighet (eng. Availability), behov av tillgänglighet hos informationen (åtkomst till informationen) för behöriga användare. Tillgänglighet avser tillgänglighet till informationen i normalfallet, t.ex. vid en normal driftsituation. Tillgänglighet kan i andra sammanhang ha en mängd betydelser (tillgänglighet för funktionsnedsatta, teknisk tillgänglighet etc.), men här avses möjligheten att åtkomma och nyttja informationen på avsett sätt.

I kraven för tillgänglighet ingår även krav avseende **kontinuitetsplanering** för åtkomst/användning av informationen (eng. Contingency Planning Requirements).

Y: Ytterligare krav, som måste ställas för skyddet av informationen, och som inte ryms inom kategorierna ovan och som därför måste skrivas i klartext (eng. Specific Requirements).

Grunder för klassificeringen

Grunden för klassificeringen är de konsekvenser som kan uppkomma vid brister i skyddet av informationen avseende de olika kategorierna ovan. Konsekvenserna ska bedömas sammantaget för:

- KTH som myndighet
- anställda och studerande vid KTH samt andra personer associerade med KTH
- samarbetspartners och finansiärer till KTH
- allmänheten
- samhället i övrigt

I all bedömning av skyddsåtgärder och konsekvenser ska människors liv, hälsa och integritet beaktas först.

Om det finns tydligt formulerade klassificeringar i lagar eller regler ska dessa utnyttjas i klassificeringen. Ett exempel är kraven på sekretess i Offentlighets- och sekretesslagen (2009:400), förkortad OSL.

I det följande avses med **konsekvenser** samtliga konsekvenser enligt ovan.

Indelningen i klasser

Klassificeringen sker för klasserna S, R och T med siffror, i en stigande skala, så att noll (0) avser det lägsta behovet av skydd/motsv. Klassificering kan också ske, om så behövs, med beteckningar i klartext för särskilda krav i kategorin Y.

Information som uppfyller kraven för flera klasser (t.ex. S0, S1 och S2) klassificeras alltid som den högsta av dessa klasser (dvs i detta fall S2).

Exempel på särskilda krav som kan behöva föras in i klassificeringen är Y:Extern tidsstämpel, eller Y:Juridiskt giltig signatur.

Exempel på klassificering är S1;R2;T2 eller S2;R2;T2;Y:Juridiskt giltig signatur.

Basnivå av skydd

Vid KTH ska **all information normalt skyddas minst motsvarande basnivån**, dvs. klass ett (1). Detta kan också uttryckas som att klass ett är underförstådd (eng. Default) om ingen annan klass anges.

Juridiskt motsvarar klass ett (1) kraven på skydd för uppgift i arbetsmaterial eller allmän handling vid en myndighet. Om det finns krav på sekretess e.d. för informationen, eller om informationen behövs för t.ex. brådskande handläggning, bör informationen ges högre klass i en eller flera kategorier.

Klass noll (0) – inga skyddsbehov

För varje kategori finns en klass noll (0). Om information klassificeras som klass noll i en kategori innebär det att det inte finns några krav på skydd inom aktuell kategori.

S0: Inga skydd mot åtkomst behövs.

R0: Inga skydd mot förändring eller förstöring behövs (dvs. det får inga konsekvenser om informationen förändras eller försvinner).

T0: Inga krav på åtkomst finns (dvs. det får inga konsekvenser om informationen inte kan åtkommas), och det finns heller inga krav på kontinuitetsplanering.

Kategori S (åtkomstskydd)

Klass S1 – grundläggande krav på åtkomstskydd

Information ska klassas som S1 om det endast blir begränsade konsekvenser för KTH eller enskilda om informationen åtkoms av obehöriga.

Information tillhörig klass S1 ska omfattas av *grundläggande skydd* mot obehörig åtkomst. Informationen ska bara kunna åtkommas av i förväg utpekade personer, eller av personer som dessa avsiktligt låter komma åt denna. Webbpublicering är ett exempel på delegation av åtkomsträttigheten till allmänheten, som kan förekomma för information tillhörig klass S1.

Klass S2 – höga krav på åtkomstskydd

Information klassas som tillhörig S2 om den har sekretesskydd i OSL eller annan lag eller regel, eller om den omfattar information som i Personuppgiftslagen (1998:204) definieras som känsliga personuppgifter (bl.a. information om hälsa och sjukdom).

Information tillhörig klass S2 ska ha ett *högt skydd* mot obehörig åtkomst.

Klass S3 – mycket höga krav på åtkomstskydd

Information klassas som tillhörig S3 om det kan uppstå mycket stora konsekvenser om informationen åtkoms av obehöriga. Information tillhörig S3 har i de flesta fall högt sekretesskydd i OSL eller i annan lag eller regel.

Information tillhörig klass S3 ska ha ett *mycket högt skydd* mot obehörig åtkomst.

Klass S4 – särskilt höga krav på åtkomstskydd

Information klassas som tillhörig S4 om det skulle kunna uppstå extremt stora konsekvenser om informationen åtkoms av obehöriga. Information klassas också som tillhörig S4 om den är skyddad av försvarssekretess enligt OSL 15 kap 2 § eller är skyddad av utrikessekretess enligt OSL 15 kap 1 §, eller har motsvarande eller högre sekretess enligt lag eller regel.

Information tillhörig klass S4 ska ha ett *kvalificerat skydd* mot obehörig åtkomst. I de flesta fall finns *externa hanteringsregler* i avtal och/eller i lagar eller regler som måste tillämpas för information tillhörig S4.

Kategori R (riktighet)

Klass R1 – grundläggande krav på riktighet

Information ska klassas som R1 om det endast blir begränsade konsekvenser för KTH eller enskilda om den förändras oavsiktligt eller av obehöriga. Informationen ska bara kunna ändras av i förväg utpekade personer, eller av personer som dessa avsiktligt låter ändra denna.

För information tillhörig klass R1 gäller *grundläggande krav* på spårbarhet och skydd mot obehörig förändring.

Klass R2 – höga krav på riktighet

Information klassificeras som tillhörande R2 om det skulle innebära stora konsekvenser om informationen oavsiktligt eller otillåtet skulle förändras eller förstöras.

För information tillhörig klass R2 gäller att *höga krav* på spårbarhet och skydd mot obehörig förändring ska vara uppfyllda..

Klass R3 – mycket höga krav på riktighet

Information klassificeras som tillhörande R3 om det skulle innebära mycket stora konsekvenser om den oavsiktligt eller otillåtet skulle förändras eller förstöras.

För information tillhörig klass R3 gäller att *mycket höga krav på* spårbarhet och skydd mot obehörig förändring ska vara uppfyllda.

Kategori T (tillgänglighet)

Vid bedömningen av skyddsbehov avseende tillgängligheten för information tillhörig de olika klasserna nedan ska behovet av robusthet beaktas. Det innebär bland annat att åtgärder för att säkra åtkomsten inte ska försämra skyddet avseende sekretess och riktighet. Vid utformning av kontinuitetsplaneringen ska allmänt accepterade principer för force majeure beaktas. Tillgänglighet mäts oftast i tid, men även rum, format och tolkning behöver ofta beaktas.

Principer för bedömning av tillgänglighet och avbrottsplanering

Kraven på tillgänglighet, liksom kraven på kontinuitetsplanering, avser, om inte annat sägs, tillgänglighet hos informationen vid KTH. Om informationen är avsedd att vara tillgänglig vid flertalet av KTH:s arbetsplatser, avses tillgängligheten vid en arbetsplats vid KTH:s campus.

Klass T1 – grundläggande krav på tillgänglighet

Informationen ska vara *omedelbart tillgänglig* för den som har rätt att utnyttja den. Kravet på omedelbar tillgänglighet kan dock *begränsas* av hur den är förvarad eller lagrad, och om det krävs bearbetning för att ta fram den. Informationen ska vara tillgänglig åtminstone under användarnas förväntade arbetstid.

Information ska klassas som T1 om det endast blir begränsade konsekvenser för KTH eller enskilda om informationen inte är tillgänglig då den behövs.

Utöver när de beror på lagringsformen, kan enstaka fördröjningar på upp till några timmar accepteras, dock högst två gånger i månaden, exempelvis beroende på oväntade fel eller planerad service.

Tillgängligheten avser informationen som sådan, i den form den finns lagrad eller representerad vid lagringen. Informationen ska inom ett dygn kunna presenteras i det format och den representation som den efterfrågas i, om formatet och representationen är rimliga.

Kontinuitetsplanering för klass T1

Information tillhörig klass T1 ska *alltid kunna återställas* oavsett händelse. Inga tidsgränser för återställandet eller prioritering av återställande åtgärder behövs.

Klass T2 – höga krav på tillgänglighet

Information klassas som tillhörig T2 om den behöver ha hög tillgänglighet, och om det kan uppstå stora konsekvenser om den inte är tillgänglig som avsett.

Med hög tillgänglighet avses att informationen ska kunna åtkommas inom *enstaka minuter* dygnet runt alla dagar på året. Endast enstaka, planerade avbrott per år i möjligheterna till åtkomst får förekomma. Tillgängligheten avser informationen i efterfrågat format och representation.

Kontinuitetsplanering för klass T2

Återställande av åtkomsten till information tillhörig klass T2 ska vara prioriterad över information tillhörig T1 eller T0. Informationen ska, oavsett händelse, kunna åtkommas inom *några dygn*. Tekniska system för åtkomst till information tillhörig klass T2 ska vara tilldelade en prioritetsordning för återställande, och ska alltid kunna återställas till normal drift inom några dygn.

Klass T3 – mycket höga krav på tillgänglighet

Information klassas som tillhörig T3 om informationen behöver vara tillgänglig med mycket hög tillgänglighet, och om det kan uppstå mycket stora konsekvenser om informationen inte är tillgänglig som avsett.

Med mycket hög tillgänglighet avses att informationen ska kunna åtkommas inom *enstaka sekunder* dygnet runt alla dagar på året. Inga avbrott i möjligheterna till åtkomst ska normalt förekomma. Tillgängligheten avser informationen i efterfrågat format och representation.

Kontinuitetsplanering för klass T3

Åtkomsten till information tillhörig klass T3 ska vara prioriterad över information tillhörig T2 eller lägre. Informationen skall, oavsett händelse, kunna åtkommas inom *enstaka minuter*. Tekniska system för åtkomst till information tillhörig klass T3 ska normalt vara dubblerade och geografiskt separerade, eller på annat sätt vara utformade för kontinuerlig drift och tillhandahållande av information oavsett störning.

Klass T4 – extremt höga krav på tillgänglighet

Information klassas som tillhörig T4 om informationen behöver vara tillgänglig med extremt hög tillgänglighet, och om det kan uppstå mycket stora konsekvenser för KTH eller enskilda om informationen inte är tillgänglig som avsett.

Med mycket hög tillgänglighet avses att informationen ska kunna åtkommas inom *bråkdelar av en sekund* dygnet runt alla dagar på året. Inga avbrott i möjligheterna till åtkomst ska förekomma.

Tillgängligheten avser informationen i efterfrågat format och representation.

Kontinuitetsplanering för klass T4

Åtkomsten till information tillhörig klass T4 ska vara prioriterad över information tillhörig T3 eller lägre. Informationen ska, oavsett händelse, kunna åtkommas inom enstaka sekunder. För tekniska system för åtkomst till information tillhörig klass T4 behöver normalt *mycket kvalificerade åtgärder* vidtas för att säkerställa möjligheterna till åtkomst.

Referenser:

- Offentlighets- och sekretesslagen (2009:400)
- Arkivlagen (1990:782)
- MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10).
- Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (RA-FS 2009:1)