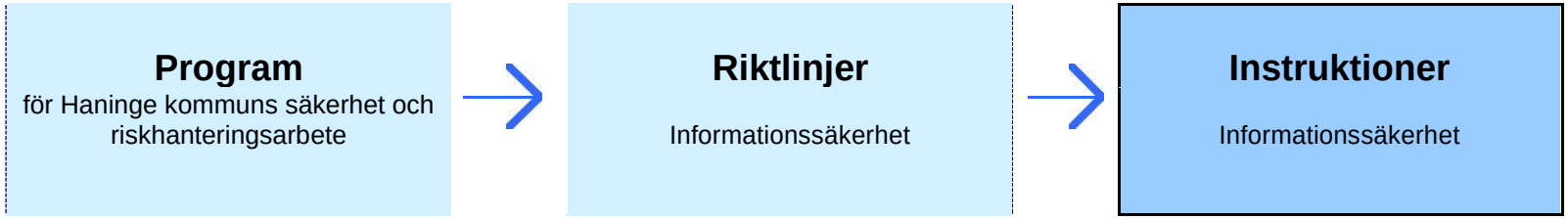
Haninge kommun

Informationsklassning – Instruktion

Genomförande modell för Haninge kommuns verksamheter



Dokumenttyp Instruktion/rutin	Dokumentnamn Informationsklassning	Fastställd/datum	Gäller från/datum
Upprättad av Säkerhet/KSF	Ansvarig avdelning och dokumentförvaltare (namn) Kommunstyrelseförvaltningen/kansliet Bo Jensen	Reviderad 2022-01-11	
Dokumentinformation Instruktionen för informationsklassning kopplat till Haninge kommuns program för säkerhet och riskhanteringsarbete 2019-2022 (KF 2020-10-12)		Diarienummer 2022-00227	Version 1.2

1. Inledning – informationsklassning

Informationsklassning är en delprocess i det administrativa arbetet med informationssäkerhet och utgör underlag för kunskapsuppbyggnad om hur information ska hanteras och behandlas. För att kunna bedöma rätt skyddsnivå för sin information måste man veta vilken sådan som är skyddsvärd och varför den är det. Kommunens informationstillgångar ska klassificeras så att de kan skyddas i enlighet med verksamhetens krav och även legala sådana. De ska också klassificeras utifrån hur stor betydelse informationen har för verksamheten och hur känslig den är för den enskildes personliga integritet. Aspekterna riktighet, tillgänglighet, spårbarhet och konfidentialitet (sekretess) är centrala i klassningsarbetet. Resultatet av klassningen vägleder i arbetet med att specificera vilka organisatoriska (regler) och tekniska åtgärder som behöver vidtas för att kunna skydda informationstillgångar/system.

Konfidentialitet (sekretess)	Att informationen inte tillgängliggörs eller delges obehöriga
Riktighet	Att den skyddas mot oönskad och obehörig förändring eller förstörelse
Spårbarhet	Att i efterhand kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt eller användare (vem, vad, när)
Tillgänglighet	Att information är tillgänglig i förväntad utsträckning och inom önskad tid
Integritet	Att hänsyn och åtgärder har tagits för att säkerställa integritet och rättigheter för de som är registrerade

Verksamhetsansvariga på samtliga nivåer i kommunen är ansvariga för att information inom det egna verksamhetsområdet hanteras på ett korrekt sätt och ges ett tillfredsställande skydd. Det gäller oavsett om informationen hanteras elektroniskt eller manuellt. Med det ansvaret följer även att bedöma informationens skyddsbehov, dvs. klassa informationen.

En informationsklassnings hållbarhet är kortvarig eftersom informationen fortlöpande förändras. Därför bör informationen klassas årligen eller oftare vid behov.

1.1 Koppling till andra styrdokument

Instruktionen för informationsklassning har koppling till Haninge kommuns program för risk och säkerhetsarbete och tillhörande riktlinjer.

1. Inledning – Informationsklassning

Instruktion är framtagen i syfte att vägleda i genomförandet av informationsklassning inom Haninge kommuns verksamheter. Instruktionen utgör kommunmodell för informationsklassning. Genom det uppnås ett likartat arbetssätt som blir igenkännande för ansvariga och nyckelpersoner. Det underlättar uppföljning genom det interna kontrollsystemet och bidrar till utveckling av informationsklassningsarbetet genom utvärderingar och erfarenheter.

Instruktionen för klassning av informationstillgångar bygger på MSB: s rekommendationer och SKL: s klassningsmodell KLASSA som båda utgår från SS-ISO/IEC 27000 standarder för informationssäkerhet.

2. Genomförande

Här beskrivs flödet för de uppgifter som ingår i informationsklassningsarbetet.

Identifiera legala krav	Med utgångspunkt från de exempel på lagstiftningar som är beskrivna i instruktionen bedöms om något legalt krav påverkar hur information hanteras. Saknas någon lagstiftning ska den läggas till i listan. De lagar som är aktuella ska markeras i kryssrutorna.
Identifiera interna krav	Utifrån frågeställningarna om interna krav bedöms informationens betydelse för verksamhetens möjligheter att leverera de åtaganden man har till uppgift att göra.
Identifiera skyddsnivåer	De fyra centrala begreppen ska här värderas ur ett skyddsperspektiv. Bedömningen görs genom att välja grön, gul eller röd nivå. Som stöd för bedömningen finns för varje nivå en konsekvensbeskrivning. Ytterligare stöd för bedömning finns i anslutning till varje begrepp.
Sammanställning	I det här avslutande avsnittet sammanställs de resultat som framkommit av att identifiera legala och interna krav samt skyddsnivåer. Resultatet ska sedan syfta till förståelse om att skyddsnivåer (organisatoriska och tekniska) kan behöva vidtas.

3. Identifiering av krav

För att kunna klassificera informationstillgångar måste man förstå vilka krav som ställs på respektive tillgång. Arbetet med att hitta kraven kan delas upp på *legala krav* som kommer från avtal, lagar och förordningar, och *interna krav* som verksamheten ställer för att uppnå sina mål. Nedan beskrivna lagstiftning påverkar i någon form kommunens klassningsarbete. Med utgångspunkt från dessa exempel kan vid behov tillägg göras med ytterligare specifik lagstiftning.

3.1 Legala krav

Tryckfrihetsordningen (SFS 1946:105)	Om allmänna handlingars offentlighet. ”Till främjande av ett fritt meningsutbyte och en allsidig upplysning ska varje svensk medborgare ha rätt att taga del av allmänna handlingar”	☐
Offentlighets- och sekretess-lagen. (SFS 2009:400)	”En uppgift för vilken sekretess gäller enligt denna lag får inte röjas för enskilda eller för andra myndigheter, om inte annat anges i denna lag eller förordning som denna lag hänvisar till”	☐
Dataskyddsförordningen Artikel 32	Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning , sammanhang och ändamål samt riskerna , av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken	☐
Arkivlagen (SFS 1990:782, 6§)	I arkivvården ingår att myndigheten ska organisera arkivet på ett sådant sätt att rätten att ta del av allmänna handlingar underlättas, upprätta dels en arkivbeskrivning som ger information om vilka slag av handlingar som kan finnas i myndighetens arkiv och hur arkivet är organiserat, dels en systematisk arkivförteckning skydda arkivet mot förstörelse, skada, tillgrepp och obehörig åtkomst avgränsa arkivet genom att fastställa vilka handlingar som skall vara arkivhandlingar, och verkställa föreskriven gallring i arkivet.	☐
Säkerhetsskyddslagen (SFS 2018:585) 2kap 1§	Den som till någon del bedriver säkerhetskänslig verksamhet (verksamhetsutövare) ska utreda behovet av säkerhetsskydd (säkerhetsskyddsanalys). Säkerhetsskyddsanalysen ska dokumenteras. Med utgångspunkt i analysen ska verksamhetsutövaren planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.	☐

3.2 Interna krav

De interna kraven för att skydda information utgår från verksamhetens målsättning och ambition i leveransen av det specificerade kommunala uppdraget. För att systematiskt identifiera och dokumentera de interna kraven kan följande frågeställningar vara till stöd.

Vilken nytta har verksamheten av informationen	Konsekvens om informationen når obehöriga
Konsekvens om informationen riktighet är felaktig eller inaktuell	**Konsekvens om informationen inte är tillräckligt tillgänglig**

4. Identifiering av skyddsnivå

4.1 Konfidentialitet (sekretess) och integritet – att informationen kan behöva åtkomst begränsas		
Klass 1	Röjande av uppgifter medför **ingen, försumbar** eller **måttlig skada**. Systemet innehåller endast allmänna offentliga handlingar och är inte skyddsvärd. Informationen är avsedd för bred spridning/publicitet och innehåller inte personuppgifter. Den enskilde kan själv ansvara för riktigheten av inmatade uppgifter.	☐
Klass 2	Röjande av uppgifterna kan medföra **betydande skada**. Systemet innehåller arbetshandlingar eller allmänna handlingar som kan bli föremål för sekretess enligt OSL. Information avsedd för internt bruk eller innehåller känsliga personuppgifter enligt GDPR.	☐
Klass 3	Röjande av uppgifterna kan medföra **allvarlig skada**. Systemet innehåller information som är föremål för sekretess enligt OSL, känsliga personuppgifter, andra områdesspecifika lagrum eller tystnadsplikt.	☐

Exempel på åtgärder som stöd för bedömning vid klassning av - konfidentialitet (sekretess)

Klass 1	• Informationen får lagras på datorns lokala hårddisk • Informationen får även lagras på flyttbart medium utan restriktioner • Informationen får överföras elektroniskt utan kryptering • Informationen oavsett form kan förflyttas utanför verksamhetens lokaler vid exempelvis distansarbeten eller möten
Klass 2	• Informationen ska lagras på central server och inte på den lokala hårddisken • Informationen får även lagras på flyttbart medium utan restriktioner • Informationen får överföras elektroniskt utan kryptering • Informationen får skickas under förutsättning att mottagarkontroll sker • Vid försändning med internpost skall förslutet kuvert användas • Normal extern posthantering får användas • Informationen ska utanför verksamhetens lokaler alltid vara under uppsikt eller krypterad
Klass 3	• Informationen ska lagras på server i kommunens skyddade nät • All elektronisk överföring ska vara krypterad • Informationen får inte faxas • Extern postbefordran ska ske rekommenderat och mottagningsbevis eller bud ska användas • Vid försändning internt ska förslutna kuvert användas • Slutanvänd hårddisk/program ska förstöras mekaniskt alternativt överskrivas så att lagrad information inte kan återskapas

4.2 Riktighet – att informationen ska vara tillförlitlig, korrekt och fullständig

Klass 1	Information som obehörigen eller av misstag har ändrats medför **ingen, försumbar** eller **måttlig skada**. Systemet innehåller uppgifter som med begränsad insats kan återställas. Förändringarna bedöms inte leda till negativ påverkan för verksamheten eller skadeståndsanspråk.	☐
Klass 2	Information som obehörigen eller av misstag har ändrats medför **betydande skada**. Systemet ingår i myndighetsutövningen eller innehåller uppgifter som omfattas av lagrum där riktighetskrav anges. Förändringar av uppgifter bedöms kunna leda till negativ publicitet för verksamheten eller skadeståndsanspråk.	☐
Klass 3	Information som obehörigen eller av misstag har ändrats medför **allvarlig skada**. Informationen innehåller uppgifter där hanteringen styrs av specifika lagparagrafer, känsliga personuppgifter eller hälso- o sjukvård. Förändringar av uppgifter bedöms leda till allvarlig påverkan för egen eller annan organisation eller för enskild individ och kan sannolikt leda till skadeståndsanspråk.	☐

Exempel på åtgärder som stöd för bedömning vid klassning av - konfidentialitet (sekretess)

Klass 1	• Inga krav ställs på verifieringen av riktigheten i informationen eller skydd mot förvanskning av informationen
Klass 2	• Informationens riktighet skall kunna verifieras genom signering eller annan loggning
Klass 3	• Informationen skall förses med skydd mot oavsiktlig eller avsiktlig förändring • Informationen får endast hanteras i ett skyddat nät med ett anpassat behörighetskontrollsystem

4.3 Tillgänglighet – att informationen kan användas i förväntad utsträckning av rätt person med rätt behörighet

Klass 1	Ett avbrott medför **ingen, försumbar** eller **måttlig skada**. Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas endast i begränsad omfattning av otillgänglighet till systemet. Systemet kan vara otillgängligt i ett par dygn med måttlig inverkan på verksamheten	☐
Klass 2	Ett avbrott medför **betydande skada.** Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas i betydande omfattning av otillgänglighet i systemet. Begränsad möjlighet för medborgare att använda e-tjänster ställer på sikt krav på bemötande från verksamheten.	☐
Klass 3	Ett avbrott medför **allvarlig skada**. Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas i allvarlig omfattning av otillgänglighet i systemet.	☐

Exempel på åtgärder som stöd för bedömning vid klassning av - tillgänglighet

Klass 1	• Inga krav ställs på att verifiera acceptabla avbrottstider • Informationen är publik
Klass 2	• Avbrottstider på upp till något dygn kan accepteras, dock inte i återkommande intervaller • Reservrutiner ska finnas och kan tas i bruk inom ett par timmar • E-tjänster kan ligga nere max 3 arbetsdagar • Behörighetsregler/kontroll för personal och medborgare ska finnas
Klass 3	• Avbrottstider på några timmar kan accepteras, dock inte i återkommande intervaller • Reservrutiner ska finnas och kunna tas i bruk omgående • E-tjänster kan ligga nere några timmar • Informationen ska vara möjlig att nå från distansarbetsplats eller annan extern tillfällig plats

4.4 Spårbarhet – att specifika aktiviteter som rör informationen kan spåras		
Klass 1	Att spårbarhet saknas medför endast **ingen, försumbar** eller **måttlig skada**. Möjligheten att härleda vad som har hänt i systemet vid förändringar av uppgifter, incident eller säkerhetsincident bedöms vara oviktigt	☐
Klass 2	Att spårbarhet saknas medför **betydande skada**. Möjligheten att härleda vad som har hänt i systemet vid förändringar, incident eller säkerhetsincident bedöms vara viktigt. Spårbarhet ska finnas för att påvisa på vilket sätt information har behandlats i systemet och av vem.	☐
Klass 3	Att spårbarhet saknas medför **allvarlig skada**. Möjligheten att härleda vad som har hänt i systemet vid förändringar, incident eller säkerhetsincident bedöms vara mycket viktigt. Spårbarhet ska finnas för alla specificerade händelser i systemet.	☐

Exempel på åtgärder som stöd för bedömning vid klassning av - tillgänglighet

Klass 1	• Inga krav ställs på spårbarhet av informationen
Klass 2	• Vid behov ska det vara möjligt att i efterhand kunna härleda specifika aktiviteter eller händelser. Vem har tagit del av informationen, vilka förändringar som gjorts och av vem
Klass 3	• Vid varje inmatning eller förändring av informationen ska det vara möjligt att i efterhand kunna härleda specifika aktiviteter eller händelser

5. Sammanställning informationsklassning

Informationstillgång/system	Informationsägare	Datum för analys
Förvaltare av tillgång/system	Ansvarig för genomförd analys	

Legala krav (3.1)		Interna krav (3.2)	
Tryckfrihetsordningen	☐	Behov att identifiera acceptabla avbrottstider	☐
Offentlighet- och sekretesslagen	☐	Behov att identifiera kritiska beroenden	☐
Dataskyddsförordningen	☐	Behov av hanteringsregler (sekretess)	☐
Säkerhetsskyddslagen	☐	Behov av reservrutiner	☐
Arkivlagen	☐	Behov av behörighetsbegränsningar	☐
Annat _____	☐	Behov av tekniska skyddslösningar	☐
Annat _____	☐	Annat _____	☐

Klassificera *sekretess* och integritet (4.1)		
Klass 1	Inga särskilda skyddsåtgärder krävs	☐
Klass 2	Organisatoriska skyddsåtgärder krävs	☐
Klass 3	Organisatoriska och tekniska skyddsåtgärder krävs	☐

Klassificera *riktighet* (4.2)		
Klass 1	Inga särskilda skyddsåtgärder krävs	☐
Klass 2	Organisatoriska skyddsåtgärder krävs	☐
Klass 3	Organisatoriska och tekniska skyddsåtgärder krävs	☐

Klassificera *tillgänglighet* (4.3)		
Klass 1	Inga särskilda skyddsåtgärder krävs	☐
Klass 2	Organisatoriska skyddsåtgärder krävs	☐
Klass 3	Organisatoriska och tekniska skyddsåtgärder krävs	☐

Klassificera *spårbarhet* (4.4)		
Klass 1	Inga särskilda skyddsåtgärder krävs	☐
Klass 2	Organisatoriska skyddsåtgärder krävs	☐
Klass 3	Organisatoriska och tekniska skyddsåtgärder krävs	☐