Informationssäkerhet

Stödanvisning
klassificering av system

Östhammars kommun

Målgrupp	Systemägare, alla kontor och verksamheter
Avsändare	Kommunledningskontoret, Digitalisering och projektledning
Dokumentansvarig	Informationssäkerhetssamordnare
Framtagen	2024-12-30
Reviderad	-

ÖSTHAMMARS KOMMUN
– EN DEL AV ROSLAGEN

Innehåll

Innehåll

Innehållet utgår från kommunens program och vägledning för informationssäkerhet och ger en fördjupad beskrivning och förklarar arbetsprocessen med att fastställa systemets högsta skyddsvärde (systemklassning) vilket styr vilken typ av information som kan/får hanteras i systemet.

Mål och syfte

Målet är en ensad process för systemklassning som svarar mot externa krav, interna behov och som bidrar till att skydda informationen i kommunens verksamheter.
Syftet är att säkra kvalitén i kommunens arbete med informationssäkerhet genom att klassa systemen och identifiera omständigheter som kräver kontroll, åtgärd och uppföljning.

Klassning

Alla digitaliserings- och IT-lösningar, tjänster och verksamhetssystem som används behöver klassas för att fastställa vilken nivå av information som kan hanteras där. Detta för att säkerställa att systemet och/eller tjänsten verkligen uppfyller de krav som den klassade informationen ställer. Ett systems möjlighet att hantera information på rätt klassningsnivå baseras på kommunens fastställda krav som utgår från standarden ISO 27002.
Även risker som faller utanför kravställningar i ISO 27002 ska beaktas.
Diarieför gärna klassningen med övriga handlingar för systemet.

Om systemet inte motsvarar verksamhetens krav på säkerhet ska informationen hanteras på annat säkert sätt fram till dess att kraven är uppfyllda!

Genomförande och dokumentation

Systemklassningen ska dokumenteras och en kopia skickas till infosakerhet@osthammar.se
Till hjälp finns *mall för klassning av system,* hur den används beskrivs nedan.

Arbetsnamn och ägarskap

Här dokumenteras grunduppgifter för klassningen

Systemnamn	Systemägare	Informationsägare	Kontor *(kontor som ansvarar för systemet)*	Diarienummer

Utförts av *(alla som deltagit vid klassningen)*	Datum för klassificering

Typ av klassning

Här definieras vad klassningen handlar om

Klassningen gäller					
☐	Anskaffning/utveckling av system	☐	Driftstart/Implementering	☐	Förändring och kontroll
Kommentar					

Anskaffning/utveckling – innebär en klassning för att i planeringsstadiet av upphandling eller utveckling av ett system klargöra förutsättningarna att ta hänsyn till.

Driftstart/implementering – innebär en slutgiltig klassning av system innan implementering för att säkerställa dess lämplighet för behandling av värderad information.

Förändring och kontroll – innebär en klassning av system som är i drift.

Systembeskrivning

Här beskrivs vad systemet används till, beskrivning av användargrupper och deras behörigheter och vilka delar systemet består av (t.ex. servrar, nätverk, applikationer).

Systembeskrivning
Funktion, syfte, användare, systemets komponenter

Klassificering

Vilken nivå av skydd finns det i systemet?

Ett systems möjlighet att hantera information på rätt klassningsnivå baseras på kommunens fastställda krav som utgår från ISO-standarden 27002.

Klassificering system – Vilken nivå av skydd finns det i systemet?						
Område	Detalj	3	2	1	Värde	Kommentar
Ansvar	Är roller och ansvar tydligt definierade för att skydda informationen i systemet?	Ja	Ja	Nej		
Autentisering	Används två faktor autentisering?	Ja	Ja	Nej		
Autentisering	Används multi faktor autentisering?	Ja	Ja	Nej		
Loggning	Registreras åtkomst och användning av systemet?	Ja	Ja	Nej		
Loggning	Är loggar skyddade mot manipulation och tillgängliga för analyser vid incidenter?	Ja	Ja	Nej		
Kryptering	Är känslig information krypterad?	Ja	Ja	Nej		
Nätverk	Finns brandväggar, nätverksövervakning och är nätverken separerade?	Ja	Ja	Ja		
Nätverk	Är kommunikation över nätverk skyddad med t.ex. VPN?	Ja	Ja	Nej		
Antivirus	Används virusskydd med regelbundna uppdateringar?	Ja	Ja	Ja		
Informations-överföring	Är all kommunikation till och från systemet skyddad mot obehörig åtkomst eller förvanskning?	Ja	Ja	Nej		

Exempel: Om svaret är **Nej** på frågan **Loggning – Registreras åtkomst och användning av systemet?** Får endast information klassad till nivå 1 hanteras i systemet.

Säkerhetsåtgärder

ISO 27002 innefattar viktiga säkerhetsåtgärder att uppfylla eller ta ställning till för att uppnå en god säkerhet. Krav som systemägaren behöver tänka på framgår av tabellen säkerhetsåtgärder**.**

Säkerhetsåtgärder	Förklaring	Har det eller kommer det att hanteras? Hur?
Utvecklingsplan	*En utvecklingsplan för fortsatt utveckling av systemet i sig och vilka kommande krav som kan komma att ställas.*	
Rutiner för åtkomsthantering	*För att säkerställa att rätt personer har rätt nivå av åtkomst till systemet och att åtkomsten är skyddad mot obehöriga.*	
Kontinuitetsplan	*Kontinuitetsplan för att säkerställa planerade aktiviteter för återställning av system och backup*	
Rutiner för gallring	*Rutin för gallring där gallring hanteras av IT.*	
Rutiner för systemförvaltning		
Rutiner för säkerhetskopiering/backupkörning		
Regelbundna säkerhetsrevisioner av ingående delar i systemet	*I samråd med leverantören*	
Regelbundna revisioner för att säkerställa att systemet uppfyller kraven i lagar och regelverk	*I samråd med leverantören*	
Dokumenterat skydd mot andra parter	*T.ex. att avtal finns med förutsättningar och avgränsningar för systemet.*	

Riskhantering

Kvarstående risker efter genomgångna säkerhetsåtgärder skall dokumenteras och hanteras. Systemägarens egen kunskap om systemet samt egen organisation är viktigt i denna genomlysning. T.ex. risker som kan uppstå vid speciella aktiviteter som backup/återläsning eller systemåterställning. Säkerhetsåtgärder som är applicerbara men väljer att inte hanteras skall även noteras här som en medveten risk. Om det finns komplexa risker eller ett större antal identifierade risker använd då *mallen Utökad riskanalys*.

Riskhantering					
Risk					
Hot Möjlig, oönskad händelse med negativa konsekvenser	Sårbarhet Problem/brister/orsaker som ligger till grund för hoten	Konsekvens 1-4	Sannolikhet 1-4	Riskvärde Konsekvens x Sannolikhet	Åtgärd Vad Kan göras för att eliminera, begränsa eller bevaka riskerna och dess sårbarheter

Sammanfattning

I sammanfattningen noteras den högsta typ av informationsklass som man med rådande säkerhetsåtgärder anser systemet kan hantera.
I sammanfattning/utvärdering noteras eventuella medvetna risker som tas ifall man väljer att hantera en högre informationsklass i systemet. Klassningen fastställs av systemägaren.

Sammanfattning	
Systemet är med medvetet risktagande godkänt för hantering av informationsklass:	
Motivering till nivån som systemet klassats till:	

Klassningen fastställs av ägare (datum, namn och roll):_____

Mall för dokumentation

Mall för klassning av system nås via INES Klassa information och Vägledning och stöd

Mall för utökad riskanalys nås via INES Vägledning och stöd