Datum
2020-09-18

Informationssäkerhetsarbete våren 2020

Informationssäkerhet är inget nytt då vikten av att ha tillgänglig och tillförlitlig information, samt ha förmåga att skydda den från obehöriga, är något som dom allra flesta av oss har hanterat förut. Den nya utmaningen ligger i att förändra hanterandet av informationen i takt med att samhället förändras. Digitaliseringen, skärpta lagkrav och förväntningar på att behandlingen av information ska ske snabbt och skyddas korrekt är faktorer som medför att arbetet med informationssäkerhet idag är mer komplext än tidigare.
Information är en av kommunens viktigaste resurser och den finns överallt, utan tillgång till information och de system de behandlas i skulle stora delar av de kommunala verksamheterna sluta fungera. Det är lätt att tänka på information som det vi har nedskrivet på ett papper eller fört in i ett datasystem, men vi hanterar information överallt, i samtal med våra kollegor eller bilder/videoklipp etc.

När vi idag pratar om informationssäkerhet handlar det främst om att se till att informationen hanteras säkert och korrekt utifrån följande aspekter:

1. **Konfidentialitet:** Att informationen inte tillgängliggörs eller delges till obehöriga behöver inte enbart vara ett brott mot lagar det kan även ha allvarliga konsekvenser för kommunens rykte och tillit
2. **Tillgänglighet:** Informationen ska förvaras utifrån det skydd den behöver men skall samtidigt finnas tillgänglig och inte utgöra ett hinder för att arbete fortlöper utan onödiga hinder.
3. **Riktighet (tillförlitlighet):** Du ska kunna spåra förändringar och veta att informationen inte är manipulerad.

Postadress
Ragunda kommun
Box 150
844 21 Hammarstrand

Besöksadress
Centralgatan 15
Telefon
0696-68 20 00

E-post
ragunda.kommun@ragunda.se
Webb
www.ragunda.se

Org.nr
212000-2452
Bankgiro
267-8761

Klassificering och klassificeringsmatris

Utifrån tillgänglighet, riktighet och konfidentialitet ska information klassificeras för att därefter hanteras utifrån de krav som ställs. Klassificering handlar om att uppskatta informationens värde utifrån de tre aspekterna, matrisen nedan är ett verktyg för att utföra detta.

Konsekvensnivå Skyddsbehov	Konfidentialitet	Riktighet	Tillgänglighet
Synnerligen Allvarlig *Mycket Höga Skyddsnivåer*	**K4**: Information som omfattas av Säkerhetsskyddslagen. Särskild hantering.	**R4:** Information som omfattas av Säkerhetsskyddslagen. Särskild hantering.	**T4:** Information som omfattas av Säkerhetsskyddslagen. Särskild hantering.
Allvarlig *Hög Skyddsnivå*	**K3:** Information där förlust av konfidentialitet innebär allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	**R3:** Information där förlust av riktighet innebär allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T3:** Information där förlust av tillgänglighet innebär allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Betydande *Utökad Skyddsnivå*	**K2:** Information där förlust av konfidentialitet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	**R2:** Information där förlust av riktighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	**T2:** Information där förlust av tillgänglighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ
Måttlig *Grundläggande Skyddsnivå*	**K1:** Information där förlust av konfidentialitet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**R1:** Information där förlust av riktighet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T1:** Information där förlust av tillgänglighet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Ringa eller Inga *Ingen Skyddsnivå*	**K0:** Information där förlust av konfidentialitet inte medför någon märkbar negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**R0:** Information där förlust av riktighet inte medför någon märkbar negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T0:** Information där förlust av riktighet inte medför någon märkbar negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.

MBSs klassningsmatris med interna förändringar. Sveriges Säkerhet se separata rutiner

Lagkrav

Som tidigare nämnt är informationssäkerhet inget nytt och det finns flertal lagar som ställer, och har ställt, krav på hur vi inom kommunen hanterar den information vi besitter. Bland annat:

- ***Kommunallagen***
- ***Arkivlagen***
- ***Offentlig Upphandling***
- ***Jordabalken***
- ***Avtalsrätt***
- ***Tryckfrihetsförordningen***
- ***Förvaltningslagen***
- ***Socialtjänstlagen***
- ***GDPR***
- ***Offentlighet och sekretess***
- ***Hälso- och Sjukvårdslagen***
- ***Skollagen***

Ett systematiskt arbete med informationssäkerhet ger oss även en god grund att stå på inför identifieringen och en del av hanteringen vad det gäller den säkerhetskyddsklassificerade informationen som styrs av ***Säkerhetskyddslagstiftningen***.

Syftet med arbetet kring informationssäkerhet har under våren varit att försöka identifiera och initiera det arbete som krävs för att Ragunda kommun ska kunna uppnå de olika lagkrav som ställs på hanterandet av information i våra verksamheter. I denna process har kunskap inhämtats både från metodstöd och litteratur som finns inom ämnet samt hur andra kommuner tagit sig an arbetet. En informationssäkerhetsgrupp har även satts samman för att bistå arbetet utifrån deras kunskap om specifika verksamhetssystem och att de i övrigt har strategiska roller.

För att kunna omsätta den kunskap som inhämtas till praktik beslutade informationssäkerhetsgruppen att några av kommunenens verksamheter skulle pröva dels informationssäkerhetsarbetets process samt specifikt SKRs verktyg KLASSA (Se Strategi för genomförande). Efter utförandet har strategin justerats och en del punkter är identifierade som belyser vad som behöver göras för att arbetet med informationssäkerhet ska komma igång (Se Punkterna nedan).

Övergripande slutsatser som är värda att poängtera är:

Att vi behöver systematiskt börja med att identifiera, analysera och hantera informationstillgångar så att vi kan säkerställa vilka rutiner och åtgärder som krävs för att hanteringen av informationen uppnår de krav som ställs på respektive informationstillgång. Detta arbetssätt beskrivs i metodstöd för systematiskt informationssäkerhetsarbete som bygger på standarden ISO/IEC 27000, Ledningssystem för informationssäkerhet.

Sveriges kommuners och regioners KLASSA tillhandahåller ett enkelt självskattningsverktyg för att kontrollera hur man förhåller sig till informationstillgångarnas respektive lagkrav. Problemet med KLASSA är att det bara behandlar systemen där information lagras och inte den övriga informationen som hanteras inom kommunen. Arbetar man endast med detta verktyg uppfyller man inte ISO-standarden.

Utifrån utfört arbete med informationssäkerhet framträder ett behov av:

1. Policy för informationssäkerhet:

Vi behöver övergripande besluta och beskriva hur informationssäkerhetsarbetet inom kommunen ska bedrivas. Arbetsfördelning och mandat bör vara tydligt och arbetet bör ske systematiskt och behöver därav även tydlig struktur av cykler och ansvar.

2. Riktlinjer för arbetet med informationssäkerhet:

Det bör finnas tydliga rutiner och riktlinjer för informationssäkerhet där medarbetares ansvar synliggörs. Rutiner och riktlinjer bör grundas i att informationssäkerheten ska stärkas genom att använda sig av samtliga skyddsåtgärderområden:

- **Administrativa skyddsåtgärder:** Exempelvis implementerade rutiner och arbetssätt
- **Fysiska skyddsåtgärder:** Exempelvis larm och lås
- **Tekniska skyddsåtgärder:** Exempelvis kryptering eller tvåstegsinlogg

Rutiner och riktlinjer bör utgå från att vara förvaltningsövergripande, verksamheterna kan sedan behöva utveckla och förtydliga vad dessa innebär för respektive arbetsplats.

3. Strategi för genomförande

Utifrån arbetet med informationssäkerhet under våren har nedan plan prövats och anpassats. Det är en tidkrävande process som kartlägger och analyserar värdet av informationen som verksamheten besitter.

Respektive verksamhet bör genomföra informationssäkerhetsarbete där resultatet av samtliga verksamheter kan analyseras på kommunövergripande nivå.

- Utse arbetsgrupp och ansvarig samordnare
- Verksamhetsanalys & Omvärldsanalys (Ska utgå från dokumenthanteringsplan)
- Klassificera informationen utifrån klassificeringsmodell
- Klassificera systemen som bär informationen med hjälp av KLASSA
- Utför riskanalyser på informationstillgångar eller system med högt klassificeringsvärde
- Åtgärds- och implementeringsplan
- Redovisa/sammanför med kommunövergripande (Är upptäckta åtgärdsförslag något som behöver förändras på annan nivå/enhet?)
- Genomför förändringsarbetet
- Utvärdera