Södertörns brandförsvarsförbund

TJÄNSTEUTLÅTANDE 2019

2019-01-25

Dnr: 2019-000410

Informationssäkerhetspolicy

Sammanfattning

Efter revisorernas granskning av IT-verksamheten hos Södertörns brandförsvarsförbund under hösten 2017 konstaterades att det saknades aktuella dokumenterade riktlinjer för IT-området. Efter detta har en övergripande IT-policy beslutats vid direktionen 2018-03-16, § 22. Ett nästa steg i denna process är att säkerställa styrdokumenten för informationssäkerhet.

Ett förslag till informationssäkerhetspolicy har tagits fram som ska reglera skyddet av Södertörns brandförsvarsförbunds informationstillgångar mot eventuella hot – interna eller externa, avsiktliga eller oavsiktliga.

Ärendets beredning

Förslaget till informationssäkerhetspolicy har arbetats fram av administrativ chef Susanne Nilsson på uppdrag av brandchef Lars-Göran Uddholm.

Bilagor

Bilaga 1 Förslag till informationssäkerhetspolicy

Förslag till beslut

1. Direktionen fastställer föreslagen informationssäkerhetspolicy.

Susanne Nilsson
Administrativ chef

Södertörns brandförsvarsförbund

Mogårdsvägen 2
143 43 Vårby

Tfn: 08-721 22 00
Fax: 08-721 22 23

www.sbff.se
brandforsvaret@sbff.se

Org.nr.: 222000-0737

Södertörns brandförsvarsförbund

Informationssäkerhetspolicy

Dnr: 2019-000410

Datum: 2019-01-25

Introduktion

Denna policy reglerar skyddet av Södertörns brandförsvars informationstillgångar mot eventuella hot – interna eller externa, avsiktliga eller oavsiktliga.

Med informationstillgångar menas både information (data) som sådan och de resurser som används för att hantera informationen (IT-system, nätverk, servrar och arbetsstationer inklusive mobila enheter som surfplattor och mobiltelefoner).

Syfte och utgångspunkter

Syftet med denna policy är att säkerställa att all information hanteras på ett säkert och effektivt sätt. Information är en av Sbff:s nyckelresurser. Genom att arbeta systematiskt med informationssäkerhet utifrån etablerade standarder och genomtänkta policyer kan Sbff åstadkomma bättre kvalitet i verksamheten och ökad trovärdighet.

Arbetet med informationssäkerhet ska ta sin utgångspunkt i följande principer:

- **Tillgänglighet**. Våra medarbetare, kunder, partners och övriga intressenter ska ha tillgång till den information de behöver, när de behöver den och på förväntat sätt.
- **Riktighet**. Vår information ska vara korrekt och tillförlitlig. Informationen ska skyddas mot oönskade förändringar och fel.
- **Konfidentialitet/sekretess**. Vår information ska inte göras tillgänglig för eller avslöjas för obehöriga utanför vår kontroll.
- **Spårbarhet**. Aktiviteter ska kunna härledas i efterhand. Vi ska kunna visa vad som har hänt och vem som har gjort vad i våra informationssystem.

Sbff:s arbete med informationssäkerhet ska ske utifrån etablerade standarder och internationella riktlinjer. Arbetet ska utföras på ett strukturerat sätt i enlighet med denna policy och Sbff:s övriga fastställda riktlinjer och rutiner.

Säkerhetsarbetet ska resultera i kostnadseffektiva och behovsanpassade säkerhetsåtgärder som harmoniserar med Sbff:s uppgift och verksamhetsmässiga åtaganden. Det ska ske på ett sätt som bidrar till att leverera kvalitet i verksamheten. Åtgärder för att säkra informationen ska i så liten utsträckning som möjligt vara ett hinder för utvecklingen av olika tekniska lösningar.

Skyddet av information ska tillgodose de krav som ställs på Sbff – både genom gällande lagstiftning och i överenskommelser med Sbff:s kunder, samarbetspartners och övriga intressenter.

Övergripande roller och ansvar

Policyn gäller för samtliga anställda och konsulter inom Sbff samt övriga kontraktsbundna intressenter. Var och en har ansvar för att skydda den information som man disponerar över utifrån givna riktlinjer och instruktioner.

Ansvaret för informationssäkerheten hos Sbff delas in i olika delar, huvudsakligen fysisk säkerhet, IT-säkerhet samt säkerhet för personuppgifter. Denna övergripande informationssäkerhetspolicy kompletteras med specifika styrdokument och riktlinjer inom dessa områden. För mer detaljerad information hänvisas till Sbff:s separata IT-policy och dataskyddspolicy.

Generella riktlinjer

Informationsklassning och riskbedömning

För att avgöra vilket skydd som behövs och hur olika typer av information får hanteras, ska känslig och/eller väsentlig information som hanteras inom Sbff klassificeras. Tillsammans med klassificeringen ska riskbedömningar avgöra vilka säkerhetsåtgärder som behövs för respektive informationstyp. Riskbedömningar ska genomföras löpande samt alltid vid större förändringar.

Åtkomst och behörighet

Information i IT-system ska alltid skyddas med antingen någon form av autentisering eller genom kryptering. Sbff ska arbeta aktivt med behörigheter i IT-system och göra medvetna bedömningar av vilka användare som ska ha tillgång till systemen, för att minska mängden information som exponeras till olika användargrupper. Vi strävar alltid efter att minimera breda behörigheter, så att endast personer som i sin roll behöver tillgång till information har åtkomst till den. Sbff ska tillämpa rollbaserad åtkomstkontroll. Alla beslut och inställningar som rör användaråtkomst ska regleras centralt i IT-miljön.

Anställda, konsulter och övrig kontraktsbunden personal får inte ta del av eller bereda sig tillgång till företagets information utifrån privata intressen.

Loggning och uppföljning

Uppföljning och kontroll, bland annat genom granskning av loggar, ska vara en naturlig del i Sbff:s säkerhetsarbete. Det ska finnas rutiner för att övervaka loggar kontinuerligt och ett ändamålsenligt system där man kan söka fram händelser och granska loggar på ett effektivt sätt.

Säkerhetsincidenter

Den som upptäcker brister i informationssäkerheten måste uppmärksamma IT-funktionen på det. Alla medarbetare måste också rapportera händelser som kan göra att våra informationstillgångar utsätts för risker. Alla incidenter som sker ska alltid dokumenteras genom en incidentrapport.

Ett strukturerat arbete med incidenthantering ger möjligheten till kontroll och uppföljning av Sbff:s säkerhetsarbete och också stora möjligheter för organisationen att förebygga eller minska effekten av framtida incidenter.

Utöver en etablerad process för incidentrapportering, ska Sbff ha en framtagen plan för hur verksamheten ska kunna upprätthållas och återställas i händelse av en allvarlig incident eller kris. Riktlinjer och rutiner för hur Sbff säkerställer kontinuitet i affärskritiska verksamheter skapas och definieras av IT-avdelningen.

Outsourcing

Även för sådana system och tjänster som är outsourcade till extern leverantör så kvarstår en skyldighet hos Sbff att säkerställa att leverantören lever upp till lämplig säkerhet och följer överenskomna instruktioner.

Revidering av dokumentet

Denna policy ska revideras vid behov i samband med förändringar i verksamhetens inriktning och omfattning. En allmän översyn av dokumentet ska göras i samband med den årliga revisionen. I samband med revideringen ska också kompletterande riktlinjer och rutinbeskrivningar revideras på motsvarande sätt.

Dokumentets historia

Upprättad/ reviderad:	Upprättad/ reviderad av:	Kontrollerad av 1:	Kontrollerad av 2:	Godkänd av:	Ersätter:
SUN		LU	AE	Direktionen 2019-02-08 §4	