Svenska kyrkan 2018-10-10
TÄBY FÖRSAMLING

Informationssäkerhetspolicy för Täby församling

Beslutad av Kyrkorådet
Datum för beslut: 2018-10-10

Syfte och samband

Dokumentet beskriver Täby församlings förhållningssätt till information och informationssäkerhet samt grundläggande principer för informationshantering i organisationen.
Informationssäkerhetspolicyn gäller för all hantering av information, oavsett form, inom ramen för kyrkorådets ansvar.

Målgrupp

Förtroendevalda, ideella och anställda medarbetare i Täby församling, kunder och leverantörer till Täby församling.

Kommunikation

Dokumentet ska tillgängliggöras via svenskakyrkan.se/tabyforsamling och presenteras i samband med att en person tillträder ett förtroendeuppdrag, personal anställs och då leverantörer eller kunder kontrakteras.

Uppföljning

Efterlevnad ska följas upp av församlingens dataskyddsombud och redovisas löpande till kyrkoråd och ledningsgrupp.

Uppdatering

Dokumentet ska aktualitetsprövas minst en gång per mandatperiod och uppdateras vid behov.

TÄBY FÖRSAMLING
POSTADRESS: Box 208, 183 23 TÄBY
BESÖKSADRESS: Tibble kyrka och församlingsbyggnad, Attundavägen 3 vid Täby c
TELEFON: 08-580 035 00 E-POST: tabyforsamling@svenskakyrkan.se
WEBB: www.svenskakyrkan.se/taby

Inledning

Trossamfundet Svenska kyrkans verksamhet är grundad på principer om öppenhet, personlig integritet och respekt för individen. Medlemmar och allmänhet ska ha möjlighet att få insyn i verksamheten. De ska kunna lita på den information som Svenska kyrkan lämnar och vara trygga med att information som samlas in får ett tillräckligt skydd.

För att verksamheten ska kunna bedrivas behövs information som är korrekt och tillgänglig. Inkorrekt information eller avbrott i tillgången till information kan leda till allvarliga konsekvenser för såväl enskilda personer som för Svenska kyrkan. För Svenska kyrkan är information således en strategiskt viktig resurs.

Enligt lagen (1998:1591) om Svenska kyrkan är Svenska kyrkans arkiv en del av det nationella kulturarvet. Det betyder att informationen som hanteras inte bara är viktig för Svenska kyrkans egen del.

I dagens informationssamhälle med en allt ökande grad av digitalisering innebär hanteringen av information i IT-system möjligheter för verksamheten, men även att sårbarheter och hot kan få stora konsekvenser om inte informationen säkras. I detta utgör hanterande av elektronisk information en särskild utmaning med stora krav på proaktivitet.

Arbetet med att säkra information består av att se till att information finns tillgänglig när den behövs, att informationen är korrekt och att obehöriga inte får åtkomst till informationen. För att åstadkomma detta ska ett systematiskt arbete bedrivas med syfte att skapa och upprätthålla ett skydd som är tillräckligt utifrån verksamhetens förutsättningar och behov.

Informationssäkerhetsarbetet ska genomsyra all verksamhet. Arbetet både berör och är beroende av såväl förtroendevalda som anställda. Arbetet syftar till att värna den enskildes integritet samt stödja och säkerställa att verksamheten kan genomföras som avsett och är därför en viktig del av internstyrning, kontroll och riskhantering.

Mål

Målet för Täby församlings informationssäkerhetsarbete är att skydda informationen inom verksamheten. Skyddet ska vara anpassat till skyddsvärde, risk och krav, såväl från lagstiftning som inomkyrklig reglering. Ett högt säkerhetsmedvetande i verksamheten är den mest centrala delen i informationssäkerhetsarbetet och ska för all information kompletteras med bland annat val av behörighetslösningar och loggsystem, skydd mot skadlig kod samt skydd mot obehörig fysisk tillgång till informationen.

Genom en god informationssäkerhet främjas verksamhetens funktionalitet, kvalitet och effektivitet, men även individers rättigheter och personliga integritet. Den goda informationssäkerheten bidrar till förmågan att förebygga och hantera allvarliga störningar samt skapar förtroende för Svenska kyrkans informationshantering och IT-system.

Omfattning

Informationssäkerhetspolicyn gäller för all hantering av information, oavsett form, inom ramen för kyrkorådets ansvar. Den gäller även för alla som arbetar på uppdrag av Täby församling.

Styrning och ledning

För att hålla samman och åstadkomma systematik i informationssäkerhetsarbetet ska ett ledningssystem för informationssäkerhet användas. Ledningssystemet ska innehålla nödvändiga processer och rutiner som behövs för att säkerställa att verksamheten uppfyller kraven på en ändamålsenlig informationssäkerhet.

Säkerhetsaspekter

Täby församling ska värdera all information efter sin känslighet och med hjälp av administrativa, tekniska och fysiska skyddsåtgärder säkerställa tillräckligt skydd, detta oavsett om information eller informationssystem hanteras internt eller av extern part.

- **Konfidentialitet (rätt person)**
  Information får inte göras tillgänglig eller avslöjas i de delar som omfattas av sekretess enligt bestämmelserna i kyrkoordningen eller offentlighets- och sekretesslagen.

- **Riktighet (rätt information)**
  Informationen får inte förändras eller gå förlorad, av misstag, genom inverkan av obehörig eller på grund av tekniskt fel.

- **Tillgänglighet (rätt tid och plats)**
  Informationen ska kunna användas i förväntad utsträckning, inom önskad tid och på rätt plats.

- **Spårbarhet**
  Händelser i behandlingen av information ska kunna spåras.

Skyddsprinciper

För att på ett systematiskt sätt kunna avgöra vad som är tillräckligt skydd ska arbetet ske utifrån följande principer:

- All information ska ha en ägare.
- All information ska informationssäkerhetsklassas, dokument ska märkas utifrån klassningen. Informationsägaren ansvarar för informationssäkerhetsklassningen och att nödvändiga säkerhetskrav ställs.
- Alla informationssystem ska ha en systemägare. Systemägaren ansvarar för att säkerhetskraven på systemet uppfylls.
- Särskilda styrdokument och processer ska finnas för att säkra hanteringen av integritetskänslig information, såsom personuppgifter.
- Regelbundna risk- och sårbarhetsanalyser samt inträffade incidenter ska ligga till grund för kontinuerlig prövning av relevans på tillämpade skyddsåtgärder.
- Valen av skyddsåtgärder ska vara kostnadseffektiva med hänsyn tagen till värdet av informationen och genomförd riskanalys.
- Kontinuitetsplanering ska genomföras, för att kunna bedriva kritisk verksamhet på fastställd nivå vid olika typer av katastrofer, störningar och avbrott.
- Såväl förtroendevalda som alla medarbetare, anställda och extern personal, ska veta vad det egna ansvaret kring informationssäkerhet innefattar och vilka regler som

gäller. Medarbetarna ska ha ett högt säkerhetsmedvetande och förmåga att kritiskt ifrågasätta händelser som kan påverka informationssäkerheten.
- Informationssäkerhet ska vara en del i kravställningen inför upphandling, utveckling, användning och avveckling av informationssystem.
- Tillämpningen av policy och riktlinjer ska kontinuerligt utvärderas, både genom internkontroll och extern granskning.

Riktlinjer

Kyrkorådet ansvarar för att det hos Täby församling finns bestämmelser som tydliggör hur denna policy ska tillämpas.