ANTIQUUS MYSTICUSQUE ORDO ROSAE CRUCIS

IT- och informationssäkerhetspolicy

Utgiven av Den Skandinaviska Storlogen av Rosenkors-Orden AMORC
Rösan, Gathes väg 141, 439 36 Onsala, Sverige
www.amorc.nu ~ Org.nr. 839400-1278 ~ e-post: info@amorc.se

Innehåll

1. Syfte och bakgrund

Den skandinaviska Storlogen inom AMORC har enligt stadgarna ansvar för att skydda medlemmarnas uppgifter, upprätthålla sekretessen kring undervisningsmaterial och säkerställa en ansvarsfull administrativ verksamhet. Denna IT- och informationssäkerhetspolicy fastställer de övergripande principerna för hur Storlogen skyddar information och IT-system i enlighet med stadgarna och gällande svensk lagstiftning.

Policyn utgår från kraven i dataskyddsförordningen (GDPR), dataskyddslagen (2018:218) och bokföringslagen (1999:1078) samt relevanta arkiv- och dokumentationskrav. Tillsynsmyndighet för behandling av personuppgifter är Integritetsskyddsmyndigheten.

Policyn stöder styrelsens övergripande tillsynsansvar och Stormästarens dagliga administrativa ansvar.

2. Tillämpningsområde

Denna policy gäller för styrelsen, Stormästaren, anställda, volontärer, lokala enheter och externa leverantörer som behandlar uppgifter på Storlogens vägnar. Den omfattar alla IT-system, databaser, arkiv och kommunikationskanaler, inklusive medlemsadministration, ekonomisystem och digitala plattformar.

3. Informationsskydd

Storlogen skyddar all information utifrån dess karaktär och känslighet. Medlemsuppgifter, undervisningsmaterial, ritualer, interna beslutsdokument och ekonomisk information betraktas som konfidentiella och får endast göras tillgängliga för behöriga personer. Administrativa dokument behandlas som interna, medan publicerat material betraktas som offentligt.

Konfidentiell information får inte vidarebefordras utan rättslig grund eller behörig auktorisation. Tystnadsplikt gäller för alla betrodda funktioner, även efter upphörande av uppdrag eller anställning.

4. Behandling av personuppgifter

Se Storlogens integritetspolicy (GDPR).

5. Åtkomst och teknisk säkerhet

Åtkomst till system och information beviljas enligt en strikt behovsprincip. Personliga inloggningsuppgifter används, och där det är möjligt tillämpas tvåfaktorsautentisering. Åtkomstbehörigheter granskas regelbundet och återkallas omedelbart vid avgång eller upphörande av tjänst.

Storlogen tillämpar lämpliga tekniska och organisatoriska säkerhetsåtgärder, inklusive kryptering vid dataöverföring, brandvägg, antivirusskydd, löpande

säkerhetsuppdateringar samt regelbunden säkerhetskopiering. Säkerhetskopieringslösningarna testas med lämpliga intervall för att säkerställa att data kan återställas.

6. Ekonomisk och administrativ information

Redovisnings- och ekonomidata hanteras i enlighet med stadgarna och svensk redovisningslagstiftning. Endast behöriga personer har tillgång till ekonomisystemen, och transaktioner ska kunna dokumenteras och spåras. Oberoende revisor har tillgång till relevant information i samband med revisionen.

7. Samarbete med leverantörer

När externa leverantörer behandlar uppgifter på Storlogens vägnar ingås databehandlingsavtal som säkerställer att behandlingen sker i enlighet med gällande lagstiftning och denna policy. Överföring av uppgifter utanför EU/EES får endast ske på laglig grund.

8. Hantering av säkerhetsincidenter

Vid misstanke om brott mot informationssäkerheten inleds en snabb bedömning av incidentens omfattning och risk. Styrelsen informeras vid väsentliga händelser. Om ett brott mot personuppgiftssäkerheten medför risk för enskilda personers rättigheter, anmäls händelsen till Integritetsskyddsmyndigheten inom 72 timmar i enlighet med lagstiftningen, och berörda personer informeras om risken bedöms som hög.

9. Övervakning och uppdatering

Styrelsen har det övergripande ansvaret för att policyn efterlevs och kontinuerligt utvärderas. Policyn ses över minst en gång om året och uppdateras vid behov för att säkerställa fortsatt efterlevnad av lagstiftning, stadgar och god praxis.