ANTIQUUS MYSTICUSQUE ORDO ROSAE CRUCIS

IT- og Informationssikkerhedspolitik

Utgitt av Den Skandinaviske Storlosjen av Rosenkors-Ordenen AMORC
Rösan, Gathes väg 141, 439 36 Onsala, Sverige
www.amorc.nu ~ Org.nr. 839400-1278 ~ info@amorc.se

Innhold

1. Formål og grundlag

Den Skandinaviske Storloge af AMORC har et vedtægtsmæssigt ansvar for at beskytte medlemmernes oplysninger, bevare fortroligheden omkring undervisningsmateriale og sikre en forsvarlig administrativ drift. Denne IT- og informationssikkerhedspolitik fastlægger de overordnede principper for, hvordan Storlogen beskytter informationer og IT-systemer i overensstemmelse med vedtægterne og gældende svensk lovgivning.

Politikken tager udgangspunkt i kravene i Dataskyddsförordningen (GDPR), Dataskyddslagen (2018:218) og Bokföringslagen (1999:1078) samt relevante arkiv- og dokumentationskrav. Tilsynsmyndighed for behandling af personoplysninger er Integritetsskyddsmyndigheten.

Politikken understøtter bestyrelsens overordnede tilsynsansvar og Stormesterens daglige administrative ansvar.

2. Anvendelsesområde

Politikken gælder for bestyrelsen, Stormesteren, ansatte, frivillige, lokale enheder og eksterne leverandører, som behandler oplysninger på vegne af Storlogen. Den omfatter alle IT-systemer, databaser, arkiver og kommunikationskanaler, herunder medlemsadministration, økonomisystemer og digitale platforme.

3. Informationsbeskyttelse

Storlogen beskytter alle oplysninger ud fra deres karakter og følsomhed. Medlemsoplysninger, undervisningsmateriale, ritualer, interne beslutningsdokumenter og økonomiske oplysninger betragtes som fortrolige og må kun tilgås af autoriserede personer. Administrative dokumenter behandles som interne, mens offentliggjort materiale anses som offentligt.

Fortrolige oplysninger må ikke videregives uden lovligt grundlag eller behørig autorisation. Tavshedspligt gælder for alle betroede funktioner, også efter ophør af hverv eller ansættelse.

4. Behandling af personoplysninger

Der henvises til Storlogens Personværnserklæring (GDPR).

5. Adgang og teknisk sikkerhed

Adgang til systemer og oplysninger gives efter et strengt behovsprincip. Der anvendes personlige loginoplysninger, og hvor det er muligt, anvendes to-faktor-autentifikation. Adgange gennemgås regelmæssigt og fjernes straks ved fratrædelse eller ophør af funktion.

Storlogen anvender passende tekniske og organisatoriske sikkerhedsforanstaltninger, herunder kryptering ved dataoverførsel, firewall, antivirusbeskyttelse, løbende sikkerhedsopdateringer samt regelmæssig backup. Backup-løsninger testes med passende intervaller for at sikre, at data kan genskabes.

6. Økonomiske og administrative oplysninger

Regnskabs- og økonomidata behandles i overensstemmelse med vedtægterne og svensk regnskabslovgivning. Kun autoriserede personer har adgang til økonomisystemer, og transaktioner skal kunne dokumenteres og spores. Uafhængig revisor har adgang til relevante oplysninger i forbindelse med revision.

7. Samarbejde med leverandører

Når eksterne leverandører behandler oplysninger på vegne af Storlogen, indgås der databehandleraftaler, som sikrer, at behandlingen sker i overensstemmelse med gældende lovgivning og denne politik. Overførsel af oplysninger uden for EU/EØS må kun finde sted på lovligt grundlag.

8. Håndtering af sikkerhedshændelser

Ved mistanke om brud på informationssikkerheden iværksættes en hurtig vurdering af hændelsens omfang og risiko. Bestyrelsen orienteres ved væsentlige hændelser. Hvis et brud på persondatasikkerheden medfører risiko for enkeltpersoners rettigheder, anmeldes hændelsen til Integritetsskyddsmyndigheten inden for 72 timer i overensstemmelse med lovgivningen, og berørte personer informeres, hvis risikoen vurderes som høj.

9. Tilsyn og opdatering

Bestyrelsen har det overordnede ansvar for, at politikken efterleves og løbende vurderes. Politikken gennemgås mindst én gang årligt og opdateres efter behov for at sikre fortsat overholdelse af lovgivning, vedtægter og god praksis.