ANTIQUUS MYSTICUSQUE ORDO ROSAE CRUCIS

IT- og Informasjonssikkerhetspolicy

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

Innhold

1. Formål og grunnlag

Den Skandinaviske Storlosjen av AMORC har et vedtektsfestet ansvar for å beskytte medlemmers opplysninger, ivareta konfidensialiteten rundt undervisningsmateriell og sikre en forsvarlig administrativ drift. Denne IT- og informasjonssikkerhetspolicy fastsetter de overordnede prinsippene for hvordan Storlosjen beskytter informasjon og IT-systemer i samsvar med vedtektene og gjeldende svensk lovgivning.

Policyen tar utgangspunkt i kravene i personvernforordningen (GDPR), personvernloven (2018:218) og regnskapsloven (1999:1078) samt relevante arkiv- og dokumentasjonskrav. Tilsynsmyndighet for behandling av personopplysninger er Datainspeksjonen.

Retningslinjene støtter styrets overordnede tilsynsansvar og stormesterens daglige administrative ansvar.

2. Gjeldende område

Retningslinjene gjelder for styret, stormesteren, ansatte, frivillige, lokale enheter og eksterne leverandører som behandler opplysninger på vegne av Storlosjen. De omfatter alle IT-systemer, databaser, arkiver og kommunikasjonskanaler, herunder medlemsadministrasjon, økonomisystemer og digitale plattformer.

3. Informasjonsbeskyttelse

Storlosjen beskytter all informasjon ut fra dens art og sensitivitet. Medlemsopplysninger, undervisningsmateriale, ritualer, interne beslutningsdokumenter og økonomiske opplysninger anses som konfidensielle og må kun gjøres tilgjengelig for autoriserte personer. Administrative dokumenter behandles som interne, mens offentliggjort materiale anses som offentlig.

Konfidensiell informasjon må ikke videreformidles uten lovlig grunnlag eller behørig autorisasjon. Taushetsplikt gjelder for alle betrodde funksjoner, også etter opphør av verv eller ansettelse.

4. Behandling av personopplysninger

Det vises til Storlosjens personvernerklæring (GDPR).

5. Tilgang og teknisk sikkerhet

Tilgang til systemer og opplysninger gis etter et strengt behovsprinsipp. Det benyttes personlige påloggingsopplysninger, og der det er mulig, benyttes tofaktorautentisering. Tilgangsrettigheter gjennomgås regelmessig og fjernes umiddelbart ved fratredelse eller opphør av stillingen.

Storlosjen benytter passende tekniske og organisatoriske sikkerhetstiltak, herunder kryptering ved dataoverføring, brannmur, antivirusbeskyttelse, løpende sikkerhetsoppdateringer samt regelmessig backup. Backup-løsninger testes med passende intervaller for å sikre at data kan gjenskapes.

6. Økonomisk og administrativ informasjon

Regnskaps- og økonomidata behandles i samsvar med vedtektene og svensk regnskapslovgivning. Kun autoriserte personer har tilgang til økonomisystemene, og transaksjoner skal kunne dokumenteres og spores. Uavhengig revisor har tilgang til relevant informasjon i forbindelse med revisjonen.

7. Samarbeid med leverandører

Når eksterne leverandører behandler opplysninger på vegne av Storlosjen, inngås det databehandleravtaler som sikrer at behandlingen skjer i samsvar med gjeldende lovgivning og denne policyen. Overføring av opplysninger utenfor EU/EØS må kun skje på lovlig grunnlag.

8. Håndtering av sikkerhetshendelser

Ved mistanke om brudd på informasjonssikkerheten iverksettes en rask vurdering av hendelsens omfang og risiko. Styret informeres ved vesentlige hendelser. Hvis et brudd på personopplysningssikkerheten medfører risiko for enkeltpersoners rettigheter, meldes hendelsen til Datatilsynet innen 72 timer i samsvar med lovgivningen, og berørte personer informeres dersom risikoen vurderes som høy.

9. Tilsyn og oppdatering

Styret har det overordnede ansvaret for at retningslinjene overholdes og vurderes fortløpende. Retningslinjene gjennomgås minst én gang i året og oppdateres etter behov for å sikre fortsatt overholdelse av lovgivning, vedtekter og god praksis.