Informationssikkerhedspolitik for Rytmisk Musikkonservatorium

Formål

Informationer er essentielle for at Rytmisk Musikkonservatorium (RMC) kan opfylde sin mission og vision. Informationssikkerhed har derfor vital betydning for konservatoriets troværdighed og funktionsdygtighed.

Informationssikkerhedspolitikken for Rytmisk Musikkonservatorium (RMC) beskriver vigtigheden af arbejdet med informationssikkerhed på RMC og fastlægger vores ambitionsniveau herfor. Med informationssikkerhedspolitikken forpligter ledelsen sig til at fastlægge og understøtte et passende sikkerhedsniveau for RMC's informationer, systemer og forretningsprocesser, med udgangspunkt i en relevant og tidssvarende risikovurdering.

Formålet med informationssikkerhedspolitikken er at definere en ramme for beskyttelse af RMC's informationer og især at sikre at kritiske, fortrolige og følsomme informationer og informationssystemer bevarer deres fortrolighed, integritet og tilgængelighed.

Informationssikkerhedspolitikken har desuden til formål at tilkendegive overfor alle med relation til RMC, at anvendelse af informationer og informationssystemer er underkastet retningslinjer og regler. På denne måde kan sikkerhedsproblemer forebygges, eventuelle skader begrænses og reetablering af informationer sikres.

RMC's informationssikkerhedspolitiske mål er, at arbejdet med informationssikkerhed skal:

- Understøtte og sikre at undervisningsmæssige og teknisk/administrative processer og forretningsgange sker på et passende sikkerhedsmæssigt niveau

RMC har implementeret et informationssikkerhedsledelsessystem (ISMS), der sikrer en løbende kontrol og sikkerhed for at ovennævnte målsætninger bliver opfyldt.

Informationssikkerhedspolitikken beskriver sammen med RMC's informationssikkerhedsvejledning med underliggende retningslinjer, procedurer og forretningsgange det ledelsesgodkendte niveau for sikkerhed.

Omfang

Informationssikkerhedspolitikken er gældende for alle ansatte på RMC.

Alle ansatte og eksterne konsulenter, som har fysisk eller digital adgang til RMC's systemer, data og informationer, skal gøres bekendt med informationspolitikken og følge denne.

Informationssikkerhedspolitikken omfatter alle RMC's informationer uanset hvilken form, de opbevares og formidles på, herunder også informationer, som ikke tilhører RMC, men som konservatoriet kan gøres ansvarlig for. Dette inkluderer f.eks. informationer om personale, finansielle forhold, alle data, som bidrager til administrationen af RMC, produktionsdata og

Rytmisk Musikkonservatorium
Leo Mathisens Vej 1
1437 København K

+ 45 4188 2500
rmc@rmc.dk

rmc.dk

anlægsdata, samt informationer, som er overdraget til RMC af eksterne parter. Disse informationer kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning, eller enhver anden information, som kun er til intern brug.

Sikkerhedsniveau

Det er RMC's politik at beskytte kritiske informationer. Derfor tillades brug, adgang til og offentliggørelse af informationer udelukkende i overensstemmelse med RMC's retningslinjer og under hensyntagen til den til enhver tid gældende lovgivning. RMC's ledelse skal fastlægge på baggrund af en risikovurdering et sikkerhedsniveau, som svarer til kritikaliteten af de pågældende informationer, og som følger ISO 27001:2013 og ISO 27701:2019 standarderne og er afstemt efter risiko og væsentlighed. Sikkerhedsniveauet overholder desuden lovkrav og indgåede aftaler og licensbetingelser. Det fastlagte sikkerhedsniveau afspejles i de til enhver tid gældende retningslinjer, regler, procedurer og forretningsgange.

Organisation og ansvar

RMC's ledelse er ansvarlig for planlægning, implementering og kontrol af informationssikkerhed. Det er desuden ledelsens ansvar at sikre, at den nødvendige viden og kompetence om informationssikkerhed kommunikeres til alle ansatte og studerende.

Det operationelle ansvar for den daglige styring af informationssikkerhedsindsatsen er placeret hos informationssikkerhedsudvalget. Dette udvalg kontrollerer, at de tiltag, der er beskrevet i informationssikkerhedspolitikkens tilknyttede dokumenter, gennemføres og efterleves. Ligeledes er det væsentligt, at informationssikkerheden integreres i alle forretningsgange, driftsopgaver og projekter. Informationssikkerhedsudvalget opdaterer mindst én gang hvert andet år risikovurderingen samt ved eventuelle større ændringer i opgaver, leverandører, it-systemer eller anvendelse deraf.

Sekretariatschefen har drift og udvikling af RMC's it som en del af sit faglige ansvarsområde. Sekretariatschefen er forperson for informationssikkerhedsudvalget, og daglig leder for informationssikkerhedskoordinatoren.

Informationssikkerhedskoordinatoren er ansvarlig for den løbende implementering, vedligeholdelse og udvikling af informationssikkerhedssystemet på RMC og for opfølgning på sikkerhedshændelser.

Alle ansatte på RMC er forpligtet til at efterleve den til enhver tid gældende informationssikkerhedspolitik med til hørende retningslinjer, procedurer og relaterede bilag.

Overtrædelse af informationssikkerhedspolitikken

En overtrædelse af informationssikkerhedspolitikken kan, efter omstændighederne, medføre disciplinære sanktioner.

Gennemgang af informationssikkerhedssystemets effektivitet og review

RMC vil hvert andet år afprøve informationssikkerhedssystemets robusthed og effektivitet ved at foretage en gennemgang af en uvildig part.

Afvigelser

Hvis der opstår situationer, hvor kravene til informationssikkerhedspolitikken ikke kan efterleves, skal der skriftligt anmodes om dispensation af RMC's rektor. Eventuelle afvigelser fra kravene skal dokumenteres, og der skal indføres alternative sikringsforanstaltninger.

Revision

Som led i den overordnede informationssikkerhedsstyring vurderer ledelsen, på baggrund af den løbende overvågning og rapportering, informationssikkerhedspolitikken hvert år, eller efter behov. Såfremt der er ændringer, godkendes disse af rektor.

Godkendt d. 18. november 2025

Henrik Sveidahl
Rektor