

Policy for informasjonssikkerhet – Artisti AS

Vedtatt av Artisti AS styre. Sist endret 3. april 2025.

Policyerklæring

Vi forplikter oss til å beskytte all informasjon vi behandler. Dette gjelder både vår egen og den som tilhører kunder, leverandører, samarbeidspartnere og ansatte.

Vi har et særskilt ansvar for å sikre personopplysninger (PII) og immaterielle rettigheter (IPR). Vi forplikter oss til å håndtere all informasjon på en lovlig, sikker og etisk forsvarlig måte.

Vi anerkjenner at god informasjonssikkerhet er en forutsetning for tillit hos våre kunder og samarbeidspartnere. Policyen er forankret i selskapets styre og revideres minst en gang pr år.

Omfang

Artistis policy for informasjonssikkerhet gjelder all informasjonsbehandling internt i virksomheten og som virksomheten har ansvaret for eksternt. Dette omfatter all behandling, lagring og sending av informasjon både muntlig, på papir og digitalt. All bruk av IKT-verktøy er også inkludert. Policyen gjelder for alle ansatte, konsulenter, leverandører og samarbeidspartnere som behandler informasjon på vegne av Artisti.

Mål og prinsipper for informasjonssikkerhet

Vårt arbeid med informasjonssikkerhet bygger på følgende prinsipper:

- **Tilgjengelighet** - at informasjonen er tilgjengelig når den trengs.
- **Konfidensialitet** - at informasjonen kun er tilgjengelig for de som har rett til innsyn i den.
- **Nøyaktighet og integritet** - at informasjonen er og forblir nøyaktig, forståelig og fullstendig.
- **Sporbarhet** - at du i etterkant kan identifisere hvem som gjorde hva og når.

I tillegg foreligger følgende prinsipper:

- Beskytte kunders personopplysninger og sikre etterlevelse av GDPR og annen relevant lovgivning.
- Beskytte samarbeidspartneres immaterielle rettigheter og konfidensiell informasjon.
- Sikre at informasjonssikkerhet er integrert i alle arbeidsprosesser og systemendringer.

Samsvar

All informasjon behandles og beskyttes i samsvar med:

- Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (Arbeidsmiljøloven).
- Lov om behandling av personopplysninger (Personopplysningsloven) (GDPR EU 2016/679).
- Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale.

Ansvarstildeling

Ansvaret for informasjonsbehandling og informasjonssikkerhet er lagt til virksomhetens øverste ledelse i samarbeid med konsernets informasjons- og datasikkerhetsavdeling i Mediehuset Andvord AS.

Sertifisering

Konsernets informasjons- og datasikkerhetsavdeling i Mediehuset Andvord AS er sertifisert i ISO 27001:2022.

Risikoanalyse og systemtest

Risikoanalyse utføres regelmessig av konsernets sikkerhetsgruppe i samarbeid med eksterne eksperter. Nødvendige tiltak for beskyttelse av informasjon blir gjennomgått og fulgt opp. Virksomhetens sikkerhetsrutiner blir regelmessig vurdert, og eventuelt tilpasset.

Opplæring

Det er obligatorisk opplæring og trening for ansatte innenfor informasjons- og datasikkerhet. Opplæringen omfatter all behandling av informasjon, rutiner og grunnleggende datasikkerhet, og innebærer onlinebaserte kurs (Nano Learning). Det tas ut rapport på gjennomførte onlinekurs blant de ansatte. Gjennom tilfeldige tester blir ansatte testet i trygg bruk av digitale flater og datasikkerhet.

Målsetning: >90% skal ha gjennomført begge kurs i informasjons- og datasikkerhet til enhver tid.

Operasjonell sikkerhet

Vi sørger for at endringer i virksomheten, forretningsstrategier eller systemer for informasjonsbehandling som påvirker informasjonssikkerheten blir kontrollert. Vi har iverksatt overvåking og prosesser for å identifisere, forebygge og håndtere datalekkasjer eller andre sikkerhetsrelevante hendelser i infrastrukturen.

Kommunikasjonssikkerhet

Vi har endepunktadministrasjon som gjør oss i stand til å vedlikeholde, vurdere og beskytte apper og enheter. Vi etablert sikkerhetsløsninger med overvåking av alle enheter og endepunkter (pc/mac/servere) Vi har etablert sikkerhetsløsninger med overvåking av all datakommunikasjon som filoverføring, e-post og alle sky-baserte tjenester.

Løsningene innebærer deteksjon, analyse og varsling til vårt sikkerhetspersonell dersom det oppstår en hendelse. Ved alvorlige hendelser blir endepunkt automatisk isolert inntil årsak er avklart og godkjent av sikkerhetspersonell. Vi har løsninger for analyse av brannmurer og lagring av logger.

Sikkerhetsprosedyrer

Rutiner og prosedyrer for informasjonssikkerhet er beskrevet i interne prosedyredokumenter. Prosedyrer og rutiner blir gjennomgått årlig eller ved avvik og hendelser som krever tiltak.

Avvik og hendelseshåndtering

Alle ansatte har tilgang til portal for registrering av avvik. Avvikene sendes til sikkerhetsansvarlig i virksomheten. Tiltak blir iverksatt. Avvik blir gjennomgått og vurderer endring i infrastruktur, prosesser og organisering.

Varsling

Varsling om uønskede hendelser kan rettes til virksomhetens øverste ledelse (ta@artisti.no) eller direkte til konsernets IT-driftsavdeling (it-avd@artisti.no).

Systemer informasjons- og datasikkerhet

Virksomheten benytter følgende programvarer i våre systemer:

Programvare	Bruksområde
Microsoft Intune	Løsning for endepunktadministrasjon for å administrere, vurdere og beskytte apper og enheter.
XDR (Extended Detection and Response) fra Trend Micro Systems	Endepunktssikkerhet med overvåking, deteksjon, analyse og varsling for alle enheter, kommunikasjonskanaler og skybaserte tjenester for lagring.
NanoLearning	Opplæring og trening av ansatte innenfor informasjon- og datasikkerhet
ManageEngine Firewall Analyzer	Analyse av brannmurer og lagring av logger.
Microsoft Azure med Single Sign-on	Tilgangsstyring for brukere, og provisjonering av informasjon til andre systemer.
NetSecurity / Palo Alto	Network Security fra Palo Alto-plattformen for brannmur og nettverkssikkerhet.

Versjonslogg:

Dato	Endring	Ansvarlig
13.04.2021	Endring i dokumentformat	Monica Nilsen
24.11.2023	Navnendring – Artisti Profil AS -> Artisti AS	Monica Nilsen
03.04.2025	Justert for tydeligere erklæring og forpliktelser	Monica Nilsen