1 FÖRUTSÄTTNINGAR

1.1 Målgrupp

Detta dokument berör alla inom Malmö Opera. Policyn omfattar all personal (oavsett anställningsform) samt övriga parter som i någon form har behörighet till Malmö Operas IT-system.

1.2 Syfte

IT-policyn skall sätta riktlinjer för de anställda och beskriver hur Malmö Opera (nedan kallat företaget) vill att den anställde skall agera i olika sammanhang gällande IT-relaterade frågor. Genom att alla följer den implementerade IT-policyn skapas bättre förutsättningar för att IT som funktion ska fungera på bästa tänkbara sätt. Verksamheten är beroende av att IT-miljön fungerar. Företagets IT-resurser ägs av företaget och är avsedda att användas inom företagets verksamhetsområden. All annan användning får endast förekomma i begränsad omfattning.

1.3 Uppföljning och revidering

IT-ansvarig ansvarar för att IT-policyn kontinuerligt följs upp samt revideras efter behov.

2 ANSVAR

2.1 Användarkonton och lösenord

Varje användare ansvarar för sina konton. Konton får inte göras tillgängliga för andra. Lösenordet är personligt och får inte lämnas vidare. Om det misstänks att någons konto eller lösenord används av annan användare, ska lösenordet omedelbart bytas.
IT-miljön får inte användas på ett sätt som vållar problem eller skadar enskild person eller företagets anseende vare sig direkt eller indirekt. Detta inkluderar att göra intrång eller på annat sätt skaffa sig tillgång till information, konton eller system som den anställde ej har behörighet till. Eventuella överträdelser kan leda till diciplinära åtgärder.
Krav vid lösenordshantering: Se separat lösenordspolicy på intranätet.

2.2 IT-avdelningens ansvar

IT-ansvarig ansvarar för IT-avdelningens verksamhet samt att IT-systemen lever upp till den säkerhet som kan anses rimlig, samt att återställnings- och kontinuitetsrutiner etableras.

2.3 Planerade underhåll

IT-ansvarig kommer att utföra schemalagt underhåll på alla maskiner veckovis för att säkerställa driften och säkerheten i IT-miljön. Under detta underhåll kan funktioner i IT-miljön vara nedsatta eller otillgängliga.

2.4 Support

Användare som vid nyttjande av företagets IT-resurser upptäcker fel eller annat som kan vara av betydelse för IT-driften inom företaget (incident), skall genast rapportera detta till IT-avdelningen, helpdesk@malmoopera.se

3 INTERNETANVÄNDNING

3.1 Nät- och bandbredd

Det är viktigt att alltid undvika att utnyttja nätverksbandbredden för privata ändamål under arbetstid. Detta för att bandbredden har en belastningsgräns och företagets arbetsrelaterade tjänster, filhantering och surfhastighet prioriteras för att bibehålla prestanda.

3.2 Internetanvändning och molntjänster

Företaget har idag ett omfattande användande av molntjänster i sin dagliga verksamhet, vilket innebär ett betydande internetanvändande för flertalet medarbetare.
Privat surfande skall undvikas på arbetstid.
Undvik att besöka sajter vars innehåll bryter mot företagets etiska regler. Detta kan till exempel vara sajter med rasistiskt, pornografiskt eller politiskt extremt innehåll. Det kan också vara sajter som innehåller någon form av olaglig information.
En anställd skall alltid iaktta största möjliga försiktighet vid nedladdning av eventuella dokument och endast göra detta från kända källor.
All användning av internet registreras i en logg. Loggningen omfattar uppgifter om användarnamn och namnet på den webbplats som besökts. Kontroll av enskilda individers internetanvändande kan komma att utföras. Företagets IT-resurser får inte nyttjas för att på otillbörligt sätt sprida, förvara eller förmedla information som strider mot gällande lagstiftning.
Företagets IT-resurser får inte användas till aktivitet som strider mot PULs eller GDPRs stadgar om den personliga integriteten eller syftar till att marknadsföra produkter eller tjänster utan anknytning till företaget.

3.3 E-post

All användning av e-post skall gälla arbetsrelaterad korrespondens. Privat korrespondens ska ej förekomma.

- All mejlkommunikation registreras i en logg. Loggningen omfattar uppgifter om användarnamn och namnet på mottagaren samt innehåll i mejlet. Kontroll av enskilda individers mejl kan komma att utföras om det råder misstanke om brott mot policy.
- Alla sända och mottagna mejl är företagets information, ej den enskilda anställdas.
- Filer och länkar från okända avsändare eller misstänkta filer och länkar från kända avsändare bör aldrig öppnas. Detta av säkerhetsskäl för att undvika virus och skadlig kod. Ring avsändaren och kontrollera om du är osäker, rapportera incident till IT-ansvarig.
- Anställda får inte skicka mejl från en annan användares mejlkonto utan dennes godkännande.
- Det är förbjudet att läsa andra medarbetares e-post utan dennes medgivande.

● Dela aldrig vad som kan anses vara känslig information via mejl. Exempel på känslig information är kreditkorts-information, lösenord eller någons personuppgifter då respekt för dennes integritet bör iakttas.
● Vid de tillfällen personuppgifter behöver delas via e-post skall korrespondens och data raderas vid tillfälle då nyttjandet är klart. Detta gäller för både avsändare och mottagare för korrespondensen. Detta för att underlätta arbete och spårbarhet i enighet med GDPR.

3.4 Sociala medier inom arbetsrelaterad användning

Vid skapande av ett nytt officiellt företagskonto på sociala medier krävs godkännande från närmsta chef med verksamhetsansvar. Sociala medier är ett viktigt verktyg i företagets externa kommunikation. Dessa kan förenkla kommunikationen med ny och befintlig publik men även göra företaget stor skada vid misstag eller felaktigt användande. Som anställd förväntas du följa de användarvillkor och riktlinjer som respektive socialt medium har. Av denna anledning kräver företaget att du som anställd läser igenom respektive socialt mediums användarvillkor och riktlinjer så att du har god kännedom om hur man ska och bör agera. Som anställd förväntas du företräda företaget professionellt, korrekt och för företagets bästa i företagets sociala medier. I de fall du som anställd publicerar inlägg i företagets externa kanaler ska inlägg handla om de områden som företaget agerar inom, t.ex. nyheter om företaget, våra produktioner, branschinformation, tips och idéer etc. som på ett sakligt sätt skapar en objektiv bild av oss. Regler för sekretess och affärshemligheter får inte äventyras på sociala medier. Eventuella överträdelser kan leda till diciplinära åtgärder.

3.5 Användning av sociala medier med privata konton

Det är inte acceptabelt att som anställd interagera med sociala medier på ett vis som kan reflektera negativt på företaget. Detta kan vara fall som, men inkluderar ej alla, negativa kommentarer om arbetsgivaren, spridning av konfidentiell information, kränkande kommentarer om arbetskollegor eller arbetskollegors skötsel av arbetsuppgifter. Denna typ av agerande kan leda till arbetsrättsliga konsekvenser enligt lojalitetsplikten.

4 ÖVERVAKNING OCH FJÄRRSTYRING

4.1 Information

All information som finns på lagringsytor som på något sätt kontrolleras eller ägs av företaget eller leverantör till företaget är företagets egendom. Anställd som har givits tillstånd att använda företagets eller annan parts material måste respektera upphovsrätt och kan därmed inte kopiera, modifiera eller vidarebefordra upphovsrättsskyddat material till annan part utan upphovsrättsmannens tillåtande. Det är inte heller tillåtet att förändra eller förmedla material skapat av annan utan dennes kännedom och/eller medgivande.

4.2 Missbruk/Överträdelse

Vid allvarligare missbruk av företagets it-resurser kan disciplinära åtgärder komma att vidtas. Lagöverträdelse polisanmäls alltid.

4.3 Sekretess

Ingen anställd, inhyrd personal eller annan person som omfattas av företagets IT-policy får lämna ut konfidentiell information till någon utomstående. Vid upphörande av anställning skall konfidentiell information återlämnas till av företaget utsedd person.

5 PROGRAMVARA, HÅRDVARA, IT-SYSTEM OCH TJÄNSTER

5.1 Inköp

All hårdvara, mjukvara och tjänster för IT skall köpas in av IT-avdelningen. En överenskommelse skall alltid godkännas av IT-chefen och/eller ansvarig sektionschef.

5.2 Standardarbetsplats

Standardarbetsplatsen innefattar dator/klient med kringutrustning, exempelvis monitor, mobiltelefon, program och mjukvara. Inköp för särskilda behov av programvaror och tillbehör hanteras av IT-avdelningen i samråd med sektions-/avdelningschef. Beslut om större investeringar sker i samråd med företagsledningen.

5.3 Hårdvara/Enheter

Anställda eller inhyrd personal får ej på eget bevåg införskaffa eller installera hårdvara eller annan utrustning såsom mobila enheter, bärbara datorer, stationära datorer, som inte först har godkänts av IT-ansvarig person/företag. Brukaren av företagets IT-utrustning skall alltid behandla utrustningen varsamt och med aktsamhet. Förbrukad hårdvara/mjukvara skall återgå till IT-avdelningen för säker rensning och återvinning.

5.3.1 Hårdvara försedd av företaget

Företagets IT-avdelning ansvarar för att enheter bibehåller en god nivå för säkerhet i form av antivirus och att regelbunden uppdatering av operativsystem genomförs.

5.3.2 Användning av personliga enheter

Den anställda eller inhyrd personal har möjlighet att använda sina egna enheter, så som mobiltelefoner, surfplattor och bärbara datorer. Det är då den anställdas ansvar att upprätthålla en god säkerhetshygien av sina enheter genom att regelbundet uppdatera sina enheters operativsystem samt förse datorer med antivirus skydd. Vid upphörande av anställning skall konfidentiell information återlämnas till av företaget utsedd person, eventuellt kan den anställda krävas återställa sina enheter till fabriksinställningar.

5.4 Mjukvara

Anställda eller inhyrd personal kan ej på eget bevåg införskaffa eller installera/avinstallera program på företagets datorer. All installation av mjukvara hanteras av it-avdelningen. Den data som lagras på servrar eller på datorers hårddiskar tillhör företaget under iakttagande av gällande sekretessbestämmelser.

6 INCIDENTHANTERING INOM IT

6.1 Bakgrund

Företaget vill att alla medarbetare ska ha grundförståelse i åtgärder och vilka riktlinjer som bör följas vid en IT-säkerhetsincident. Genom att tydligt definiera dessa åtgärder kan vi förbättra organisationens förmåga att hantera och minimera skador vid eventuella säkerhetsintrång.

6.2 Rapportera incidenten

Den anställda skall omedelbart rapportera misstänkt incident till sin närmaste chef eller till IT-avdelningen. Ju tidigare en incident rapporteras, desto snabbare kan åtgärder vidtas.

6.3 Isolera drabbade system

Om den anställda misstänker att dennes dator eller system är kompromitterat, bör de omedelbart isolera enhet -en/-erna från nätverket. Detta minskar risken för att en pågående attack sprids.

- Nätverksisolering: Koppla bort nätverkskablar från enheten, alternativt koppla bort enheten från det trådlösa nätverket. Ifall dessa alternativ inte är möjliga så är det bättre att stänga av enheten än att sitta och invänta IT.
- Användarkonton: Om anställd misstänker att deras konto är kompromitterat så skall de byta lösenord med omedelbar verkan. Sedan skall incidenten rapporteras till IT för vidare analys av vad som kan ha hänt med kontot och om eventuellt data har stulit eller ändrats.

6.4 Samarbeta med IT

Den anställda bör samarbeta med IT för att utreda incidenten. Tillsammans kan IT och anställda hjälpa till att analysera loggar för att identifiera vilken trafik som inte är anställds. På så vis kan IT på ett mer effektivt vis identifiera angreppsmetoder och vidta åtgärder för att förhindra framtida incidenter.

6.5 Incidentgenomgång

IT bör återkoppla till anställda med ett kortare presentationstillfälle där de vid detta tillfälle presenterar händelseförlopp och förklarar hur incidenten inträffat. Remediering av problemet kommer även presenteras, om en sådan finns vid presentationstillfället. Remediering kan vara utbildning inom olika typer av attacker, adderade lager av skydd vid autentisering, etc..

7 UTBILDNING OCH MEDVETENHET INOM IT-SÄKERHET

7.1 Bakgrund

Företaget vill säkerställa en trygg och säker arbetsmiljö därför är det viktigt att alla anställda har en god förståelse för IT-säkerhet. Detta avsnitt beskriver företagets åtagande att utbilda och öka medvetenheten om IT-säkerhet.

7.2 Syfte

Syftet är att alla anställda ska vara medvetna om risker och god praxis inom IT-säkerhet. Genom utbildning och kontinuerlig medvetenhet kan vi minska sårbarheter och skydda våra tillgångar.

7.3 Utbildning och Träning

Obligatorisk IT-säkerhetsutbildning: Alla anställda ska genomgå regelbunden utbildning om IT-säkerhet. Detta inkluderar grundläggande säkerhetsprinciper, hantering av lösenord, e-posthantering och säker surfning.

Specialiserad utbildning: Anställda som hanterar känslig information eller specifika system bör få specialiserad utbildning.

7.4 Medvetenhet och Kommunikation

Rapportering av incidenter: Alla anställda bör veta hur man rapporterar misstänkta säkerhetsincidenter.

7.5 Ansvar

Ledningens ansvar: Ledningen är ansvarig för att främja en kultur av IT-säkerhet och tillhandahålla resurser för utbildning.

Anställdas ansvar: Varje anställd är ansvarig för att följa IT-säkerhetsriktlinjer och rapportera eventuella avvikelser.

8 RIKTLINJES BROTT

Vid tillfälle då anställd inte har följt företagets riktlinjer för internetanvändning och bedöms ha gjort detta på ett medvetet och oaktsamt vis så kan detta få allvarliga konsekvenser som påföljd.

1. **Skriftlig varning:** För mindre allvarliga överträdelser kan en anställd tilldelas en skriftlig varning. Detta fungerar som en påminnelse om att fortsättningsvis följa angivna riktlinjer.
2. **Uppsägning:** Allvarliga överträdelser kan leda till uppsägning av anställningen. Detta gäller särskilt om internetanvändning har skadat företagets rykte eller säkerhet.
3. **Rättsliga åtgärder:** Om en anställd har begått allvarliga brott, så som stöld eller andra olagliga aktiviteter via företagets internetanslutning, kan rättsliga åtgärder vidtas.