

IT/Säkerhetspolicy

1. Introduktion

Syfte: Denna IT-policy syftar till att skydda organisationens information, teknikinfrastruktur och upprätthålla en effektiv, produktiv och säker arbetsmiljö.

Omfattning: Policyn gäller alla anställda och associerade som använder organisationens IT-resurser.

Nyckelansvar: Medan IT-ansvarig har ansvaret för att upprätthålla och övervaka den infrastrukturella integriteten, är varje medlem av organisationen ansvarig för att följa och respektera dessa riktlinjer.

2. Lösenordshantering och inloggning

Komplexitetskrav: Lösenord bör vara minst 12 tecken långa och innehålla en blandning av versaler, gemener, siffror och symboler.

Tvåfaktorsautentisering: Obligatoriskt för att få åtkomst till organisationens e-post. Rekommenderas för andra tjänster där det finns tillgängligt.

Delning av Lösenord: Strikt förbjudet.

Lösenordslagring: Anställda uppmanas att använda lösenordshanteraren godkänd av organisationen.

Misstänkt läckt lösenord: Rapportera omedelbart till IT-avdelningen eller klubbchef.

Anledning: Ett lösenord bestående av ett vanligt ord tillsammans med några siffror tar enbart ett par minuter att knäcka

4. Antivirus

Antiviruspåbud: Alla företagsenheter kommer att ha ett antivirusprogram godkänt av IT, som uppdateras automatiskt.

Misstänkt programvara: Rapportera omedelbart vid oregelbundenheter.

Förbjudna åtgärder: Ingen inaktivering av antivirus eller nedladdning från obekräftade källor.

5. Företagsutrustning

Definition: Detta inkluderar teknisk utrustning såsom laptops, stationära datorer, mobiltelefoner, surfplattor och relaterade enheter som tillhandahålls för arbete.

Användningsriktlinjer: Förvara säkert. Lämna aldrig olåst.

Försvunnen/Stulen utrustning: Rapportera omedelbart till IT eller klubbchef.

6. Kommunikation

Godkända plattformar: Använd plattformar som tillhandahålls av organisationen, till exempel Microsoft Teams och e-post via Microsoft Outlook.

Beteenden: Dela inte känslig information utanför säkra kanaler.

7. Godtagbar e-postanvändning

Syfte: Föreningens e-post är för professionell kommunikation relaterad till jobbroller och ansvarsområden.

Användning: Dela inte känslig data. Undvik att skicka skräppost eller vidarebefordra obekräftad information.

Varumärkesprofilering: Följ företagets riktlinjer för e-postsignaturer.

Medvetenhet om Phishing: Klicka inte på misstänkta länkar eller dela uppgifter. Rapportera misstänkta e-postmeddelanden till IT eller klubbchef.

8. Datasäkerhet och Integritet

Dat klassificering: Var medveten om datakänslighet (Offentlig, Intern, Konfidentiell) och hantera därefter.

Lagringsriktlinjer: Förvara data på tilldelade säkrade platser/drivenheter.

Intrång: Larma IT eller klubbchef omedelbart om du misstänker ett dataintrång.

9. Tillämpning och konsekvenser

Övervakning: IT kommer periodvis att granska efterlevnaden.

Överträdelser: Beroende på allvarlighetsgrad kan konsekvenserna bli varningar.

Rapporteringsmekanism: Anställda kan anonymt rapportera potentiella överträdelser eller bekymmer.

Framtida delar:

- AI-policy
- Internetanvändning och övervakning
- Företagsutrustning: VPN vid hemma-arbete