IT-policy

Omfattning

Denna IT-policy omfattar alla anställda, inhyrd personal, konsulter och andra som får tillgång till Arconas IT-system. Syftet är att uppnå säker och effektiv användning av IT-systemen genom en gemensam uppsättning regler för acceptabel användning i hela Arcona. Begreppet IT-utrustning innefattar vanligtvis användarutrustning såsom datorer med tillbehör, skrivare, mötesrumsutrustning, mobiltelefoner, surfplattor och relevanta tillbehör.

Användandet av IT-system

- Du är ansvarig för din arbetsplats och dess verktyg, och har därför rapporterings-skyldighet om något skiljer sig från normalt. Systemen är i första hand till för att tillgodose Arconas behov, men får utnyttjas för privat bruk i rimlig omfattning. All användning ska ske på ett ansvarsfullt och genomtänkt sätt
- Endast godkänd IT-utrustning får anslutas till Arconas företagsnätverk. All annan IT-utrustning, inklusive privat IT-utrustning, skall endast anslutas till det trådlösa gästnätverket.
- Systemen ska användas utan att Arcona utsätts för onödiga risker eller förknippas med kriminell eller omoralisk verksamhet.
- Du får ett epostkonto av Arcona som används för intern och extern kommunikation och skyddas enligt de regler som gäller för lösenord och återställning. Även här gäller det att visa omdöme vid användning.
- Det är inte tillåtet att använda Arconas e-postadress för att registrera dig på webbplatser eller tjänster för privata ändamål.
- GDPR-lagen innebär att du inte får skicka/spara personuppgifter utan samtycke eller ändamål som krävs för verksamheten.
- Som användare av IT-system förbinder man sig att delta i de av Arcona tillhandahållna utbildningar i IT-säkerhet såsom Nanolearning.

Sekretess

- Personuppgifter ska hanteras i enlighet med GDPR.
- All information som finns lagrad i vår IT-miljö ägs av Arcona och behandlas med sekretess.
- Ingen information om IT-miljön får spridas utanför Arcona. Vi ska inte delta i marknadsundersökningar inom IT-, data och telefoniområdet.

ARCONA

Artificiell intelligens (AI)

Arcona använder AI-tjänster inom olika områden, när du använder AI-tjänster gäller följande:

Undvik att dela känslig information som personnummer, bankuppgifter, lösenord och intern Arcona-information. Det finns en risk att obehöriga får tillgång till den information du delar. Var medveten om att resultaten du får kan omfattas av upphovsrättsliga bestämmelser. Var kritisk till informationen du får från AI-tjänster, den kan vara felaktig och måste granskas manuellt.

Installationer

Alla applikationer ska installeras och konfigureras centralt av Arconas IT-leverantör.

Inköp

Inköp av ny hård- och mjukvara ska alltid godkännas av IT-råd, IT-chef eller IT-leverantör.

Hårdvara

Du ansvarar för utkvitterad hårdvara, och ska återlämna denna vid anställningens upphörande eller på annan anmodan.

Lokaler

För att skydda information och utrustningar är det viktigt att säkerhetssystem i Arconas lokaler hanteras på rätt sätt. Hit räknas hantering av passer- och ID-kort, aktivering av larm och att de dörrar och fönster som ska vara låsta och stängda är det.

Stöldskydd

Du ska hantera Arconas IT-utrustning med största försiktighet, och alltid minimera risken för stöld, vilket innebär att

- Du bör ha koll på bärbara datorer, mobiltelefoner och liknande utrustning.
- Bärbar dator bör gömmas undan om den lämnas utom synhåll under längre tid.
- Bärbar dator får inte lämnas i bil eller på annat obevakat ställe.

Stulen/förkommen hårdvara eller information ska inom 72 timmar anmälas till Arconas Personuppgiftsincidentgrupp, (namnen finns i Arconas medarbetarportal under GDPR Hantering av personuppgifter) som rapporterar personuppgiftsincident till Integritetsskyddsmyndigheten (IMY).

Lösenord och åtkomst

- Användaridentiteten och lösenordet är personliga handlingar. Du ansvarar själv för att upprätthålla säkerheten genom att inte sprida uppgifterna till vare sig kollegor, familj eller andra personer. Användaridentitet och lösenord bör inte sparas på samma plats. Ditt lösenord får inte heller återanvändas utanför Arcona. Om du vet eller misstänker att ditt lösenord har blivit känt för obehöriga måste du omedelbart ändra ditt lösenord.
- Din dator måste vara utloggad eller låst (Win+L) när du lämnar arbetsplatsen.

IT-säkerhetsincidenter & Riskhantering

- Om det finns misstankar eller att en IT-säkerhetsincident inträffat, såsom till exempel virusattacker, stulen/förlorad IT-utrustning och lösenord som kommer på avvägar, måste detta omedelbart rapporteras till Arconas IT-leverantörs Helpdesk på 08-545 726 35.

Kontroll/revision

IT policy och övriga säkerhetsåtgärder granskas på årsbasis och avrapporteras till ledningen. Vid denna översyn granskas också förändrade lagkrav för att säkerställa efterlevnad. Vid behov tas extern part in för revision.

2026-01-01

Peter Kvist VD, Arcona AB

PKvist