2026-08-21

Cybersäkerhetspolicy

Syfte

Denna policy fastställer de principer och åtgärder som Nova Åkeri AB tillämpar för att skydda företagets information, IT-system och personuppgifter mot obehörig åtkomst, förlust eller felaktig användning.

Omfattning

Policyn gäller för samtliga anställda, underleverantörer och andra personer som har tillgång till företagets system eller information.

1. Principer för informationssäkerhet

- Företagets information ska hanteras på ett säkert sätt och endast vara tillgänglig för behöriga personer.
- Personuppgifter ska behandlas i enlighet med GDPR och företagets interna styrande dokument.
- Konfidentiell information får inte delas med obehöriga personer.

2. Hantering av åtkomst och lösenord

- Anställda ska använda starka lösenord och hålla dem hemliga.
- Behörighet till företagets system tilldelas utifrån arbetsuppgifter och ansvarsområde.
- Användarkonton och lösenord får inte delas mellan anställda.
- Behörigheter ska ändras eller tas bort när en persons arbetsuppgifter förändras eller anställningen eller samarbetet upphör.

3. Användning av IT-utrustning

- Företagets IT-utrustning ska användas på ett ansvarsfullt sätt och i första hand för arbetsrelaterade ändamål.
- Programvara får inte installeras utan godkännande.
- Anställda ska undvika att öppna misstänkta länkar eller ladda ner filer från okända eller osäkra källor.
- Företagets utrustning ska skyddas mot obehörig åtkomst och får inte lämnas oskyddad.

4. Dataskydd och lagring

- Dokument som innehåller personuppgifter, konfidentiell information eller annan känslig information ska lagras och hanteras på ett säkert sätt.
- Företagets digitala arbetsdokument lagras på företagets datorer och säkerhetskopieras automatiskt till NAS-servern.
- Viktiga dokument bevaras även i pappersform när det är relevant.
- Information får inte överföras till obehöriga externa enheter, privata lagringslösningar eller ej godkända plattformar.
- Endast behöriga personer ska ha tillgång till lagrad information och säkerhetskopior.

5. Rapportering av IT- och personuppgiftsincidenter

Misstänkta cybersäkerhetsincidenter ska omedelbart rapporteras till företagsledningen.

Exempel på incidenter är:

- misstänkta e-postmeddelanden, länkar eller bilagor;
- försök till nätfiske eller dataintrång;
- obehörig åtkomst till företagets system;
- förlust eller stöld av dator, telefon eller annan utrustning;
- oavsiktlig delning av personuppgifter eller annan känslig information;
- förlust eller otillgänglighet av företagsinformation.

6. Hantering av incidenter

- Företagsledningen ska bedöma incidenten och vidta omedelbara åtgärder för att begränsa eventuell skada.
- Behörigheter kan begränsas och system kan tillfälligt stängas av när det är nödvändigt.
- Berörda system och uppgifter ska säkras och incidentens orsak ska utredas.
- Vid behov ska lösenord ändras och berörda personer, leverantörer eller försäkringsbolag kontaktas.

- Om personuppgifter berörs ska incidenten hanteras enligt GDPR, inklusive anmälan till behörig tillsynsmyndighet när detta krävs.
- Incidenten och vidtagna åtgärder ska dokumenteras och följas upp.

7. Ansvar

- Samtliga anställda och andra personer med tillgång till företagets system ansvarar för att följa denna policy.
- Verkställande direktören ansvarar för den övergripande uppföljningen av cybersäkerheten och hanteringen av incidenter.
- Användare ansvarar för att omedelbart rapportera misstänkta händelser, säkerhetsbrister och förlorad utrustning.