Styrdokument
Dokumenttyp: Regler
Beslutat av: Kommunstyrelsen
Fastställelsedatum inkl. dnr: 2026-01-14 §8, KS.2025.198
Gäller för: Gislaveds kommuns organisation
Ansvarig: Avdelningschef verksamhetsstyrning och it
Revideras: vid behov eller vart fjärde år
Följs upp: It-enheten

Regler för it-användning och informationsskydd

2025-11-26

Innehållsförteckning

1 Syfte

Reglerna anger krav för säker användning av kommunens digitala resurser och informationshantering. De gäller för alla som använder kommunens it-miljö och syftar till att skydda information, system och verksamhet.

2 Omfattning

Reglerna gäller för:

- alla medarbetare, förtroendevalda, konsulter och andra med åtkomst till kommunens it-resurser
- all hantering av arbetsrelaterad information, oavsett plats och enhet
- all användning av kommunens system, tjänster, program och utrustning

3 Ansvar

- Varje användare ansvarar för att följa dessa regler och agera så att kommunens information och system skyddas.
- Chef ansvarar för att medarbetare, konsulter och andra i verksamheten känner till och följer reglerna.
- Avdelningen verksamhetsstyrning och it ansvarar för stöd, uppföljning och kontroll av efterlevnad samt för att kommunicera aktuella säkerhetskrav och säkerhetsmeddelanden.

Brott mot reglerna, inklusive försök att kringgå tekniska skydd eller säkerhetslösningar, kan leda till indragen åtkomst, incidentutredning eller arbetsrättsliga åtgärder.

4 Grundläggande säkerhetsprinciper

Kommunens information ska skyddas enligt principerna som redogörs i kommunens informationssäkerhetspolicy.

Kommunens it-miljö är loggad och spårbar. Aktiviteter i system och nätverk kan registreras och granskas för att upptäcka, förebygga och utreda säkerhetsincidenter, i enlighet med gällande lagstiftning och interna rutiner.

All hantering av information ska följa kommunens informationsklassningsmodell och tillhörande skyddsnivåer.

5 Identitet och åtkomst

5.1 Personliga uppgifter

- Inloggningsuppgifter är personliga och får inte delas med någon annan.
- Misstanke om att inloggningsuppgifter röjts ska omedelbart rapporteras enligt avsnitt 10.

5.2 Lösenord

- Lösenord ska följa kommunens krav på styrka och komplexitet.
- Lösenord får inte förvaras synligt eller i okrypterade dokument.
- Lösenord får inte skickas via osäkra kanaler.

5.3 Flerfaktorautentisering (MFA)

- MFA ska användas där kommunens säkerhetskrav anger det.
- MFA får inte kringgås eller inaktiveras.

6 Hantering av digital kommunikation

Användare ska följa säkerhetsmeddelanden, varningar och instruktioner från it-enheten och informationssäkerhetsfunktionen, inklusive krav på uppdateringar, förändrade arbetssätt och åtgärder vid incidenter.

6.1 E-post

- E-post används i första hand för arbetsrelaterad kommunikation.
- Information och dokument ska inte lagras i e-postsystemet utan flyttas till system eller annan lagringsplats i enlighet med informationshanteringsplan.
- Känslig eller skyddsvärd information får endast skickas enligt kommunens säkerhetskrav och informationsklassning.
- Misstänkt e-post (phishing, okända bilagor, oväntade länkar) ska inte öppnas och ska hanteras enligt it-enhetens anvisningar.

6.2 Internetanvändning

- Internet får endast användas på ett sätt som inte utsätter kommunen för säkerhetsrisker.
- Nedladdning av program, tillägg eller filer som kan påverka säkerhet eller drift får endast ske enligt it-enhetens anvisningar.
- Webbplatser och tjänster som bedöms osäkra får inte användas.

6.3 Sociala medier och meddelandetjänster

- Arbetsrelaterad information får endast delas i kommunens godkända system/tjänster.
- Sociala medier, externa chattappar och privata lagringstjänster får inte användas för arbetsinformation eller personuppgifter om de inte uttryckligen godkänts.

7 Informationshantering

- Arbetsrelaterad information ska lagras i kommunens godkända lagringsytor och system.
- Skyddsvärd eller känslig information ska hanteras i enlighet med kommunens informationsklassningsmodell och anvisningar för respektive informationsklass.
- Arbetsrelaterad information får inte lagras i privata molntjänster, på privat utrustning eller i andra ej godkända tjänster.
- Utskrifter, anteckningar och dokument ska hanteras så att obehöriga inte får tillgång till dem.

8 Fysisk och miljömässig säkerhet

8.1 Arbetsplats

- Datorer, mobiler och annan utrustning ska låsas när de lämnas obevakade.
- Utrustning får inte lämnas i allmänna utrymmen utan uppsikt.

8.2 Offentliga miljöer

- Vid arbete utanför kontoret ska skärm och material skyddas mot insyn.
- Samtal om skyddsvärd eller känslig information ska undvikas i miljöer där obehöriga kan höra.

8.3 Distansarbete

- Distansarbete får endast ske via godkända enheter och anslutningar.
- Arbetsmaterial får inte lagras på privat utrustning.
- Skyddsvärd information får endast hanteras när säker anslutning används enligt it-enhetens anvisningar.

9 Användning av AI-tjänster

- Endast AI-tjänster som godkänts av kommunen får användas för arbetsrelaterad information.
- Sekretessbelagd, känslig, personuppgiftsbehandlad eller internt skyddsvärd information får inte matas in i externa AI-verktyg utan uttryckligt godkännande.
- AI-genererat innehåll ska alltid granskas för riktighet, lämplighet och efterlevnad av lagar och interna riktlinjer innan det används.
- Beslut som kräver mänsklig bedömning får inte automatiskt överlåtas till AI, om inte detta särskilt reglerats i verksamheten.

10 Incidentrapportering

Alla it- och informationssäkerhetsincidenter ska omedelbart rapporteras enligt kommunens incidenthanteringsrutin.

Det gäller bland annat:

- misstänkt intrång eller skadlig kod
- förlorad eller stulen utrustning
- felaktig eller oavsiktlig delning av information
- misstänkt phishing eller annan riktad påverkan

Användare ska medverka vid felsökning och utredning enligt anvisningar från avdelningen för verksamhetsstyrning och it.