

| Styrdokument                                              |
|-----------------------------------------------------------|
| Dokumenttyp: Regler                                       |
| Beslutat av: Kommunstyrelsen                              |
| Fastställersedatum inkl. dnr: 2026-01-14 §11, KS.2025.207 |
| Gäller för: Gislaveds kommuns organisation                |
| Ansvarig: Avdelningschef verksamhetsstyrning och it       |
| Revideras: vid behov eller vart fjärde år                 |
| Följs upp: It-enheten                                     |

# Regler för införande och förändring av digitala system, tjänster och utrustning

2025-11-26

## Innehållsförteckning

|    |                                                 |   |
|----|-------------------------------------------------|---|
| 1  | Syfte .....                                     | 3 |
| 2  | Omfattning .....                                | 3 |
| 3  | Ansvar .....                                    | 3 |
| 4  | Grundregler .....                               | 4 |
| 5  | Införande av digitala system och tjänster ..... | 4 |
| 6  | Förändringar av befintliga system.....          | 4 |
| 7  | Upphandling och avtal.....                      | 5 |
| 8  | Tekniska och säkerhetsmässiga krav .....        | 5 |
| 9  | Drift, support och ansvarsfördelning .....      | 5 |
| 10 | Om en lösning inte uppfyller kraven .....       | 5 |
| 11 | Avveckling av system och tjänster .....         | 6 |
| 12 | Uppföljning .....                               | 6 |

# I Syfte

Reglerna säkerställer att digitala system, tjänster och utrustning införs, förändras och avvecklas kontrollerat, säkert och i enlighet med kommunens tekniska, juridiska och informationssäkerhetskrav.

## 2 Omfattning

Reglerna gäller för:

- alla digitala system, tjänster, integrationer och applikationer
- all utrustning som ansluts till kommunens it-miljö
- alla förändringar som påverkar drift, funktion, säkerhet, dataflöden eller informationsklassning
- leverantörer och externa aktörer som tillhandahåller digital funktionalitet

Reglerna gäller oavsett om lösningen är molnbaserad, lokalt driftad, hyrd, licensierad eller utvecklad internt.

## 3 Ansvar

- Verksamheter beskriver behov, processer och krav samt samverkar med it-enheten och andra stödfunktioner i införande och förändring av tjänster och system.
- Chefer säkerställer att beställningar och förändringar sker enligt dessa regler och tillhörande rutiner.
- It-enheten stödjer verksamheten genom bedömningar inom teknik, arkitektur, säkerhet, drift och anslutning.
- Upphandling/inköp involverar it-enheten och informationssäkerhetsfunktionen i digitala avtal.
- Informationssäkerhetsfunktionen ger stöd i risk- och säkerhetsfrågor.

Brott mot reglerna kan leda till stoppat införande, avbruten anslutning, isolering av lösning, incidentutredning eller arbetsrättsliga åtgärder.

## 4 Grundregler

Följande gäller för alla digitala lösningar:

- införande och större förändringar sker genom en kvalitetssäkrad process i samverkan mellan verksamheten, it-enheten och andra stödfunktioner.
- lösningar ska genomgå teknisk och säkerhetsmässig bedömning innan införande, förändring eller avveckling.
- informationsklassning och riskanalys ska genomföras vid behov
- leverantörer ska uppfylla kommunens krav på säkerhet, integritet och drift
- loggning, spårbarhet och åtkomstkontroll ska kunna utföras och vara aktiverad, utifrån verksamhetens behov och gällande rättsliga krav.
- lösningar får tas i bruk först när drift, support och säkerhet är säkerställda

## 5 Införande av digitala system och tjänster

Följande ska alltid hanteras tillsammans med it-enheten innan införande:

- nya system, appar, e-tjänster, integrationer och API-kopplingar
- lösningar som hanterar personuppgifter eller skyddsvärd information
- utrustning som ansluts till nätverket, inklusive IoT och driftutrustning
- lösningar som använder kommunens identitetshantering (IAM)
- automatiseringar som script, flows, makron eller robotstyrning

Införande får påbörjas först när bedömning och beslut är genomförda.

## 6 Förändringar av befintliga system

Verksamheten ska samverka med it-enheten och andra stödfunktioner vid förändringar som påverkar:

- teknisk arkitektur, plattform, nätverk eller driftmiljö
- informationsflöden, datasäkerhet eller klassningsnivå
- integrationer eller systemkopplingar
- större uppgraderingar, modulinföranden eller funktionstillägg
- övergång till moln eller byte av leverantör

Mindre konfigurationer kan genomföras enligt systemets/tjänstens förvaltningsplan.

## 7 Upphandling och avtal

Vid upphandling eller avtal av digital funktionalitet samarbetar verksamheten, it-enheten och informationssäkerhetsfunktionen för att säkerställa:

- tekniska krav och kompatibilitet
- krav på säkerhet, loggning, spårbarhet och åtkomstkontroller
- hantering av personuppgifter och informationsklassning
- krav enligt GDPR, NIS2/cybersäkerhetslag, arkivlag och kommunens säkerhetskrav

Avtal tecknas först när tekniska och säkerhetsmässiga krav är godkända och säkerställda.

## 8 Tekniska och säkerhetsmässiga krav

Alla digitala lösningar ska uppfylla krav på:

- uppdateringar, sårbarhetshantering och livscykelstöd
- dokumentation av drift, funktion och återställning
- övervakning och logghantering
- autentisering, behörighet och segmentering

Lösningar som inte uppfyller kraven kan behöva åtgärdas.

## 9 Drift, support och ansvarsfördelning

Verksamheten och it-enheten säkerställer tillsammans att:

- drift sker på ett sätt som stödjer verksamhetens behov och säkerhetskrav
- lösningens tekniska krav kan upprätthållas långsiktigt
- förvaltning, incidenthantering och support är säkerställda

En lösning får inte införas om långsiktiga krav inte är uppfyllda.

## 10 Om en lösning inte uppfyller kraven

En digital lösning kan behöva åtgärdas om den:

- innebär en säkerhetsrisk
- inte uppfyller tekniska eller juridiska krav
- saknar tillräcklig drift- eller förvaltningskapacitet
- införts utan föregående bedömning

Otillåtet införande kan utredas som säkerhetsincident.

## I I Avveckling av system och tjänster

Vid avveckling säkerställs att:

- information hanteras enligt gällande arkiv- och lagkrav
- data migreras, bevaras eller gallras korrekt
- åtkomster avvecklas enligt IAM-regler
- tekniska komponenter tas bort eller inaktiveras på ett säkert sätt

## I2 Uppföljning

Efterlevnad följs upp genom:

- loggning och teknisk övervakning
- granskning av förändringar och införanden
- säkerhetsbedömningar och kontroller enligt kommunens styrdokument