

# Riktlinje

Gullspångs kommun

## Riktlinje för informationssäkerhet



Beslutad av: Kommunfullmäktige

Datum och paragraf: 2025-09-25, § 81

Dokumentansvarig:  
Informationssäkerhetsstrateg

Gäller från: 2025-10-01

Diarienummer: KS 2025-165



**GULLSPÅNGS  
KOMMUN**

# Innehåll

Riktlinje för informationssäkerhet .....	3
Inledning.....	3
Mål för informationssäkerhet .....	4
Principer och arbetssätt .....	4
Termer och definitioner.....	5
Övergripande riktlinjer för informationssäkerhet .....	7
Dispenser och undantag .....	7
Styrning av informationssäkerhet.....	7
Roller, ansvar och organisation.....	7
Grundläggande princip .....	7
Övergripande roller och ansvar .....	7
Dedikerade roller och ansvar.....	8
Systemägare .....	8
Ansvar i projekt.....	8
IT-avdelning .....	8
IT-säkerhetsspecialist .....	9
Informationssäkerhetsstrateg.....	9
Informationssäkerhetssamordnare.....	9
Informationssäkerhetsnätverk .....	10
A.1. Dokumentstruktur.....	10
A.2. Informationsklassning och riskanalys .....	11
A.3 Ledningssystem för informationssäkerhet (LIS).....	11
A.4 Personalsäkerhet.....	12
Före och i samband med anställning.....	12
Under anställning .....	12
Avslut eller ändring av anställning.....	13
A.5 Leverantörsrelationer.....	13
Efterlevnad och granskning.....	14
Intern kontroll.....	14
Uppföljning av riktlinje.....	14

# Riktlinje för informationssäkerhet

Gullspångs kommuns riktlinje innehåller både kommunens mål och de övergripande riktlinjer avseende informationssäkerhetsarbetet i kommunen.

Denna riktlinje gäller för kommunens samtliga verksamheter. Kommunala bolag ska så långt det är möjligt utifrån aktiebolagslagen följa dessa riktlinjer. För kommunala verksamheter finns det inte utrymme att besluta om lokala regler som avviker från dessa riktlinjer.

Riktlinjen för informationssäkerhet och arbetet med informationssäkerhet baseras på den vedertagna standardserien för informationssäkerhet, SS-ISO/IEC 27000.

## Inledning

Information är en av kommunens viktigaste tillgångar för att genomföra vårt samhällsuppdrag. Kommunens verksamheter och bolag är beroende av tillgång till information för att genomföra verksamheten. Informationen rör exempelvis vår personal, våra tjänster, vår ekonomi och vår omgivning med medborgare, företag och civila samhället.

Information är medieoberoende och kan till exempel vara text, ljud, bilder, film och kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal.

Informationssäkerhet handlar om hur vi skyddar information både utifrån legala krav och för att möta interna och externa intressenters behov. Kraven ställs utifrån tre aspekter – Konfidentialitet, Riktighet och Tillgänglighet, se figur 1 nedan.



Figur 1: Om Informationssäkerhet

En viss informationsmängd har krav på sig gällande de tre aspekterna som kan vara interna eller härledas från rättsliga krav eller förväntningar och behov från externa aktörer. Rättsliga krav i form av lagar, förordningar, föreskrifter och avtal ställer krav på en verksamhets informationshantering som ofta inbegriper krav på informationens konfidentialitet, riktighet och tillgänglighet. Dessutom har ofta externa aktörer behov och förväntningar som påverkar organisationens informationssäkerhet.

Vad som är lämplig nivå av skydd för en viss informationsmängd beror på dessa krav, hotbild, och i vilka situationer informationen hanteras – hur den lagras, bearbetas, kommuniceras osv.

## Mål för informationssäkerhet

Informationssäkerhet har inget egenvärde utan ska bidra till att kommunen och de kommunala bolagen når sina övergripande visioner, strategier och mål.

Det övergripande målet är att:

- Gullspångs kommun och de kommunala bolagen ska etablera och upprätthålla ett systematiskt informationssäkerhetsarbete som säkrar vår verksamhet så den tryggt kan utföras även vid incidenter eller pågående störning.

Målet är kopplat till kommunens vision: Gullspång kommun 2035 - Trygg och levande med driv och mod att utvecklas.

För att uppnå det övergripande målet ska Gullspång kommun och kommunala bolag uppnå en informationshantering som:

- är robust, säker och tillförlitlig,
- löpande förebygger, hanterar och rapporterar incidenter,
- säkrar verksamhetens behov av information,
- ökar kvaliteten på kommunens hantering av information,
- efterlever krav i lagar, förordningar och avtal,
- stärker medarbetarnas säkerhetsmedvetenhet och förmåga att upprätthålla informationssäkerhet i vardagen,
- värnar om den personliga integriteten med hänsyn till den enskildas friheter och rättigheter,
- möjliggör ett aktivt deltagande i det digitala samhället.

## Principer och arbetssätt

Gullspångs kommun och kommunala bolag ska arbeta med informationssäkerhet på ett sätt så att ovanstående strategiska mål uppfylls.

Arbetet med informationssäkerhet ska:

- vara systematiskt enligt gällande författningar,
- utgå från kommunens ledningssystem för informationssäkerhet (LIS) som är normerande, stödjande och kontrollerande,
- löpande ses över och förbättras, eftersom kommunen och de kommunala bolag, samt cybersäkerhetshoten mot dessa, är under ständig förändring,
- vara proaktivt, och ändå ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa,
- bygga på kommunens värderingar och uppfylla lämpliga krav relaterade till informationens skyddsbehov, systemens skyddsbehov, verksamhetens behov, externa krav samt rådande hotbild,

- vara väl kommunicerat till verksamheten; chefer ska tillse att all personal fortlöpande får information och utbildning för att nå och upprätthålla ett högt säkerhetsmedvetande och för att kunna leva upp till denna riktlinje för informationssäkerhet samt underliggande anvisningar,
- följa och samverka med omgivande samhället såsom myndigheter, företag och nätverk - särskilt normgivande aktörer inom informationssäkerhet och dataskydd såsom Myndigheten för samhällsskydd och beredskap (MSB), Integritetsskyddsmyndigheten (IMY) och Sveriges kommuner och regioner (SKR),
- i tillämpliga delar samordnas med kommunens arbete rörande säkerhet och dataskydd.

Dataskydd är en del av arbetet med informationssäkerhet och behandling av personuppgifter innebär unika krav, se kommunens riktlinje Hantering av personuppgifter.

## Termer och definitioner

Term	Definition
Autentisering	Verifiering av att en användare eller IT-resurs är den som den utger sig för att vara.
Behandling av personuppgifter	Behandling av personuppgifter omfattar alla åtgärder som vidtas med personuppgifter, såsom insamling, registrering, organisering, lagring, bearbetning, ändring, framtagning, fotografering, läsning, användning, utlämning, spridning eller tillhandahållande på annat sätt. Även vid justering eller sammanföring, radering eller förstöring är det fråga om behandling av personuppgifter.
Behörighet	Tilldelade rättigheter att använda information eller en IT- resurs på ett specificerat sätt.
Biometriska uppgifter	Är en persons fysiska, fysiologiska eller beteendemässiga egenskaper som gör det möjligt att identifiera människor för exempel via fingeravtryckskanning, ansiktsskanning eller ögonskanning.
Data	Representation av fakta i form av till exempel tecken eller signaler som är lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel.
Dataskydd / Dataskyddsförordningen	Dataskydd eller dataskyddsförordningen avser kommunens behandling av personuppgifter.
Hot	Möjlig oönskad händelse med negativa konsekvenser för verksamheten.
Information	Innebörd i data, d.v.s. data tolkad av människor.
Informationsklassning	Att genom klassificering identifiera skyddsbehovet för en viss informationsmängd.
Informationssäkerhet	Konfidentialitet, riktighet och tillgänglighet hos information.
Informationssäkerhetsincident	En eller flera händelser som kan tänkas få allvarliga konsekvenser för verksamheten och hota informationssäkerheten.

Informationstillgång	Information som är av värde för organisationen, och även de resurser som hanterar den, exempelvis människor, papper, mjukvara, hårdvara och immateriella tillgångar (till exempel rykte).
IT-resurs	IT-baserad komponent som hanterar information, till exempel system, verktyg, tjänster och infrastruktur i form av mjuk- och/eller hårdvara.
IT-säkerhet	Säkerhet i IT-resurser för att uppnå och upprätthålla informationssäkerhet.
Konfidentialitet	Att information inte tillgängliggörs eller avslöjas till obehörig.
Konfidentiell information	Information som endast får vara tillgänglig för medarbetare som har särskild behörighet att hantera informationen, exempelvis sekretessbelagd information, känsliga personuppgifter m.m.
Känsliga personuppgifter	Uppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, uppgifter som rör hälsa, sexualliv eller sexuell läggning samt genetiska och biometriska uppgifter. Patientuppgifter är känsliga uppgifter. Uppgifter om barn är känsliga uppgifter.
Ledningssystem för informationssäkerhet (LIS)	Ett administrativt ledningssystem som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet.
Personuppgifter	All information som direkt eller indirekt kan kopplas till en enskild fysisk individ som är i livet, till exempel namn, adress och personnummer. Även information som beskriver någon eller på annat sätt kan härledas till en enskild individ såsom registreringsnummer på fordon, filmer, bilder, IP-nummer och cookies. Även information som har kodats, krypterats eller pseudonymiserats men som kan hänföras till en enskild individ med hjälp av kompletterande uppgifter klassas som personuppgifter.
Personuppgiftsansvarig	Personuppgiftsansvarig (PuA) är den som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Respektive nämnd och styrelse är personuppgiftsansvarig i kommunen.
Riktighet	Att information är korrekt, aktuell och fullständig.
Risk	Produkten av sannolikheten och konsekvensen att ett hot realiseraras.
Sekretess	Information som inte ska lämnas ut och bli allmänt tillgänglig. Sekretessbelagd uppgift innebär tystnadsplikt för den som har eller har fått befattning om uppgiften.
Tillgänglighet	Att information är åtkomlig och användbar av behörig.

# Övergripande riktlinjer för informationssäkerhet

Dessa övergripande riktlinjer kan detaljeras ytterligare i anvisningar och rutiner.

## Dispenser och undantag

Ansökan om dispens och undantag från denna riktlinje ställs till kommunens informationssäkerhetsstrateg. Beslut om godkännande fattas av kanslichef och IT-chef i samråd med berörda.

Undantag och dispenser är inte permanenta utan ska ha en giltighetstid som bedöms från fall till fall. Efter att giltighetstiden passerat ska en ny begäran om dispens göras.

## Styrning av informationssäkerhet

Detta avsnitt beskriver och reglerar hur arbetet med informationssäkerhet ska bedrivas i Gullspång kommun.

## Roller, ansvar och organisation

### Grundläggande princip

Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret inom kommunen och bolag. Detta innebär att den som är ansvarig för en verksamhet (eller enhet, process, projekt osv.) också är ansvarig för informationssäkerheten inom verksamhetsområdet.

Kommunens informationssäkerhetsstrateg och verksamheternas informationssamordnare och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor fungerar som stöd till medarbetare, verksamheter och kommunens ledning för att kunna ta ansvaret för informationssäkerhet.

### Övergripande roller och ansvar

**Kommunfullmäktige** - fastställer med denna riktlinje både mål och övergripande riktlinjer för informationssäkerhet som ska gälla för kommun och bolag.

**Nämnd** – är ägare av den information som uppstår och hanteras i dess verksamhet. Nämnden är ansvarig för informationssäkerheten inom sitt verksamhetsområde och ska säkerställa att verksamheten följer antagna riktlinjer, anvisningar och rutiner. Nämnden är även personuppgiftsansvarig – se riktlinje för hantering av personuppgifter.

**Kommunstyrelsen** - ska följa upp efterlevnaden av styrande dokument avseende informationssäkerhet. Kommunstyrelsen ansvarar för samordningen av informationssäkerhetsarbetet i kommunen.

**Kommundirektören** - har från kommunstyrelsen i uppdrag att sörja för att informationssäkerhetsarbetet bedrivs så effektivt som möjligt i linje med den av kommunfullmäktige fastställda riktlinjen för informationssäkerhet. Kommundirektören

ansvarar för att övergripande tillämpningsanvisningar utarbetas och hålls aktuella i enlighet med denna riktlinje.

**Kommundirektörens ledningsgrupp (KDLG)** – stödjer kommundirektören i det övergripande ansvaret att leda och utveckla förvaltningens informationssäkerhetsarbete. Kommunledningsgruppen ska följa upp informationssäkerhetsarbetet 1-2 gånger per år.

**IT-chef** – samråd tas med IT-chef när informationssäkerhetsstrategen tar fram gemensamma anvisningar kring informationssäkerhet i operativa frågor som för exempel rör anskaffning, utveckling och förvaltning av IT-system. KD beslutar om de gemensamma anvisningarna.

**Verksamhetsansvarig (alla nivåer)** - ansvarar för informationssäkerheten inom sin verksamhet. Det åligger varje verksamhetsansvarig att se till att medarbetarna efterlever riktlinjer, har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en erforderlig informationssäkerhet i verksamheten kan uppnås. Ansvaret omfattar även att tillgängliga tjänster/processer/system används på de sätt som är avsedda.

**Medarbetare** - har ett ansvar för verksamhetens informationssäkerhet. Varje anställd ska i eget arbete följa riktlinjer och anvisningar för informationssäkerhet samt eventuella verksamhetsspecifika rutiner och regler. Varje anställd har även skyldighet att rapportera brister och incidenter rörande såväl informationssäkerhet som hantering av personuppgifter.

## Dedikerade roller och ansvar

### Systemägare

Systemägaren ansvarar för att informationssäkerheten hanteras enligt gällande styrdokument vid anskaffning, utveckling och förvaltning av system.

Informationssäkerhetsansvar hos övriga roller inom förvaltningsorganisationen beskrivs i Gemensamma anvisningar för informationssäkerhet. Verksamhetschef är på nämnden/styrelsens vägnar ytterst ansvarig för system inom sin verksamhet. Verksamhetschef kan utse någon annan inom sin verksamhet till systemägare.

### Ansvar i projekt

Utsedd projektägare säkerställer att informationssäkerhetsfrågorna beaktas och ansvarar för fastställande av informationssäkerhetsklassning i projektet. Projektledaren tillsammans med styrgrupp ansvarar för informationssäkerheten beaktas och efterlevs under hela projektiden. Under ett projekts gång ska styrgruppen följa upp hanteringen av de säkerhetsrelaterade frågorna.

### IT-avdelning

IT-avdelningen ansvarar för att säkerheten i kommunens IT-miljö som tjänster, processer, system, infrastruktur, verktyg etcetera motsvarar verksamhetens krav, legala krav och riktlinje för informationssäkerhet samt gemensamma anvisningar för informationssäkerhet.

## IT-säkerhetsspecialist

IT-avdelningen ska ha en roll som leder och samordnar området IT-säkerhet, här benämnd IT-säkerhetsspecialist. Rollen är stödjande vid kravställning gentemot externa aktörer. Rollen IT-säkerhetssamordnare kan beskrivas utförligare i Gemensamma anvisningar för informationssäkerhet.

## Informationssäkerhetsstrateg

Det ska finnas en utpekad informationssäkerhetsstrateg i kommunen. Rollen leder och samordnar kommunens informationssäkerhetsarbete. Informationssäkerhetsstrategen ansvarar för att:

- ta fram och uppdatera kommunens styrande dokument inom informationssäkerhet och dataskydd.
- utveckla, besluta och förvalta kommun övergripande metoder, anvisningar och annat stödmaterial inom båda områdena,
- ge stöd till övriga roller inom informationssäkerhet och dataskyddsområdet,
- ta fram övergripande internt utbildningsmaterial och utbilda internt inom båda områdena,
- rådfråga och samråda med dataskyddsombudet för kommunens räkning,
- ansvara för omvärldsbevakning kring informationssäkerhet och dataskydd
- stödja i uppföljning av arbetet med både områdena,
- årligen rapportera status inom informationssäkerhet till kommunfullmäktiga
- sammankalla Informationssäkerhetsnätverket regelbundet.

## Informationssäkerhetssamordnare

Varje verksamhet och bolag utser minst en informationssäkerhetssamordnare med ansvar för att arbeta löpande med verksamhetsnära frågor relaterade till informationssäkerhet och dataskyddsförordningen.

Rollen informationssäkerhetssamordnare kräver god kännedom om verksamheten och dess processer. Det är viktigt att rollen har dedikerat tid för arbetet och rätt mandat för att driva verksamhetens arbete med informationssäkerhet och dataskydd. Rollen ska ha ett dokumenterat och av verksamhetschefen beslutat uppdrag att arbeta med informationssäkerhet och dataskyddsförordningen. Uppdraget innebär bland annat att:

- är ett stöd till verksamhetens ledning kring informationssäkerhet och dataskydd,
- stödjer verksamheten i utförandet av operativa aktiviteter kring exempelvis uppdatering av registerförteckning och genomförande av konsekvensbedömning (dataskydd) eller informationsklassning och riskanalyser (informationssäkerhet),
- stödja verksamheten i för att uppmärksamma och åtgärda incidenter inom informationssäkerhet och dataskydd,
- rådfråga och samråda med dataskyddsombudet för verksamhetens räkning,
- rapporterar status om verksamhetens arbete kring informationssäkerhet och dataskydd till verksamhetens ledning löpande samt på begäran till Informationssäkerhetsstrategen,
- deltar regelbundet i Informationssäkerhetsnätverkets arbete.

## Informationssäkerhetsnätverk

I kommunen ska finnas ett informationssäkerhetsnätverk för samordning av kommunens informationssäkerhet och dataskyddsarbete. Nätverket leds av informationssäkerhetsstrateg och dataskyddsombudet. Representanter för kommunens verksamheter ska ingå i nätverket och inneha rollen informationssäkerhetssamordnare.

Nätverket ansvarar för att ta fram gemensamma mallar, arbetsätt, rutiner och vägledningar gällande informationssäkerhet och dataskydd. Nätverket har också till ansvar att identifiera behov för kompetensutveckling och utbildning inom informationssäkerhet och dataskydd.

### A.1. Dokumentstruktur

Följande dokument är centrala för Gullspång kommuns arbete med informationssäkerhet:

- Riktlinje för informationssäkerhet (detta dokument)
- Gemensamma anvisningar för informationssäkerhet
- Nulägesanalys för informationssäkerhet

Riktlinje för informationssäkerhet samt gemensamma anvisningar för informationssäkerhet riktar sig till alla medarbetare inom kommunen. Nulägesanalys för informationssäkerhet riktar sig främst till de som arbetar med styrning av informationssäkerhet i Gullspång kommun.

**Riktlinje för informationssäkerhet** (detta dokument) uttrycker mål och de övergripande grundläggande riktlinjer för informationssäkerhet exempelvis personalsäkerhet. Beslutas av kommunfullmäktige och revideras var fjärde år eller vid behov.

**Gemensamma anvisningar för informationssäkerhet** beskriver de mera operativa regler för hur förvaltningen och IT ska agera inom olika områden för att leva upp till riktlinje för informationssäkerhet. Beslutas av kommundirektören.

**Nulägesanalysens** syfte är att skapa en gemensam bild av hur effektivt organisationen arbetar med att skydda sin information utifrån behov, krav och förutsättningar. Analysen genomförs vartannat år.

A.1	Dokumentationsstruktur
A.1.1	Gullspångs kommun ska ha en riktlinje för informationssäkerhet som uttrycker ledningens viljeinriktning med informationssäkerhet samt ger övergripande riktlinjer.
A.1.2	Det ska finnas gemensamma anvisningar för informationssäkerhet
A.1.3	Gullspångs kommuns informationssäkerhet ska vartannat år göra en nulägesanalys av informationssäkerheten som ska ligga till grund för hur arbetet med informationssäkerhet ska bedrivas.
A.1.4	Kommunens verksamheter och bolag ska årligen planera in nödvändiga aktiviteter för informationssäkerhet och dataskydd i handlingsplaner.

Modeller, metoder, vägledningar och andra stöddokument tas fram centralt för att stödja arbetet med informationssäkerhet på olika nivåer och att underlätta tillämpningen efterlevnaden av denna riktlinje.

## A.2. Informationsklassning och riskanalys

Informationsklassning är en grundläggande komponent i informationssäkerhetsarbetet. Informationsklassning innebär att verksamheter klassar sina informationstillgångar utifrån extern och interna krav på konfidentialitet, riktighet och tillgänglighet. Genom att klassa information kan verksamheter identifiera känslig och kritisk information och säkerställa att denna får lämpligt skydd, ibland också för att undvika att information får onödigt överskydd.

Klassning av information ska ske utifrån rättsliga krav som lagar och föreskrifter, men även interna krav på informationens värde, känslighet och betydelse för Gullspångs kommuns verksamheter.

I den vägledande standarden SS-ISO/IEC 27002 rekommenderas att man ska ta fram en organisationsgemensam modell för informationsklassning. En sådan modell definierar nivåer av skydds krav kopplat till de tre aspekterna konfidentialitet, riktighet och tillgänglighet så att information kan klassas på ett enhetligt sätt i hela organisationen.

Gullspångs modeller för klassning och riskanalys finns på intranätet under sidan Informationssäkerhet.

A.2	Informationsklassning och riskanalys
A.2.1	Gullspångs kommun ska ha gemensamma modeller för informationsklassning och riskanalys.
A.2.2	Gullspångs kommuns modell för informationsklassning ska tillämpas för kravställning på informationssäkerhet. Information ska klassas i enlighet med modellen
A.2.3	Gullspångs kommuns modell för riskanalys ska tillämpas för kravställning på säkerhetsåtgärder kopplade till informationsklassningens olika nivåer.

## A.3 Ledningssystem för informationssäkerhet (LIS)

Kommunens informationssäkerhetsarbete ska vara systematiskt och att det ska bygga på den vedertagna standardserien ISO/IEC 27000 med strävan att ett ledningssystem för informationssäkerhet integreras i kommunens styrning.

Ett systematiskt arbete med informationssäkerhet med ett LIS syftar i stort till att informationssäkerheten över tid anpassas efter externa och interna förutsättningar, och som därigenom upprätthåller en lämplig skyddsnivå över tid.

I Gullspångs kommun har arbetet med att skapa ett LIS påbörjats i och med dessa riktlinjer där roller, ansvar och informationsklassning är viktiga element. Att planera och fortsätta införa ett LIS kommer dock att fortgå under de kommande åren.

<b>A.3</b>	<b>Ledningssystem för informationssäkerhet</b>
A.3.1	Gullspångs kommun ska införa och underhålla ett ledningssystem för informationssäkerhet (LIS)

## A.4 Personalsäkerhet

Gullspångs kommuns personal hanterar dagligen information, manuellt eller med stöd av IT. Många funktioner kommer i kontakt med och hanterar kritisk och känslig information, därför är det viktigt att personalen får information och utbildning om informationssäkerhet och dataskydd. Det är även viktigt att det finns rutiner i samband med anställning, förändring och avslut av anställning.

### Före och i samband med anställning

Bakgrundskontroll av sökande till tjänster i Gullspångs kommun ska ske genom verifiering av sökandes meritförteckning, till exempel genom kontakt med referenspersoner och bekräftelse av lämnade akademiska och yrkesmässiga kvalifikationer. ID-kontroll ska ske vid anställning.

Registerkontroll ska ske där det finns författningskrav om detta. Till exempel för skydd av barn och unga.

För befattningar som har betydelse för rikets säkerhet och omfattas av Säkerhetsskyddslagen (2018:585), ska det i anställningsförfarandet genomföras en säkerhetsprövning.

Säkerhetsprövningen ska genomföras innan en person genom anställning eller på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet. Säkerhetsprövningen administreras av kommunens säkerhetsorganisation. Hur kontrollen ska gå till återfinns i riktlinje för säkerhetsskydd.

Alla bakgrundskontroller ska ta hänsyn till gällande lagstiftning rörande hantering av personuppgifter.

Nyanställda ska informeras om ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet.

Alla anställda som får tillgång till konfidentiell information ska underteckna ett sekretessavtal som även ska gälla efter avslut av anställning.

### Under anställning

Medarbetare ska få lämplig utbildning för att kunna efterleva kommunens riktlinje för informationssäkerhet. Detta gäller även externa aktörer såsom exempelvis konsulter.

Roller som har särskilda uppgifter inom informationssäkerhet, till exempel inom IT-säkerhet eller systemförvaltning, ska få lämplig fortbildning inom området som är relevant för respektive befattning.

Om anställda bryter mot gällande informationssäkerhetsregler ska dessa ärenden hanteras på samma sätt som vid andra misskötselärenden.

## Avslut eller ändring av anställning

Vid avslut eller ändring av anställning kan ansvar och skyldigheter för informationssäkerhet fortsätta att gälla, exempelvis tystnadsplikt om den anställda haft tillgång till konfidentiell information. Chef ansvarar för att detta kommuniceras till den anställda vid anställning/tillträde av roll samt vid avslut eller ändring av anställning.

Vid avslut eller ändring av anställning ska åtkomsträttigheter till information upphöra och återlämning av IT-resurser ske omgående. Avlämnande chef ansvarar för att detta verkställs.

A.4	Personalsäkerhet
A.4.1	Bakgrundskontroll av sökande ska göras före anställning där sökandes meritförteckning verifieras.
A.4.2	Registerkontroll ska ske där det finns författningskrav om detta. För exempel för skydd av barn och unga.
A.4.3	För befattningar som har betydelse för rikets säkerhet, och som omfattas av Säkerhetsskyddslagen (2018:585) ska det i anställningsförfarandet genomföras en säkerhetsprövning.
A.4.4	Nyanställda ska informeras om ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet.
A.4.5	Anställda som får tillgång till konfidentiell information ska underteckna ett sekretessavtal.
A.4.6	Alla medarbetare ska få lämplig utbildning för att kunna efterleva kommunens riktlinje för informationssäkerhet. Detta gäller även externa aktörer såsom exempelvis konsulter.
A.4.7	Roller som har särskilda uppgifter inom informationssäkerhet ska få lämplig fortbildning inom området som är relevant för deras befattning
A.4.8	Om anställda bryter mot gällande informationssäkerhetsregler ska dessa ärenden hanteras på samma sätt som vid andra misskötselärenden.
A.4.9	Ansvar och skyldigheter för informationssäkerhet som förblir gällande efter avslut eller ändring av anställning ska definieras och kommuniceras vid anställningstillfället och vid ändring eller avslut av anställning av ansvarig chef
A.4.10	Vid avslut eller ändring av anställning ska åtkomsträttigheter till information upphöra och återlämning av IT-resurser ske omgående

## A.5 Leverantörsrelationer

Det ska finnas en vägledning med informationssäkerhetskrav som ska baseras på Gullspångs kommuns modell för informationsklassning. Kravkatalogen ska kunna användas som stöd vid extern upphandling av IT-tjänster såsom system och molntjänster. En kravkatalog baserad på standarden SS-ISO/IEC 27002:2014 ska tas fram.

Det ska finnas en vägledning som beskriver hur en kontroll av en IT-tjänst ska genomföras. Den ska kunna användas som stöd inför användandet av en ny tjänst eller vid kontroll av en befintlig tjänst.

A.5	Leverantörsrelationer
A.5.1	Det ska finnas en vägledning med informationssäkerhetskrav som ska baseras på kommunens modell för informationsklassning. Vägledningen ska kunna användas som stöd vid extern upphandling av IT-tjänster.
A.5.2	Det ska finnas en vägledning för kontroll av IT-tjänst. Syftet med vägledningen ska vara att säkerställa att IT-tjänsten kan skydda verksamheten och dess information under hela dess livscykel

## Efterlevnad och granskning

Efterlevnad av denna och riktlinje för informationssäkerhet, samt de gemensamma anvisningarna ska följas upp.

### Intern kontroll

Nämnd eller bolagsstyrelse ansvarar för att årligen kontrollera och följa upp verksamhetens arbete med informationssäkerhet och dataskydd.

Uppföljningen görs genom följande tre frågeställningar:

- Hur är status på verksamhetens arbete med informationssäkerhet och dataskydd?
- Vilka författningar är aktuella för hantering av information och hur efterlever verksamheten dem?
- Vilka övergripande risker har verksamheten identifierat i deras hantering av information?

Kommunens och bolagens verksamheter ska årligen självskatta sitt arbete kring informationssäkerhet i verktyg som tas fram av informationssäkerhetsstrategen. Självskattningen ska vara grund för den årliga rapporteringen till nämnd/bolagsstyrelse.

Verksamheterna och bolagen ska planera in aktiviteter för informationssäkerhet och dataskydd i årliga handlingsplaner. Sårbarheter och brister som upptäcks ska tas upp för åtgärdande i den årliga handlingsplanen. Akuta sårbarheter och brister ska åtgärdas omedelbart. Rapportering av större sårbarheter och brister ska även ske till informationssäkerhetsstrategen.

### Uppföljning av riktlinje

Efterlevnaden av denna riktlinje för informationssäkerhet ska följas upp regelbundet inom kommunens ledningssystem för informationssäkerhet (LIS). Kommunledningen bestämmer närmare hur uppföljningen ska gå till genom antagande av regler för informationssäkerhet.

Informationssäkerhetsstrategen ska årligen rapportera läge och status gällande informationssäkerhet direkt till högsta ledningen, kommunfullmäktige. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.

A.6	Efterlevnad och granskning
A.6.1	Efterlevnad gällande de styrande dokument för informationssäkerhet ska följas upp genom internkontroll.
A.6.2	Kommunens och bolagens verksamheter ska självskatta sitt arbete med informationssäkerhet årligen.
A.6.3	Informationssäkerhetsstrategen ska årligen rapportera läge och status gällande informationssäkerhet till kommunfullmäktiga