Styrdokument
Dokumenttyp: Regler
Beslutat av: Kommunstyrelsen
Fastställelsedatum: 2020-11-25
Ansvarig: IT-chef
Revideras: Vid behov
Följas upp: Vart 4:e år

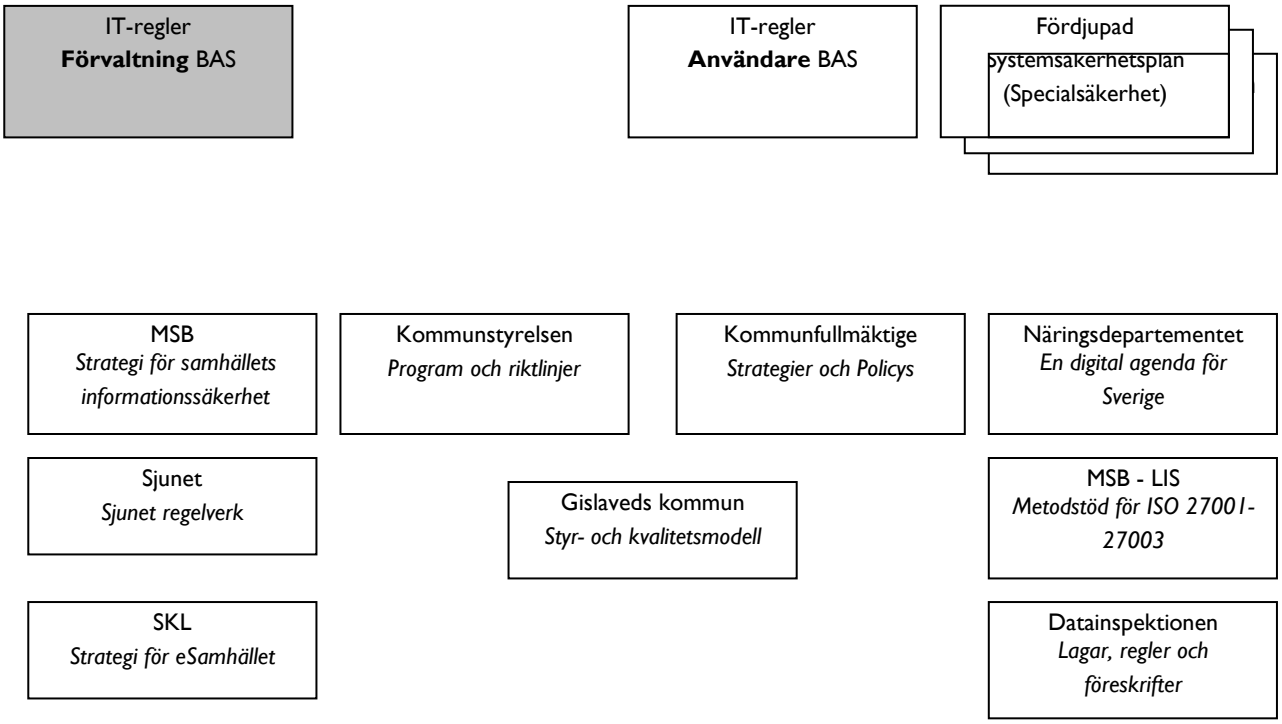
IT-regler Förvaltning BAS

BAS-säkerhet Gislaveds kommun

Dnr: KS.2020.170
2020-09-01

Innehållsförteckning

1 Struktur



2 IT-reglernas roll i kommunkoncernens informations- och IT-säkerhetsarbete

Ordet informationssäkerhet i dokumentet används genomgående för informations- och IT-säkerhet.

Styrande dokument för arbetet med informationssäkerhet inom Gislaveds kommun är:

- Kommunfullmäktiges Policy och strategi för informationssäkerhet
- Förvaltningsmodellen med dess strategiska, taktiska och operativa möten
- Kommunstyrelsens riktlinjer för IT-regler Förvaltning BAS
- Kommunstyrelsens riktlinjer för IT-regler Användare BAS
- Kommunstyrelsens Digital Agenda för Gislaved

Dessa dokument redovisar kommunens planer och regler för arbetet med informationssäkerhet och syftar till att klarlägga:

- den interna organisationen för säkerhetsarbetet
- omfattningen av det ansvar som vilar på Gislaveds kommuns organisation för säkerhetsarbetet
- hur säkerhetsarbetet ska bedrivas
- de krav, strategier och riktlinjer som är aktuella är exempelvis
    - MSB Strategi för samhällets informationssäkerhet
    - Sjunet regelverk
    - SKL Strategi för eSamhället
    - Näringsdepartementet En digital agenda för Sverige
    - Lagar, regler och föreskrifter (GDPR och OSL)
    - MSB LIS – Metodstöd för SS-EN ISO/IEC 27001
    - Kommunfullmäktige - Strategier och Policys
    - Kommunstyrelsen - Program och Riktlinjer

Vid arbetet med att ta fram IT-regler BAS har metodstödet enligt LIS – *Metodstöd för* SS-EN ISO/IEC 27001 använts som grund. Säkerhetsnivån har lagts på en basnivå som täcker in de grundläggande säkerhetskraven för samtliga kommunens system. Vid behov av högre säkerhet för ett system eller en verksamhet upprättas en fördjupad systemsäkerhetsplan.

3 Organisation och ansvar

En fastställd ansvarsfördelning för informationssäkerheten är en förutsättning för att leva upp till de krav, strategier och riktlinjer som gäller för systemen.

Nedan redovisas ansvarsfördelningen för olika rollinnehavare. I många fall kan samma person inneha flera av dessa roller, till exempel tjänsteägare och verksamhetsansvarig.

3.1 IT-regler BAS kontra fördjupad systemsäkerhetsplan

Fördjupad systemsäkerhetsplan ska först tas fram om tjänsteägaren anser att regler och rutiner

behöver förtydligas/förstärkas, alternativt att informationssäkerheten klassas som **Mycket hög nivå** (se pkt 3.2 och Bilaga 1 – Klassning av information). Detta framgår enligt:

- IT-regler Förvaltning BAS
- IT-regler Användare BAS

Analyser ska då initieras och genomföras av tjänsteägaren enligt MSB *LIS – Metodstöd för* SS-EN ISO/IEC 27001. Information om metodstödet finner du på intranätet.

3.1.1 Kommunstyrelsen

Kommunstyrelsen svarar för den övergripande styrningen och samordningen av kommunens arbete med digitalisering, e-utveckling och IT-strategiska frågor samt informationssäkerhet. Kommunstyrelsen beslutar om strategier och program samt om riktlinjer och regler inom området.

3.1.2 Nämnder

Varje enskild nämnd ansvarar för den information och de system som finns inom det egna verksamhetsområdet. De olika nämnderna är också ansvariga för utvecklingen av den egna administrationens system. De är också uppdragsgivare för de projekt som berör den egna förvaltningen. Nämnden fastställer förvaltningarnas behov av IT-utvecklingsinsatser.

Nämnden ska till kommunens dataskyddsombud säkerställa att de personregister som tas fram inte strider mot GDPR.

3.1.3 Förvaltningarna

Förvaltningen har ansvar för de förvaltningsspecifika IT-frågorna.

Förvaltningen har ansvar för att IT-regler för användare och förvaltning tillämpas. Vid behov även upprätta fördjupade systemsäkerhetsplaner. Fördjupad systemsäkerhetsplan tillsammans med IT-regler visar gällande säkerhetsnivå för redovisat förvaltningssystem.

Före nyanskaffning, uppgradering och avveckling av ett system ska ett behov lämnas in i behovsfångsten till den fasta digitaliseringsgruppen. Med hänsyn till konsolideringseffekter i Gislaveds kommun så har förvaltningschefen ansvar för att avstämning sker med Upphandlingsenheten och kommunarkivarie.

3.2 Förvaltningschef

Förvaltningschef är ansvarig för att utse en tjänsteägare för varje förvaltningsspecifik tjänst. Om ingen tjänsteägare har utsetts faller tjänsteägarrollen på förvaltningschefen. Förvaltningschef är även ansvarig att utse en informationssäkerhetssamordnare på förvaltningen. Om ingen informationssäkerhetssamordnare utsetts faller informationssäkerhetssamordnarrollen på förvaltningschefen.

Se Gislaveds kommuns informationssäkerhetspolicy, ” Policy och strategi för informationssäkerhet”, gällande rollfördelning informationssäkerhet.

3.3 Tjänsteägare

Tjänsteägare äger det yttersta ansvaret för en IT-tjänst och dess ingående användarstöd. Tjänsteägaren ska ha god kunskap om den aktuella verksamheten som IT-tjänsten stödjer. Tjänsteägaren utser en tjänsteförvaltare som ges uppdraget att förvalta IT-tjänsten och dess ingående användarstöd. Är det en större tjänst behöver även tjänsteägaren utse superanvändare och/eller tjänsteadministratörer. Om dessa roller inte behövs faller detta ansvar på tjänsteförvaltaren.

Tjänsteägaren ansvarar för:

- IT-tjänst
- överenskommen IT-tjänst, inklusive SLA med IT-avdelningen
- mål och budget för IT-tjänsten
- att IT-tjänsten finansieras och kostnadsfördelas mellan förvaltningar där tjänst delas vid behov
- IT-tjänstens lämplighet samt att verksamhetsbehov realiseras
- att förvaltningsplan för IT-tjänsten upprättas samt godkännande av årliga revideringar
- att utse tjänsteförvaltare
- att strategiska direktiv från den fasta beredningsgruppen för digitalisering hanteras
- att följa upp IT-tjänstens kostnader.

3.4 Tjänsteförvaltare

Tjänsteförvaltare utses av tjänsteägare och är den person i berörd verksamhet som har ansvaret för den dagliga användningen av systemet. Tjänsteförvaltaren ska ha god kunskap om den aktuella verksamheten som IT-tjänsten stödjer samt om det ingående användarstödet.

Tjänsteförvaltaren ansvarar för:

- att specifika funktionskrav tas fram baserat på verksamhetskraven
- att förvalta tjänsten och dess ingående användarstöd
- att beslut om implementation och leveransgodkännande av framtagna lösningar vid realisering av verksamhetskrav
- att ta fram underlag till IT-tjänstens budget
- hanteringen av tjänstens livscykel, ergonomi och miljöaspekt från installation till avveckling
- godkännandet av förslag till förbättringar och anpassningar av IT-tjänsten inom ramen för förvaltningsbudget
- att vid behov samråda med andra tjänsteförvaltare, samt inom sin egen förvaltning med exempelvis verksamhetsansvariga, för säkerställande av att IT-tjänsten är funktionell samt har tillräcklig kvalitet och kapacitet
- att årligen revidera IT-tjänstens förvaltningsplan
- att etablera relationer mellan IT-tjänsteleverantörer där det krävs
- framtagning och underhåll (samordning- inte praktiskt) av utbildningsmaterial, etc. för IT-tjänsten
- att följa upp levererad kvalitet i IT-tjänst och användarstöd
- att service level agreement (SLA) på tjänsten tas fram tillsammans med leveransansvarig
- den övergripande behörighetsstrukturen
- att följa framtida krav på tjänsten utifrån tillgänglighet, kapacitet och säkerhet vilket kräver t.ex. riskanalyser, kapacitetsanalyser, etc.

3.5 Tjänsteadministratör

Tjänsteadministratör är en roll som behövs om man har ett stort system där tjänsteförvaltarollen inte räcker till eller där det finns många superanvändare som behöver koordineras. Tjänsteadministratören har en god kunskap om verksamhetsprocesser och integrerade system. Tjänsteadministratör utses av tjänsteägare. Utses ingen tjänsteadministratör faller nedanstående uppgifter på tjänsteförvaltaren.

Tjänsteadministratör kan ha följande uppgifter:

- Användaradministration inkl. kontroll
- Uppdatering, samordning och beställning
- Felsökning och uppföljning av åtgärder
- Supportkontakt som inte faller på IT
- Utbildning tjänst, inkl. utbildningsmaterial
- Behörighetstilldelning bestämt av tjänsteägare
- Statistikuttag
- Medverka i utvecklingsprojekt
- Samordnare Superanvändare
- Felsökning, rättning

3.6 Superanvändare

Superanvändare är en medarbetare med mycket god insikt i hur tjänsten fungerar på en användarnivå och hur den hjälper verksamheten.

Superanvändare kan ha följande uppgifter:

- Ge användarstöd och support i tjänsten
- Tjänsteintroduktion av användare
- Utbildning av användare
- Inloggningssupport och viss användaradministration
- Medverka i arbetsgrupper och testa funktioner

3.7 IT-chef

IT-chefen är tjänsteägare för Gislaveds kommuns IT-infrastruktur, generella system och generella säkerhetssystem och har det övergripande ansvaret för att de olika datasystemens tekniska delar fungerar.

IT-chefen utser en leveransansvarig per förvaltning och en kompetensgrupp per tjänst. Om dessa roller inte utses faller dessa roller på IT-chefen.

IT-chefen har ansvars för:

- att besluta om behörighet till den gemensamma infrastrukturen
- att besluta om avregistrering av användare från den gemensamma infrastrukturen
- att säkerhetskopierat material förvaras på ett betryggande sätt och kontrollera att återläsningsrutiner fungerar
- att tillhandahålla teknisk support för användare (“IT-support“)
- att nätverk har tillräcklig kapacitet

- att ansvara för att IT-säkerheten i den generella infrastrukturen ligger på rätt nivå
- att en översikt av säkerhetsarkitekturer för interna nätverket och kommunikationsanslutningar upprättas
- administrationen av brandväggen samt besluta om vad som ska loggas i den, vem som ansvarar för uppföljningen av loggarna, hur ofta uppföljning ska ske och hur länge loggarna ska sparas.

3.8 Leveransansvarig

Rollen som leveransansvarig på IT-avdelningen innebär ett ansvar mot en eller flera förvaltningar för att följa upp deras IT-leveranser.

Leveransansvarig kan ha följande uppgifter:

- Ansvar för att följa upp och rapportera tillgänglighet gentemot SLA
- Lyfta förändringsbehov utifrån ett IT perspektiv för verksamhetssystem till tjänsteförvaltare
- Kontaktperson på IT för tjänsteförvaltare och tjänsteägare
- SLA på tjänsten tas fram tillsammans med tjänsteförvaltare.

3.9 Användare

Varje användare ansvarar för att gällande regler för IT-säkerhet följs, se *IT-regler Användare (BAS)*. I detta ansvar ingår även att noga ta del av och följa de säkerhetsinstruktioner som finns för de system den enskilde användaren nyttjar. I ansvaret ingår även att till överordnad chef eller till IT - organisationen rapportera olika former av incidenter, t.ex. intrång eller misstänkt virusangrepp.

3.10 Lagar och andra regelverk

Ramarna för Gislaveds kommuns IT-säkerhetsarbete sätts utifrån lagar och andra regelverk. Dessa anger bland annat villkoren för de övergripande säkerhetskrav som ställs på verksamheten och därmed även på hanteringen av information i tjänsterna.

Detta omfattar bland annat:

- skyddet av den personliga integriteten
- att sekretessbelagd information ska skyddas mot otillbörlig åtkomst, med iakttagande av offentlighetsprincipen
- olika intressenters krav på korrekt information och allmänhetens lagliga rätt till insyn i offentliga handlingar
- speciallagstiftning

3.11 IT-säkerhetsarbetet inom Gislaveds kommun

IT-säkerhetsarbetet inom Gislaveds kommun följer den process i säkerhetsarbetet som baseras på *Myndigheten för samhällsskydd och beredskap (MSB)* rekommenderade metodstöd samt de generella krav, strategier och riktlinjer som redovisas i detta dokument.

Metodstödet är uppbyggt så att det indirekt anger en logisk arbetsprocess för informationssäkerhetsarbetet.

Detta innebär att

- Utefter de generella krav, strategier och riktlinjer, som redovisas i detta dokument, tar IT-avdelningen fram IT-regler
- Tjänsteägaren ska fastställa om *IT-regler* för användare och förvaltning är tillräckligt för aktuellt tjänst
- Vid behov av förhöjd säkerhet enligt KLASSA eller systemsäkerhetsplanen fastställer tjänsteägaren vilka säkerhetsregler som ska gälla för aktuell tjänst enligt regler och rutiner i MSB metodstöd. (Då skapas en fördjupad systemsäkerhetsplan)
- För varje enskilt system ska en avbrottsplan upprättas
- Beredskapsplanen för Gislaveds kommun ska innehålla en beskrivning av lägsta behov av IT-stöd under höjd beredskap
- Nödvändiga säkerhetsåtgärder vidtas för att tillgodose kraven i systemsäkerhetsplanen
- För att kontrollera att vidtagna säkerhetsåtgärder i tjänsten uppfyller ställda krav genomförs en granskning av befintliga säkerhetsåtgärder. Denna granskning ligger till grund för beslut om driftgodkännande av tjänsten .

4 Regler och rutiner

4.1 Klassificering av information

Alla system inom Gislaveds kommun klassas utifrån den information som hanteras i tjänsten. Klassning görs från aspekterna konfidentialitet, riktighet och tillgänglighet.

Med detta menas:

- Konfidentialitet – Att informationen kan åtkomst begränsas
- Riktighet – Att informationen ska vara tillförlitlig, korrekt och fullständig
- Tillgänglighet – Att informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet.

Tas information ut ur tjänsten och lagras på andra medier, eller används i ett annat sammanhang, måste den klassas där den används och hanteras därefter. Även information i arbetsmaterial måste klassas. Gislaveds kommun klassningsmodell framgår av bifogad bilaga 1. Observera att föreliggande IT-regler avser och hanterar Basnivån och Hög nivå vad avser informationsklassning som framgår av bifogad bilaga 1. Är informationsklassningen m*ycket hög nivå* så krävs särskild analys och eventuellt framtagning av särskild Fördjupad systemsäkerhetsplan för det aktuella systemet. Förvaltningens modell för klassning av information ska vara avstämd enligt MSB metodstöd.

4.2 Under anställningen

Information och utbildning av anställda ska omfatta:

- Informationssäkerhetens betydelse för verksamheten
- IT-regler Användare
- Information om IT-säkerhetsutbildning (http://disa.msb.se)

Nya användare ska ges grundläggande IT-säkerhetsutbildning före eller i samband med tilldelning av behörighet i nätverket.

Tjänsteägare ansvarar för att:

- Användarhandledning för aktuell tjänst finns.
- Medarbetare har tillräckliga kunskaper om säkerhetsreglerna för de tjänster vilka används för de egna arbetsuppgifterna.

4.3 Säkrade utrymmen

Känslig information från tjänsterna ska lagras på resurser i datorhallar som ska vara försedda med kontrollsystem för in- och utpassering. Utrymmen med konsolutrustning ska vara låsta när de är obemannade. Utrymmen med kopplingspunkter ska vara låsta. Övervakning av servicepersonal, städpersonal m.fl. ska ske och beslut ska tas av IT-chefen om och när tillträde till säkrade utrymmen tillåts.

4.4 Säkrad information

Känslig information som inte hanteras i tjänsterna ska förvaras i brandklassade säkerhetsskåp.

4.5 Lagring av information i molntjänster

Konsekvensbedömningsmall, vilket finns på intranätet, måste först genomarbetas innan lagring kan ske i molntjänst. Konsekvensbedömningen genomföras tillsammans med förvaltnings informationssäkerhetombud. Respektive nämnd fattar beslut om utförd konsekvensbedömning. Därefter görs en riskanalys gällande informationssäkerhet tillsammans med SKA.

4.6 Kontroll av utomstående tjänsteleverantör

Beställare av utomstående leverantörers tjänster ska följa upp och granska att säkerhetsöverenskommelser följs.

Extern part t.ex. leverantör/konsulter ska ha undertecknat *Tystnadsplikts- och säkerhetsavtal* (bilaga 2) innan åtkomst till Gislaveds kommuns datanät och system beviljas.

4.7 Hantering av datamedia

Datamedia med sekretessbelagd information som ska avvecklas överlämnas till IT-avdelningen som hanterar avvecklingen.

4.8 Utbyte av information

Om media som innehåller känslig information måste transporteras fysiskt ska Säkerhet, Kunskap och Analys (SKA) kontaktas för beslut om tillvägagångssätt.

4.9 Övervakning

För tjänsternas loggar ska tjänsteägaren besluta:

- Hur ofta de ska analyseras
- Vem som ansvarar för att analysera informationen
- Hur länge de ska sparas
- Hur de ska förvaras

Detaljerad information samt anvisningar för användning och övervakning av loggfiler framgår av separat dokument.

4.10 Styrning av användares åtkomst

För att säkerställa att endast behöriga användare förekommer i systemen krävs en beställning och borttagande av systemåtkomsten. Tjänsteägaren ansvarar för att informera IT-avdelningen om vem och till vilken tjänst åtkomst krävs.

4.11 Styrning av åtkomst till nätverk

IT-chefen ska i anvisningar reglera:

- autentisering vid externa anslutningar
- anslutning av utrustning till interna och externa nätverk
- anslutning av externa nätverk till myndighetens eget nät med ingående säkerhetsfunktioner, autentisering etc.
- anslutning av trådlösa nät

- säkerhet vid internetanslutning.

4.12 Styrning av åtkomst till operativsystem

IT-chefen beslutar i vilken utsträckning användning av administrationsverktyg eller systemhjälpmedel som kan förbigå system- och tillämpningsspärrar ska användas.

4.13 Mobil datoranvändning och behörighet för distansarbete

Verksamhetsansvarig chef beslutar om en tjänsts information ska få hanteras på distans med stationär eller mobil utrustning. Behörighet för distansarbete ska vara överenskommet med chef som i sin tur meddelar IT om godkännande.

4.14 Införande/Uppgradering/Avveckling av tjänster/system

Digitaliseringsprocessen är vår styrmodell som stimulerar till verksamhetsutveckling genom digitalisering i Gislaveds kommuns verksamheter och består av behovsfångs och förvaltningsmodell.

Behovsfångsten fångar upp verksamheteters behov och beredningsgruppen för digitalisering tar beslut om prioritering av ärenden.

Förvaltningsmodellens huvudsakliga syfte är att säkra tydliga och strukturerade arbetsformer inom Gislaveds kommun och innehåller grundläggande principer om hur IT införskaffas, förvaltas och utvecklas.

Vid större förändringar av tjänster t.ex. införande, uppgradering eller avveckling behöver detta gå via behovsfångsten. Detta behov bereds och tas sedan upp i den fasta beredningsgruppen för digitalisering för ett riktningsbeslut. Efter riktningsbeslutet går det vidare till en förstudie i en projektgrupp där input tas från både IT och verksamheten. Beslutsunderlaget går sedan tillbaka till den fasta beredningsgruppen för digitalisering för beslut. I beslutsunderlaget ska det framgå vem som äger tjänsten och hur rollen ska besättas samt vilka kostnader som uppstår. I de fallen det godkänns skapas en ny projektgrupp som får leda ett införandeprojekt.

4.15 Vid behov av förändringar i tjänsterna

Förslag om önskemål på mindre förändringar i tjänsten kan lämnas till leveransansvarig. Större förändringar behöver hanteras genom en Request For Change process (RFC).

Vid RFC-processen beslutas om:

- Vad ska göras
- Vem ska göra det
- När ska det göras, samt en plan för hur vi kan backa förändringen ifall det inte blev som det var tänkt.

4.16 Hantering av incidenter i kommunens driftmiljön

Vid misstanke om intrång eller andra incidenter ska användare agera enligt *IT-regler Användare.* Alla incidenter ska dokumenteras och följas upp i Gislaveds kommun ärendehanteringssystem för support och felanmälan.

IT-avdelningen dokumenterar och åtgärdar problemet. Vid misstanke om säkerhetsincident meddelas IT-chef som eskalerar ärendet till SKA.

4.17 Personuppgiftsincidenter

En personuppgiftsincident uppstår när de personuppgifter vi behandlar har medvetet, omedvetet eller olagligt förstörts. När någon som inte ska ha behörighet till personuppgifterna får tillgång till dessa. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att en individs rättigheter inskränks/minskas.

Personuppgiftsincidenten ska rapporteras så fort du **vet**, **misstänker** eller **ser** en risk för att det kan inträffa en incident. Inträffad incidenten ska inom 72 timmar rapporteras till Datainspektionen, det gäller även om incidenten hunnit bli åtgärdad. Varje myndighet ska ta fram rutiner för hur anmälan för personuppgiftsincidenter ska gå till.

4.18 Efterlevnad av rättsliga krav

Anvisningar för skydd av register och handlingar ska följas.

Bilaga 1 – Klassning av information

A. Information som hanteras i IT-baserade system

För information som lagras i system måste inte bara sekretessaspekten beaktas, utan även kraven på riktigheten i informationen och tillgängligheten till den.

Säkerhetsaspekt **Kravnivå**	**Konfidentialitet**	**Riktighet**	**Tillgänglighet**
Mycket hög nivå	Information som kan medföra mycket allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra **mycket allvarliga** negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som ska vara åtkomlig inom högst 2 timmar för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet

			eller för enskild person
Hög nivå	Information som kan medföra **allvarliga** negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra **allvarliga** negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som inte behöver vara åtkomlig inom 2 timmar, men **inom högst 8 timmar** för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet eller för enskild person
Basnivå	Information som kan medföra **mindre allvarliga** negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra **mindre allvarliga** negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som inte behöver vara åtkomlig inom 8 timmar för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet eller för enskild person

Anm: Följande typ av information hanteras utanför klassningsmodellen:

- Information som avser rikets säkerhet. Sådan information ska hanteras enligt särskilda bestämmelser.
- Information som har extrema krav på sig att vara tillgänglig och där utgångspunkten är att den alltid ska vara det.
- Information som inte bedöms ha krav på sig vare sig avseende konfidentialitet, riktighet eller tillgänglighet.

De åtgärder som ska vidtas för att uppfylla säkerhetskraven på respektive system framgår av tjänsteägarens analys.

B. Information på datamedia

Med datamedia menas tex USB-minnen etc. Dessa medier ska inte ses som slutliga förvaringsformer, såvida de inte avser backup-tagning. Information på datamedia är alltid kopierad och måste hanteras med samma säkerhet som det system som den kommer ifrån. Eftersom informationen är kopierad behöver endast kraven på konfidentialitet beaktas. De krav på sekretess som

ställs för ett specifikt system framgår av användarhandledningen för systemet.

För information på datamedia gäller följande krav:

Krav på sekretess	**Åtgärder**
Mycket hög nivå	Förvaring *- Endast krypterade USB-minnen eller motsvarande får användas och ska förvaras inlåsta* Kopiering *- Får kopieras endast med godkännande från tjänsteägaren för systemet som informationen kommer ifrån* Återanvändning *- Får inte återanvändas* Destruktion *- Lämnas till IT för destruktion. Destruktion sker hos IT*
Hög nivå	Förvaring *Endast USB-minnen eller liknande får användas och ej förvaras synligt* Kopiering *- Får kopieras i samråd med systemets förvaltare/administratör* Återanvändning *- Tillåten* Destruktion *- Lämnas till IT för destruktion*
Basnivå	Förvaring *- Inga krav* Kopiering *- Tillåten* Återanvändning *- Tillåten* Destruktion *- Krävs ej*

C. Information på andra media

Med andra media menas papper, inspelad film, inbrända DVD-skivor, OH-bilder etc. Information på dessa media är alltid kopierad och måste hanteras med samma säkerhet som det system som den kommer ifrån. Eftersom informationen är kopierad behöver endast kraven på konfidentialitet beaktas. De krav på sekretess som ställs för ett specifikt system framgår av användarhandledningen för systemet.

För information på ovanstående media gäller följande krav:

Krav på sekretess	**Åtgärder**
Mycket hög nivå	Förvaring *- Förvaras inlåsta* Kopiering *- Får kopieras endast med godkännande från tjänsteägaren för systemet som informationen kommer ifrån* Återanvändning *- Får inte återanvändas* Destruktion *- Papper och OH-film destrueras i papperstugg* *- Övrigt lämnas till IT för destruktion*
Hög nivå	Förvaring *- Ej förvaras synligt* Kopiering *- Får kopieras i samråd med systemets förvaltare/administratör* Återanvändning *- Tillåten* Destruktion *- Lämnas till IT för destruktion*
Basnivå	Förvaring *- Inget speciellt förvaringskrav* Kopiering *- Tillåten* Återanvändning

	- Tillåten Destruktion *- Krävs ej*

D. Information som lagras i externa molntjänster

För den information som hanteras inom en förvaltning är alltid förvaltningen själv ansvarig. Idag finns möjlighet att lagra information i molnbaserade lagringstjänster. Exempel på sådan är Dropbox. Eftersom det idag är svårt att garantera säkerhet och sekretess i dessa tjänster utifrån ett informationssäkerhetsperspektiv är det generellt inte tillåtet att använda denna typ av tjänster inom Gislaveds kommun.

I de fall då förvaltningen genomfört en informationssäkerhetsanalys och tagit fram och tillämpat erforderliga riktlinjer för hur molntjänsten får användas inom berörd förvaltning, görs ett undantag från huvudregeln och den generella hållningen att inte använda molnbaserade tjänster. En risk och konsekvensanalys ska alltid göras innan en molntjänst tas i bruk.

Bilaga 2 – Tystnadsplikts- och säkerhetsavtal

FÖRBINDELSE OM TYSTNADSPLIKT ENLIGT OFFENTLIGHETS-OCH EKRETESSLAGEN SAMT TEKNISKT SÄKERHETSAVTAL FÖR EXTERNA KONSULTER/UPPDRAGSTGARE/SAKKUNNIGA

Efternamn	Personnummer (ååmmdd-nnnn)
Förnamn	Företag
Telefonnummer (direkt)	
E-postadress	
Uppdragsgivare (Förvaltning, Enhet, Namn)	
Tjänstebenämning/uppdrag (ex Teknisk konsult IT)	

(OBS! Texta tydligt i ALLA fält)

☐ Önskar inloggningskonto i till Gislaveds kommuns IT-miljö (kryssa)

Jag har denna dag informerats av Gislaveds kommun att tystnadsplikt, enligt offentlighets- och sekretesslagen, samt tekniskt säkerhetsavtal gäller vid uppdrag/arbeten/möten och motsvarande inom Gislaveds kommun.

Tystnadsplikt innebär förbud mot att lämna ut en sekretessbelagd uppgift.

Tekniskt säkerhetsavtal innebär förbud att lämna ut konfidentiell information om Gislaveds kommuns IT-säkerhetsuppbyggnad eller annan information som kan skada Gislaveds kommun.

Undertecknad är medveten om att brott mot tystnadsplikt kan medföra straff, även om brott endast sker av oaktsamhet.

Denna förbindelse gäller även efter uppdragets/arbetets/mötets upphörande.

Ort och datum .....

....

Egenhändig namnteckning Namnförtydligande (texta)

Avtalet skrivs ut och undertecknas av den person som avtalet avser.

Undertecknat avtal skickas eller scannas/mailas till IT-enheten på Gislaveds kommun.

Adress: Gislaveds kommun, IT-enheten, 332 80 Gislaved. Epost: it@gislaved.se