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

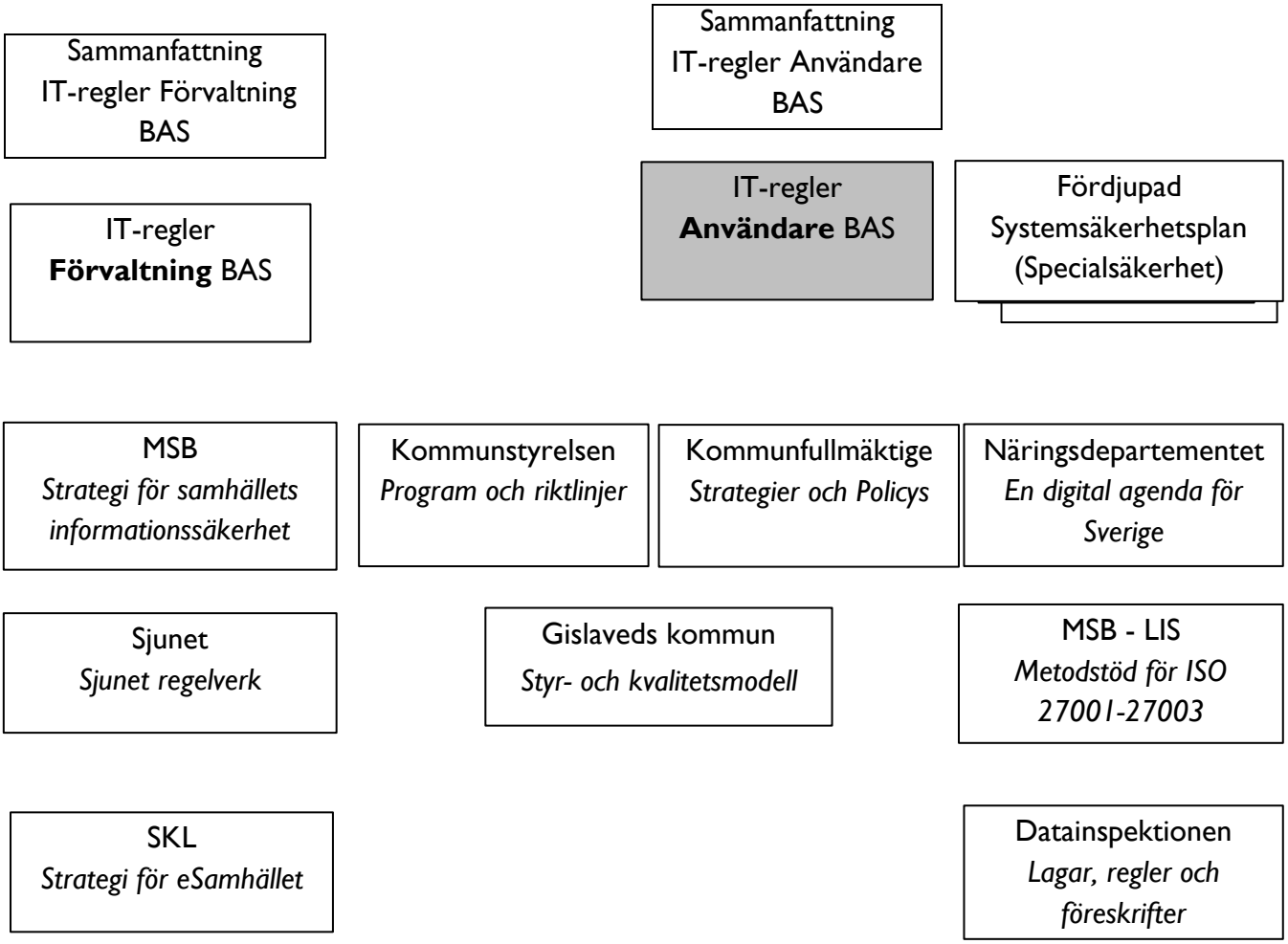
IT-regler Användare BAS

BAS-säkerhet Gislaveds kommun

Dnr: KS.2020.171
2020-09-01

Innehållsförteckning

1 Struktur



2 Att komma igång

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

Informationssäkerhet innebär att skydda information utifrån krav på dess konfidentialitet, riktighet, tillgänglighet och spårbarhet. Det gäller att Gislaveds kommun och du som enskild användare hjälps åt att skydda informationen - som vi använder i både tal och skrift - genom sunt förnuft och med stöd från de IT-regler som finns framtagna. I och med ökad användning av bl.a. eTjänster i samhället är informationssäkerheten en förutsättning för att dessa tjänster ska fungera och vara säkra, tillförlitliga och tillgängliga.

IT-säkerhet innebär att med hjälp av lämpliga tekniska och organisatoriska säkerhetsåtgärder skydda information och tjänster i IT-systemen. Till tekniska åtgärder räknas saker som brandväggar, krypteringsfunktioner och antivirus, medan organisatoriska åtgärder handlar om säkerhetsarbetets organisation och rutiner, regler och planer.

3 Ditt ansvar som användare

Du som användare, av Gislaveds kommuns IT-system, ansvarar för att gällande IT-regler för informationssäkerheten följs. I detta ansvar ingår att noga ta del av och följa de säkerhetsinstruktioner som finns för de informationssystem du använder. I ansvaret ingår även att till överordnad chef rapportera olika former av incidenter, t.ex. intrång eller misstänkt virusangrepp.

3.1 Utbildning – informationssäkerhet

I Gislaveds kommuns ska all personal som arbetar i kommunens informationssystem genomgå IT-säkerhetsutbildning enligt http://disa.msb.se eller motsvarande. Närmaste chef ansvarar för att medarbetaren genomför denna utbildning. Instruktioner och länkar för denna utbildning finns på Intranätet.

4 Åtkomst till information

4.1 Behörighet

Våra informationssystem inom kommunen är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information. De behörigheter du blir tilldelad beror på dina arbetsuppgifter och bestäms av din chef.

4.2 Inloggning

Vid första inloggningen erhålls ett temporärt lösenord från IT-enheten för åtkomst till interna datanätverket. Lösenordet ska bytas till ett personligt lösenord efter första inloggningen. Samma förfarande gäller för de enskilda informationssystem som kräver lösenord för åtkomst.

Alla lösenord och rättigheter till de olika informationssystemen inom respektive förvaltning hanteras av förvaltningens systemansvarige.

4.3 Val av lösenord

För val lösenord gäller att det ska:

- vara minst åtta (8) tecken långt
- bestå av minst en (1) stor och en (1) liten bokstav samt minst en (1) siffra. Specialtecken bör användas.
- inte använda ääöÅÄÖ
- inte återanvändas

4.4 Byte av lösenord

Byte av lösenord är aktuellt:

- när du via dialogruta på skärmen eller på annat sätt blir meddelad att det är dags att byta lösenord i datanätverket efter stipulerad tid.
- för enskilda informationssystem efter ett visst tidsintervall som bestäms av respektive systemägare.
- omedelbart om misstanke finns att någon annan känner till det.

5 Din arbetsplats

5.1 Utrustning

Den utrustning som förfogas över, t.ex. dator, surfplatta eller mobiltelefon med tillhörande utrustning gäller:

- fysiska ingrepp får endast utföras efter godkännande från IT-avdelningen.
- fel ska omgående anmälas till IT-supporten via webbgränssnitt länkat från Insidan på eller per telefon 0371-816 80.
- all installation och konfiguration av dator utförs av IT-avdelning eller av annan medarbetare utsedd av IT-avdelningen.

5.2 Programvaror på dator

- programvaror ska godkännas och installeras av IT-avdelningen eller av IT-avdelning anvisad/godkänd person

- egna program får inte installeras i kommunens datorer
- vid behov av ytterligare programvaror eller hårdvara anmäls detta till närmaste chef.

5.3 Appar på mobiltelefoner och surfplattor

Enbart appar nedladdade från Googles eller Apples appbibliotek, eller från appen HUB får laddas ned och installeras på surfplattor och telefoner. Appar som ska användas i verksamheten måste godkännas av respektive förvaltningschef eller annan utsedd person.

5.4 Återlämning av utrustning

Kontakta IT-enheten för återlämning. All IT-utrustning är registrerad i ett inventeringssystem. All återlämning ska ske via IT-avdelningen för avregistrering av licenser, koder m.m. Detta gäller all typ av IT-utrustning tex datorer, surfplattor och telefoner.

5.5 Om du lämnar arbetsplatsen

Vid de tillfällen då du som användare inte har uppsikt över IT-arbetsplatsen ska den låsas med lösenord eller lösenkod. För en PC gör man detta med kortkommandot: Windowstangent + L. I annat fall ska man logga ur datorn.

5.6 Distansarbete

Länkar för distansarbete (inloggning hemifrån som exempel) finns under www.gislaved.se/personal. På denna sida väljer du om du vill ansluta till din arbetsplats på jobbet via PC eller surfplatta alternativt enbart till din mailbox.

Se nedan vad som gäller kring hantering av information.

5.7 IT-support

IT-support tillhandahålls alla användare av våra IT-system. IT-supporten ska primärt kontaktas via webbanmälan. Efter att ärende är skapat kan IT-avdelningen kontaktas per telefon. IT-supportens öppettider är vardagar mellan kl. 8.00-12.00.

6 Hantering av information

Den information som lagras på centrala disksystem (G:, H: X: och Y:) säkerhetskopieras automatiskt minst 1 gång/dygn. Lokala hårddiskar/lagringsmedia på datorer och surfplattor säkerhetskopieras inte med automatik.

En bärbar arbetsdator ska ses som ett arbetsredskap som din arbetsgivare tillhandahåller. Den ska inte användas till annat än vad den är avsedd för, eller vad policyn på din arbetsplats tillåter. Så snart du börjar

använda datorn kommer den att innehålla uppgifter om ditt arbete och din arbetsplats. Mängden information fylls sedan kontinuerligt på, ju längre du använder den.

Tänk på att inte lämna din dator utan uppsikt, låna inte ut den och använd den inte till privata ändamål. När du arbetar med din dator i publika miljöer, utgå ifrån att obehöriga inte ska kunna se vad du arbetar med, oavsett materialets känslighet eller sekretessvärde.

Flyttbara lagringsmedia, som USB-minnen, erbjuder även de allt större minneskapaciteter och det är därför mycket viktigt att ha kontroll på vilken information som sparas ner på dem. Använder du USB-minnen på arbetet bör du kontrollera med IT-enheten vilka regler som gäller för att skydda minnena när de lämnar arbetsplatsen.

7 Internetsidor

Vid surfning på internetsidor kan säkerheten i Gislaveds kommuns lokala nätverk påverkas i mycket hög grad beroende på beteende. Gislaveds kommun förutsätter att den som surfar på internet endast besöker välrenommerade webbplatser.

8 E-post

Tänk även på att regelbundet radera i mapparna ”Inkorgen”, ”Skickat”, och ”Borttaget” för att känslig information inte ska ligga kvar. E-postsystemet ska inte användas som ett arkivsystem utan är endast ett transportsystem. All information som ska bevaras, såsom meddelanden, bifogade filer mm, sparar du på samma sätt som du lagrar annan information. Informationen sparas som filer på dina lagringsplatser eller i aktuellt förvaltningssystem. E-mail som du raderar sparas max 30 dagar i backupen och kan efter det inte återställas.

Var selektiv med att skicka eller vidarebefordra meddelanden som innehåller stora filer (över 10MB) för att undvika onödig belastning av epostsystemet.

Om du under en längre period inte har möjlighet att kontrollera din e-post ska du sätta frånvarobesked med eventuell uppgift om vem som ska hantera dina inkommande ärenden.

Enligt offentlighet- och sekretesslagstiftningen ska all post inklusive e-post öppnas varje arbetsdag för att kunna avgöra om det är en allmän handling. Det innebär att om du är borta och du själv inte öppnar posten ska någon annan göra det.

Observera! E-postsystemet får inte användas för att skicka sekretessbelagd information

Då du använder kommunens epostsystem representerar du alltid Gislaveds kommun. Därför rekommenderas ett privat epost-konto utanför kommunens system som du använder då du kommunicerar privat. Det finns ett flertal gratis-tjänster som lämpar sig utmärkt för detta.

9 Incidenter

9.1 Allmänt

Om du misstänker att någon använt din användaridentitet eller att du varit utsatt för någon annan typ av incident ska du:

- notera när du senast var inne i IT-systemet
- notera när du upptäckte incidenten
- omedelbart anmäla förhållandet till IT-enheten eller din chef.
- dokumentera alla iakttagelser i samband med upptäckten och försöka fastställa om kvaliteten på din information har påverkats.

Om du upptäcker fel och brister i de system du använder ska du rapportera dessa till IT-enheten, din närmaste chef eller systemansvarig.

IT-enheten begär **ALDRIG** via mail att du ska berätta vilket lösenord du har i de olika systemen.

9.2 Virus och skadlig kod

Gislaveds kommun har programvaror för viruskontroll både i klienterna och i nätverket, men kan ändå drabbas av effekter av s.k. skadlig kod. Om du misstänker att din dator innehåller virus ska du:

- dra ut nätverkskabeln, slå av wifi (görs via ett tryck på knappen F11 på din dator) och låt datorn vara på
- omedelbart anmäla förhållandet till endera IT-avdelningen eller till närmaste chef. **OBS!** Anmälan ska ske per telefon eller besök, **inte per e-post**.

Om du får mail med virusvarning gör inget annat än att kontakta IT-enheten.

10 Mobiltelefoner, surfplattor och molntjänster

Överordnad chef beslutar om vem som ska ha tillgång till mobiltelefon och/eller surfplatta i tjänsten. För kommunens förvaltningar finns framtaget ett antal modeller av mobiltelefoner och surfplattor som man har att välja på. Beställning görs via kommunens Intranät.

Molntjänster, såsom Dropbox, får inte användas utan medgivande av förvaltningen. Varje molntjänst som är intressant att använda måste först analyseras ur ett informationssäkerhetsperspektiv. Detta ansvar åligger förvaltningschef eller annan person förvaltningschef har utsett.

Mobiltelefoner och surfplattor ska förses med skärmlås. Skärmlåset aktiveras automatiskt efter inaktivitet och ska innehålla minst fyra tecken.

11 Sociala medier, surfning etc.

Gislaveds kommun ser positivt på att du som medarbetare i kommunen deltar i sociala medier. Ditt deltagande kan göra skillnad och är en möjlighet för dig att utveckla vår gemensamma verksamhet och dessutom stärka Gislaveds kommuns varumärke. För att använda sociala medier i tjänsten måste du få ett tydligt uppdrag av din närmaste chef och uppdraget ska anmälas till Gislaveds kommuns kommunikationsenhet på kommunstyrelseförvaltningen.

12 Avslutning av anställning

När du slutar din anställning ansvarar du för att:

- rådgöra med din chef om vilket av ditt arbetsmaterial som ska sparas. Notera att allt arbetsmaterial du framställt anses vara kommunens egendom och får inte tas med utan chefs godkännande. Vad som ska sparas/gallras framgår i din förvaltnings informationshanteringsplan.
- Kontot inaktiveras och raderas inom 3 månader.