

# Riktlinje

## Informationssäkerhetsinstruktion - Användare

<b>Beslutsdatum</b>	2025-05-22	<b>Dokumenttyp</b>	Riktlinje
<b>Beslutad av</b>	Kommundirektör	<b>Dokumentägare</b>	Chef Demokrati och Säkerhet
<b>Diarienummer</b>	KS/2025:270	<b>Giltighetstid</b>	Tillsvidare

## Innehållsförteckning

<b>1</b>	<b>Introduktion</b> .....	<b>4</b>
<b>2</b>	<b>Terminologi</b> .....	<b>5</b>
<b>3</b>	<b>Säkert beteende</b> .....	<b>11</b>
3.1	Allmänt.....	11
3.2	Säkerhetsmedvetenhet .....	11
3.2.1	Besöksrutiner i Kommunhuset Tyresö .....	11
3.2.2	Muntlig information.....	12
3.2.3	Fysisk information .....	12
3.2.4	Digitala möten .....	13
3.3	Förbindelse vid nyanställning .....	13
<b>4</b>	<b>Lösenord</b> .....	<b>13</b>
4.1	MFA (Multifaktorautentisering) .....	14
4.2	Byte av lösenord .....	15
4.3	Spärrad behörighet eller glömt lösenord till användarkonto.....	15
4.4	Ändrade behörigheter .....	15
4.5	Användarsupport.....	15
<b>5</b>	<b>IT-utrustning och Säkerhetskopiering</b> .....	<b>15</b>
5.1	Standardutrustning .....	15
5.2	Fast utrustning .....	16
5.3	Mobila enheter .....	17
5.3.1	Bärbar dator .....	17
5.3.2	Mobiltelefon och surfplatta .....	17
5.4	Flyttbar lagringsmedia.....	18
5.4.1	USB och Extern hårddisk .....	18
5.4.2	CD/DVD.....	18
<b>6</b>	<b>Internet</b> .....	<b>18</b>
6.1	Molntjänster .....	18
6.2	Publika trådlösa nätverk .....	19
6.3	E-post.....	19

6.3.1	Allmänt .....	19
6.3.2	Säkra meddelanden .....	20
6.3.3	Bifogade filer och länkar .....	20
6.4	Sociala medier .....	20
<b>7</b>	<b>Granska avsändaren .....</b>	<b>21</b>
7.1	Social manipulation .....	21
7.1.1	E-post.....	21
7.1.2	Telefonsamtal.....	21
7.1.3	Sms .....	21
7.1.4	Videosamtal.....	22
<b>8</b>	<b>Skadlig kod .....</b>	<b>22</b>
<b>9</b>	<b>Utanför arbetsplatsen .....</b>	<b>23</b>
9.1	Distansarbete.....	23
9.2	Att tänka på vid resor och vid publika platser.....	23
9.3	Övrigt om IT utrustning.....	24
9.3.1	Stöld av IT-utrustning .....	24
9.3.2	Service på IT-utrustning.....	24
9.3.3	Kassering av IT-utrustning .....	24
<b>10</b>	<b>Incidenter, rapportering och hantering .....</b>	<b>24</b>
<b>11</b>	<b>Informationsklassning .....</b>	<b>25</b>
11.1	Offentlighetsprincipen .....	26
11.1.1	Allmän handling och diarieföring .....	27
11.2	Dataskyddsförordningen (GDPR).....	27
11.3	Systemklassning .....	27
11.4	Skyddsnivå .....	28

## 1 Introduktion

Information betyder kunskap eller budskap. Det bygger på en samling fakta och används i tal och skrift, med symboler, bilder och data. Information är en av de viktigaste tillgångarna i Tyresö kommuns verksamhet. Kommunens informationssäkerhetsarbete ska skydda informationen mot oönskade händelser som kan medföra negativa konsekvenser för verksamheten och kommunens invånare. Oavsett om informationen behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer omfattas den av informationssäkerhetsarbetet. Med informationssäkerhet menas den samlade effekten av de skyddsåtgärder som syftar till att förebygga, minimera eller eliminera oönskade konsekvenser av olika händelser som negativt påverkar kommunens informationstillgångar. Detta gäller de hot och risker som riktar sig mot IT-stödets och informationsresursernas tillgänglighet, riktighet, konfidentialitet och spårbarhet.

Samtlig personal och förtroendevalda inom Tyresö kommun som använder kommunens informationstillgångar är skyldiga att känna till och följa kommunens policys, riktlinjer och rutiner inom informationssäkerhet. Informationssäkerheten är en integrerad del av alla verksamheter. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten.

Myndigheten för samhällsskydd och beredskap (MSB) har tagit fram ett metodstöd för informationssäkerhetsarbete som syftar till att förtydliga hur ett systematiskt informationssäkerhetsarbete kan utformas utifrån standarderna om Ledningssystem för Informationssäkerhet (LIS). Metodstödet är baserat på standardserien ISO/IEC 27000, vilket är samma standard som Tyresö kommuns informationssäkerhetsarbete, enligt den gällande Informationssäkerhetspolicyn (2021), ska bygga på.

*Informationssäkerhetsinstruktion Användare* ingår i kommunens LIS och är en konkretisering av *Informationssäkerhetspolicyn* och beskriver hur du som användare ska agera för att upprätthålla en god säkerhetsnivå och säkerhetsmedvetenhet. Säkerhetsmedvetenhet innebär att alla som arbetar inom Tyresö kommun själva ska kunna identifiera möjliga risker inom sitt eget arbetsområde, samt att känna till och följa befintliga regler och instruktioner för informationssäkerhet. Säkerhetsmedvetenhet hos dig som användare är mycket viktigt för Tyresö kommun och ligger till grund för Tyresö kommuns informationssäkerhetsarbete.

Dokumentet ersätter tidigare riktlinje Informationssäkerhetsinstruktion – Användare Diarienummer: 2023/KS 0166

## 2 Terminologi

Myndigheten för samhällsskydd och beredskap (MSB) har till sitt metodstöd för informationssäkerhet tagit fram en termbank som innehåller den nationella terminologin för informations- och cybersäkerhetsområdet och innehåller svenska och engelska termer, definitioner och förtydligande anmärkningar på svenska med hänvisning till relevanta källor. Nedan följer ett urval av begrepp som är relevanta för instruktionen.

<b>Applikation</b>	En mjukvara för ett specifikt syfte (t ex Microsoft Word)
<b>Behörighet</b>	Tilldelade rättigheter att använda en informationstillgång på ett specificerat sätt. Rättigheter kan innefatta t.ex. rättigheten för en viss användare att ta del av innehållet i en databas eller att skriva ut från en viss skrivare. För verksamhetssystem ska det, i ett rutindokument, finnas regler för vem som kan beställa behörigheter, hur det går till och vad som är tillåten användning för olika behörigheter.
<b>Behörighetssystem</b>	Ett system som används för att hantera funktioner som rör identitets- och åtkomstkontroll. Tyresö kommun använder Microsoft Active Directory (AD)
<b>Data</b>	Representation av fakta, idéer eller liknande i en form lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel  I speciella sammanhang kan termen ges den vidare definitionen 'sekvens av symboler' eftersom "data" inte

alltid behöver vara en representation eller en instruktion.

Data kan vara såväl digitala som analoga. Skiljer sig från ”Data” i dataskyddslagstiftning där begreppet används synonymt med ”personuppgifter”.

## **Dataskydd**

Åtgärder som ska säkerställa att personuppgifter hanteras lagligt, säkert och ansvarsfullt. Det innebär bl.a. att skydda individers integritet genom tekniska och organisatoriska skyddsåtgärder som förhindrar obehörig åtkomst, ändring eller förlust av data. Regleras genom Dataskyddsförordningen (GDPR) och här används ”data” i betydelsen ”personuppgifter”.

## **Dataskyddsombud**

Fysisk eller juridisk person som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt enligt vad som närmare anges i lagen.

## **Dataskyddsamordnare**

Operativt stödjande funktion som stöttar verksamheten i att säkerställa att personuppgifter behandlas författningsenligt och på ett korrekt sätt enligt vad som närmare anges i lagen.

## **Flerfaktorsautentisering**

Autentisering baserad på flera oberoende tekniker för autentisering. Ofta kombineras något som användaren har, vet eller har som

biometrisk egenskap. Ett exempel på tvåfaktorautentisering kan vara ett smartkort i kombination med ett lösenord. Används synonymt med tvåfaktorsautentisering, 2Fa, multifaktorsautentisering

### **Hårdvara**

Fysisk utrustning (t.ex. dator, serverenhet, mobil)

### **Information**

Relaterar till Data - I strikt mening är det skillnad mellan data och information. Data blir information när någon har tolkat innebörden av dem. Vid t.ex. överföring mellan datorer eller lagring i datorminnen är det data, inte information, som hanteras.

### **Informationstillgång**

Information och informationsbehandlande resurser som är av värde för organisationen. Informationstillgångar kan vara av fysisk och/eller logisk karaktär, t ex:

Information  
Informationssystem  
Nätverk  
Kommunikationstjänster  
Fysiska tillgångar  
Människor och deras kompetens  
Rykte eller varumärke, också kallat immateriella tillgångar.

### **Informationssystem**

Ett system som används för att samla in, lagra och bearbeta information av olika slag i en verksamhet där syftet är att uppfylla ett specifikt verksamhetsbehov. Det innefattar både den tekniska utrustningen och ett strukturerat

arbetsätt med nödvändiga aktiviteter som utförs av personer och/eller datorer. Kan vara både IT-system och verksamhetssystem.

**Informationssäkerhet**

Alla de säkerhetsåtgärder, både tekniska och organisatoriska, som avser att möta informationens skyddsbehov när det gäller konfidentialitet, riktighet och tillgänglighet.

**Informationssäkerhetspolicy**

Informationssäkerhetspolicyn redovisar ledningens viljeyttring och engagemang gällande informationssäkerhetsarbetet.

**Informationssäkerhets-  
instruktion**

Beskriver hur en användare ska verka för att upprätthålla en god säkerhet.

**Informationsklassning**

Informationsklassning är ett sätt att värdera organisationens informationstillgångar utifrån interna och externa krav på konfidentialitet, riktighet och tillgänglighet. Skiljer sig från klassificering som är ett begrepp inom arkiv och informationsförvaltning. Skiljer sig även från säkerhetsklass som är ett begrepp inom säkerhetsskydd.

**Informationsägare**

Ansvarar för att informationen är riktig, tillförlitlig och hanteras enligt beslutat regelverk. I Tyresö kommun följer det ansvaret det ordinarie verksamhetsansvaret.

<b>Informationssäkerhetssamordnare</b>	Informationssäkerhetssamordnarens huvudsakliga arbetsuppgifter är att leda och samordna informationssäkerhetsarbetet bl. a. genom att utbilda, följa upp och ta fram årliga planer för informationssäkerheten. Begreppet används ofta synonymt med CISO (eng. Chief Information Security Officer).
<b>Lagring</b>	Processen att spara och/eller förvara data eller information på ett fysiskt eller digitalt medium. Till exempel lokalt eller i en molntjänst.
<b>Mjukvara</b>	Ett generellt begrepp för program i en dator.
<b>Nätverk</b>	Infrastruktur för datorkommunikation. En sammankoppling av datorer och andra enheter som kan <b>kommunicera och dela information</b> med varandra, vanligtvis via internet. Gör skillnad på <b>Slutet nätverk</b> – t.ex. ett företags- eller kommunnät – där endast behöriga enheter och användare har åtkomst – och <b>Publikt (öppet) nätverk</b> – som offentligt Wi-Fi på caféer eller tågstationer – där vem som helst kan ansluta. Det är osäkrare eftersom trafiken lättare kan avlyssnas.
<b>Nätverksenhet</b>	Utrustning som är kopplad till nätverket, t ex skrivare.

<b>Systemägare</b>	Har ett överordnat ansvar för administration, drift och säkerhet för ett informationssystem.
<b>Systemansvarig</b>	En roll vars funktion har ett delegerat ansvar från systemägaren att säkerställa att beslutat regelverk efterlevs i respektive system.
<b>Systemförvaltare</b>	En roll vars funktion svarar för att den dagliga hanteringen av informationen i systemet följer beslutat regelverk.
<b>Utskriftshanteringssystem</b>	Ett system som möjliggör utskrift och där utskrift kan hämtas i valfri ansluten skrivare efter personlig inloggning (FollowMe Print)
<b>VPN</b>	Virtuellt privat nätverk är en teknik som används för att skapa en säker förbindelse eller "tunnel" mellan två punkter i ett icke-säkert datanätverk.

## 3 Säkert beteende

### 3.1 Allmänt

God kännedom om säkerhet hos dig som användare är mycket viktigt för Tyresö kommun och ligger till grund för Tyresö kommuns informationssäkerhetsarbete. Alla som läser, lägger till, tar bort, förändrar eller på annat sätt påverkar förutsättningarna för informationen i kommunens verksamhet anses vara användare. Du har som användare ett ansvar att känna till och följa befintliga regler och instruktioner för informationssäkerhet samt veta var du finner dessa.

Alla användare inom Tyresö kommun ska skydda den information som man hanterar och kommer i kontakt med. Det är varje användares ansvar att ha kunskap om hur information ska hanteras så att kommunens information förblir korrekt, tillgänglig och inte sprids eller hanteras så att den kan nå av obehöriga.

Närmsta chef är ansvarig för att ge de förutsättningar som krävs för att utbilda och informera dig som användare om informationssäkerhet, både vid nyanställning och kontinuerligt i din tjänstgöring.

### 3.2 Säkerhetsmedvetenhet

Om du lämnar ditt arbete, arbetsplats eller skrivbord utan uppsikt kom ihåg att låsa in eller lägga undan allt känsligt arbetsmaterial så att det inte kan läsas eller nås av obehöriga. En dator som lämnas olåst och utan uppsikt är en säkerhetsrisk. Obehöriga kan använda din dator under din användaridentitet för att få obehörig tillgång till information eller utföra otillåtna handlingar. Tänk på att låsa datorn genom att hålla ner Windows ikonerna + L på tangentbordet då du lämnar den utan uppsikt. Din närmsta chef beslutar om enskilda rum ska låsas som hanterar särskilt känslig information. Lösenordskyddad skärmläckare aktiveras automatiskt efter 15 minuter.

#### 3.2.1 Besöksrutiner i Kommunhuset Tyresö

Vid mottagande av besök till Tyresö kommuns lokaler gäller följande för dig som mottagare och besökare:

1. Besökare ska anmälas i receptionen
2. Besökare ska hämtas i receptionen av ansvarig besöksmottagare
3. Besökare ska under hela besöket hållas under uppsikt
4. Efter besöket ska besökaren följas ner till receptionen igen

Mer information om besök och säkra möten i kommunhuset finns på intranätet. Vi ska i samtliga kommunens lokaler eftersträva en hög säkerhetsmedvetenhet, detta gör vi genom att tydliggöra för besökare att de ska anmäla sig samt att i den mån det går alltid vägleda och hålla besökare under uppsikt. Genom att du är uppmärksam och lyhörd för vilka personer som vistas i kommunens lokaler bidrar du till att upprätthålla en god säkerhetskultur.

### **3.2.2 Muntlig information**

I ditt dagliga arbete utbyter du mycket information muntligen med kollegor och andra människor. Det är lätt att information felaktigt sprids om vi inte är aktsamma på var, hur och vad som diskuteras. Tänk på att:

- Inte tala om sekretessbelagd information i publika utrymmen där obehöriga kan ta del av informationen
- Det är lätt för andra att höra vad du säger när du talar i telefon

### **3.2.3 Fysisk information**

När du skriver ut ett dokument på en skrivare som delas av flera användare är det viktigt att du efter varje utskrift själv hämtar utskrivna dokument. Du bär själv ansvaret om kvarglömda dokument leder till felaktig informationsspridning.

I Tyresö kommun används FollowMe Print. Ditt lösenord i datorn hör ihop med skrivare och kopiator. Efter inslagen kod eller scannat kort i skrivaren kommer utskriften ut, se till att hela utskriften kommer ut och tag hand om denna. Omvandling av kopierade eller inskannade dokument, med säkerhetsklassad information, till e-post är inte tillåtet.

Tänk på att inte låna ut ditt lösenord eller kort. Alla utskrifter kan spåras till specifik användare genom loggar.

Konferensrum och vissa andra utrymmen är utrustade med projektorer och andra stora skärmar, whiteboardtavlor eller pappersblock. Dessa ska självklart användas för att underlätta arbetet men de utgör också en säkerhetsrisk. Tänk på att:

- Alltid sudda ut anteckningar på whiteboard efter avslutat möte
- Lämna inte kvar anteckningar på pappersblock
- Aldrig anteckna sekretessbelagd information på whiteboardtavla eller pappersblock
- Vara uppmärksam på vilken information som kan läsas utifrån via t.ex. fönster

### 3.2.4 Digitala möten

Det viktigt att ha ett säkerhetsmedvetet förhållningssätt till videomöten då det kan vara svårt att säkerställa identiteten hos deltagarna och att obehöriga inte kan lyssna in. Kontrollera alltid vilka som deltar i mötet, dela inte känslig information i öppna eller inspelade möten utan tydlig åtkomstkontroll. Det gäller såväl muntlig information som material som delas på skärm eller skickas som fil. Det är inte tillåtet att använda personliga enheter eller publika nätverk vid hantering av känsliga ärenden. Informationshanteringsplan (IHP) och informationsklassning är vägledande för vilken information som kan delas i videomöten – för information som har ett högt skyddsvärde finns tjänsten Säkra Videomöten.

### 3.3 Förbindelse vid nyanställning

Vid nyanställning och vid undertecknandet av anställningsavtal samtycker du som anställd att följa de regler som finns. Beställning av behörighet och tilldelning till internt nätverk sker enligt rutin för nyanställning och hanteras av din närmaste chef i samråd med Digitaliseringsavdelningen. Vid introduktion av nyanställda finns stödmaterialet *Checklista vid nyanställning* och *Sekretesförbindelse* på intranätet.

## 4 Lösenord

För att nyttja din behörighet i Tyresö kommuns datorer, interna nätverk och IT-system krävs att du har ett personligt användarnamn och lösenord. Det är du som användare som har ansvar för dina personliga inloggningsuppgifter. Det är inte tillåtet, att lämna ut användarnamn eller lösenord till någon annan. All användning av kommunens IT-tjänster kan spåras till specifik användare genom loggar.

### Digitaliseringsavdelningens personal efterfrågar aldrig ditt lösenord

Tänk på att:

- Användarnamn (användar-ID) är inte hemligt men ska hanteras säkerhetsmedvetet
- Skydda ditt lösenord väl, och ditt lösenord ska endast du känna till.
- Andra personer får inte stå bakom dig eller titta över din axel när du skriver in ditt lösenord.
- Omedelbart byta lösenord om du misstänker att någon känner till det.

Använd inte samma lösenord privat som du har på jobbet. Ett bra lösenord är den lättaste vägen till en förbättrad informationssäkerhet. Ett lösenord ska vara lätt att minnas men samtidigt bör det vara så komplext att ingen annan kan

gissa sig till det. Tänk på att konstruera dina lösenord så att det inte på ett lätt sätt kan kopplas till dig som person. Krav på lösenord i interna nätverk och verksamhetskritiska IT-system:

- Lösenordet ska innehålla minst 12 tecken
- Lösenordet ska innehålla minst en stor bokstav, en liten bokstav och en siffra eller ett specialtecken
- Använd inte å, ä eller ö
- Använd med fördel en lösenordsfras som till exempel:

Katten ar svart!

Mitt Hus ar Gult!

Where is the sun?

OBS! Fraserna ovan är bara exempel, använd egna lösenordsfraser.

När lösenord skapas finns 96 tecken till förfogande, det inkluderar stora och små bokstäver, siffror och specialtecken. Det innebär att ett lösenord med två tecken har  $96*96$  möjliga kombinationer, tre tecken ger  $96*96*96$  osv. Det innebär i sin tur att även om ett lösenord är väldigt krångligt och innehåller olika specialtecken kan det knäckas av en maskin inom några sekunder om det innehåller ett för litet antal tecken.

Alltså är det inte nödvändigtvis är komplexiteten i lösenordet som är det viktiga, utan snarare antalet tecken. Ett lösenord med 16 tecken ger ett antal kombinationer som är ett så stort tal att det skulle ta tusentals år för en maskin att gissa alla möjliga kombinationer, detta trots att det med dagens datorkraft går att gissa upp till en triljon gissningar i sekunden.

## 4.1 MFA (Multifaktorautentisering)

Multifaktorsautentisering innebär att det behövs mer än ett lösenord för att verifiera en identitet, till exempel vid inloggning eller signering. Det finns tre faktorer:

- Något man kan – Till exempel lösenord eller PIN-kod. Det är något du vet men som kan bli gissat eller stulet.
- Något man har – Till exempel en authenticator app eller en dosa som genererar engångskoder, de brukar kallas Time-based one-time passwords, eller TOTP. Det är något du äger och måste ha fysisk tillgång till.
- Något man är – Biometriska uppgifter så som fingeravtryck eller ansiktigenkänning. Något som är unikt för en användare och som inte kan glömmas bort eller lånas ut.

Notera att MFA uppnås genom att två eller flera faktorer används – två olika lösenord eller ett lösenord och en PIN-kod innebär inte MFA eftersom det är två ”saker man vet”. Genom att använda MFA med TOTP gör du risken för obehörig åtkomst mycket mindre. Det är ett enkelt sätt att skydda både dig själv och organisationens information.

## **4.2 Byte av lösenord**

För att försvåra stöld av behörighet och lösenord ska alla lösenord bytas ut regelbundet. Som användare ansvarar du för att byta lösenord. I det interna nätverket samt de flesta IT-stöd som kräver inloggning kommer påminna via en automatiskt genererad påminnelse. Livslängden på lösenordet är 12 månader. Det innebär att du kommer att få en påminnelse om att byta lösenord efter drygt 11 månader, om du själv inte valt att byta tidigare.

## **4.3 Spärrad behörighet eller glömt lösenord till användarkonto**

Efter upprepade misslyckade inloggningsförsök kommer ditt användarkonto att spärras, kontakta då Servicedesk.

## **4.4 Ändrade behörigheter**

Du som användare kan behöva förändra dina behörigheter t ex vid byte av tjänst vilket kan innebära både utökning eller nerdragning av rättigheter. Din närmaste chef ansvarar för att beställa behörigheter.

## **4.5 Användarsupport**

All felanmälan och support görs i IT-Portalen på intranätet som går till ServicedeskIT.

# **5 IT-utrustning och Säkerhetskopiering**

## **5.1 Standardutrustning**

All IT-relaterad utrustning (t.ex. dator, mobiltelefon, skrivare, projektorer) och IT-relaterade tjänster är arbetsgivarens egendom samt den information som lagras där. Utrustningen ska användas i verksamheten för arbetsrelaterade ändamål. Visst överseende finns för privat användning så länge det inte inverkar negativt på arbetet eller utsätter Tyresö kommun, Tyresö kommuns IT-miljö och dess information för risker eller utgör brottslig handling.

Privat information som t ex. e-post eller dokumentation bör inte synkroniseras och lagras på arbetsenheter. Arbetsrelaterad information får aldrig synkroniseras till privata enheter.

Din närmsta chef ansvarar för att varje användare har tillräcklig kunskap för att kunna hantera sin IT-utrustning på ett korrekt sätt. Vid utökat behov av IT-utrustning ska du kontakta närmsta chef som avgör behov.

Det finns två huvudgrupper av standardutrustning som kan finnas tillgänglig för dig som användare:

- Fast utrustning
- Mobila enheter

Utrustningen tillhör och ägs av Tyresö kommun, tänk på att:

- Hantera utrustningen aktsamt
- Hantera utrustningen efter de regler som gäller för specifik teknisk utrustning
- Egna fysiska ingrepp får inte genomföras på någon typ av utrustning

## 5.2 Fast utrustning

Stationär dator och skrivare ska användas på ett säkerhetsmedvetet sätt. Skydd mot skadlig kod t ex. viruskydd och brandvägg ska alltid vara installerat på datorn för att förhindra eller försvåra intrång i kommunens datorer och interna nätverk. Känslig information ska sparas på anvisat lagringsutrymme, inte lokalt på datorn. Digitaliseringsavdelningen ansvarar för att alla datorer innehåller nödvändig programvara för att upprätthålla säkerhetsnivån.

Lokalt lagrad information på din dator kan ligga okrypterad och tillgänglig, vilket innebär att den kan läsas av andra om du förlorar kontrollen över din dator. När du sparar information ska detta ske i Tyresö kommuns nätverksbaserade lagringsmapp (G:) eller liknande där informationen omfattas av central säkerhetskopiering. Information som tillhör Tyresö kommun får inte lagras på privata enheter eller molntjänster (exempelvis Dropbox) som inte tillhandahålls av Tyresö kommun. Central säkerhetskopiering görs en gång per dygn på Tyresö kommuns alla system som är uppkopplade på kommunens interna nätverk. Allt material som lagras på Tyresö kommuns servrar och datorer är att betrakta som tillhörande Tyresö kommun och kan kopieras, avlägsnas, flyttas.

Om du saknar någon programvara eller misstänker att dator inte uppfyller andra säkerhetskrav, kontakta Servicedesk.

## 5.3 Mobila enheter

### 5.3.1 Bärbar dator

Tänk på att hantera din bärbara dator och dess information på ett säkerhetsmedvetet sätt. Du ansvarar för att datorn skyddas från stöld och intrång. Tänk därför på var du förvarar din bärbara dator.

Din bärbara dator ska skyddas med inloggning till operativsystemet. Mer information om lösenordshantering i kapitel 4 Lösenord.

För skydd mot skadlig kod t ex. viruskydd och brandvägg samt installation av programvaror gäller samma regler som för stationär dator, se kapitel 5.2 Fast utrustning.

### 5.3.2 Mobiltelefon och surfplatta

Telefonen ska användas till arbetsrelaterade samtal, informationsinhämtning samt verksamhetssystem som kommunen erbjuder för mobilt arbete. Om arbetsuppgifter och ansvarsområde kräver tillgång till arbetsmobil utanför arbetstid kan närmsta chef godkänna privat användande av arbetsmobil.

En mobiltelefon är en mindre dator och är lika utsatta för risker avseende virusmitta och andra risker som vanliga datorer. Använd din e-post i mobilen på samma säkra sätt som din e-post på din dator.

Kommer telefonen i orätta händer så kan all information som du har i e-post och tillhörande bilagor läsas, spridas eller förvanskas. Det är därför av yttersta vikt att mobiltelefonens säkerhetsfunktioner som kodlås m.m. används. För mer information, se kapitel 6.2 Publika trådlösa nätverk.

Appar som installeras på enheten ska uppfylla följande krav:

- Installerade från betrodd källa dvs från App Store, Google Play Store.
- Användaravtalet medger kommersiell användning och ev. licensavtal med Tyresö kommun finns.
- Appen är bedömd som säker för användning inom kommunen.

För att säkerställa att kommunens mobila miljö är säker kan kommunen hindra att vissa appar installeras samt regelbundet kontrollera vilka appar som är installerade. Om en app är säker bedöms av Digitaliseringsavdelningen. Kontakta Servicedesk om du har frågor gällande appinstallationer.

Inga filer eller bilder på din mobiltelefon säkerhetskopieras automatiskt. Har du arbetsrelaterat material på din mobiltelefon som du vill kopiera till din dator, kan detta ske manuellt. Det är inte tillåtet att kopiera annat än arbetsrelaterat material till Tyresö kommuns interna lagringsutrymmen.

För surfplatta gäller samma regler som för mobiltelefon.

**OBS! Det är inte tillåtet att lagra privata filer såsom, datafiler, program, musik eller bilder på utrustning som tillhör Tyresö kommun.**

## **5.4 Flyttbar lagringsmedia**

### **5.4.1 USB och Extern hårddisk**

Tänk på att USB-minnen kan innehålla skadlig kod, t ex de som delas ut på mässor, butiker eller där du på något annat sätt inte kan vara helt säker på att de kommer från en betrodd källa. Använd endast USB-minnen du kan lita på. Se vidare information i kapitel 8. Skadlig kod.

USB-minnen och externa hårddiskar ska hanteras i enlighet med hur informationen på den är klassad och vilka lagrum som är tillämpliga, tänk på att informationen kan utgöra allmänna handlingar och därför kräver gallringsbeslut för att kunna raderas. Se vidare information i kapitel 11 Informationsklassning.

Känslig information som lagras på USB-minnen och externa hårddiskar ska skyddas genom kryptering. Externa hårddiskar bör inte användas förutom i undantagsfall t.ex. vid längre frånvaro från kommunens nätverk. Alla sådana undantag ska stämmas av med närmsta chef.

USB-minnen ska användas med stor försiktighet och måste skyddas mot stöld. Tänk därför på var du förvarar dem. De ska t.ex. inte ligga oskyddade utan uppsikt i bilen eller i publika utrymmen. Så lite information som möjligt ska sparas på USB-minnen då de inte omfattas av central säkerhetskopiering.

Samma säkerhetsmedvetenhet och försiktighet gäller för extern hårddisk som för USB-minne.

### **5.4.2 CD/DVD**

Information på vanliga CD/DVD-skivor går inte att radera vilket innebär att CD/DVD-skivorna ska förstöras efter att informationen använts eller lagrats på det interna nätverket. Informationen på CD/DVD-skivor ska innan anslutning kontrolleras för innehåll av skadlig kod. CD/DVD skivor ska hanteras i enlighet med hur informationen på den är klassad. Kryptering av information ska göras vid behov. Se vidare information i kapitel 10 Informationsklassning.

## **6 Internet**

### **6.1 Molntjänster**

Användande av olika typer av molntjänster förekommer i olika former, till exempel exempelvis Dropbox, GoogleDrive, Microsoft Onedrive.

Användande av molntjänster får endast ske i de fall kommunen har gällande

avtal med leverantören. Användande av molntjänster utan upprättade avtal kan innebära att kommunen bryter mot lagar och förordningar exempelvis GDPR. I de fall en extern leverantör exempelvis inom ett projekt tillhandahåller lagringsytor eller samarbetsytor för det specifika uppdraget eller projektet, rådgör alltid med Digitaliseringsavdelningen innan denna typ av tjänster börjar användas.

## 6.2 Publika trådlösa nätverk

Publika trådlösa nätverk, även kallade hotspots, är nätverk som är vanliga på offentliga platser så som caféer, hotell eller flygplatser. Dessa kan oftast användas för att kostnadsfritt ansluta till internet. Vem som helst kan skapa ett publikt nätverk och det är svårt att veta vilka som är trovärdiga. Följande gäller för anslutning till privata nätverk:

- Publika nätverk är alltid att betrakta som osäkra, använd istället mobilens mobildatadelning (hotspot) om du behöver tillgång till internet utanför kommunens lokaler – det är både säkrare och mer kontrollerat.

## 6.3 E-post

### 6.3.1 Allmänt

Eftersom e-post både är ett effektivt och vanligt förekommande kommunikationshjälpmedel är det viktigt att du som användare vet hur du ska hantera e-posten. Risken att utsättas för skadlig kod, bedrägerier och alltför stora informationsmängder ökar vid e-postanvändning. Det är inte tillåtet att använda något annat än Tyresö kommuns e-postprogram för arbetsrelaterat material.

E-postens inkorg är endast en tillfällig förvaringsplats. Detta betyder att du ska rensa inkorgen och utkorgen regelbundet; minst en gång per vecka. Dina raderade mejl töms automatiskt, varje gång du stänger Outlook. Behöver du ta tillbaka ett mejl kan du göra det inom 30 dagar.

### **Outlook e-post får inte användas för att skicka sekretessbelagd information.**

Hantering av personuppgifter regleras av GDPR, personuppgifter ska inte lagras i e-postsystemet vilket innebär att e-post innehållande personuppgifter ska raderas så snart som hanteringen av ett ärende medger. Känsliga personuppgifter får aldrig lagras i e-post och inkommer denna typ av uppgifter ska eventuellt nödvändiga uppgifter förflyttas till lämpligt verksamhetssystem och e-postmeddelandet omgående raderas. Enligt 5 kap. 1 § OSL ska allmänna handlingar som omfattas av sekretess registreras. Detta görs lämpligen i Lex eller annat system som uppfyller kraven i 5 kap. 2 § OSL.

### 6.3.2 Säkra meddelanden

Medarbetare och verksamheter inom Tyresö kommun som har behov av att skicka känslig information och vara säkra på att det är rätt mottagare som tar del av informationen använder tjänsten Säkra meddelanden. För att använda tjänsten behöver sändare och mottagare logga in med e-legitimation.

### 6.3.3 Bifogade filer och länkar

Det är endast tillåtet att skicka eller öppna mottagna filer som är arbetsrelaterade. Vid problem med bifogade filer eller misstanke felaktiga länkar eller skadlig kod i e-postmeddelande, kontakta Servicedesk.

#### Var källkritisk!

Som användare ska du vara medveten om att skadlig kod fortplantar sig som en bilaga till ett e-postmeddelande. Den bifogade filen kan se ut som ett vanligt dokument, som t.ex. ett textdokument eller en bild. Om du inte känner igen avsändaren och ser att det är en bifogad fil ska du, utan att öppna den, kontakta Servicedesk. Vidta försiktighet innan du öppnar ett e-postmeddelande där:

- Avsändaren är okänd
- Ärendet eller rubriken är tvivelaktig eller om ämnesraden är tom
- Det finns bifogade filer där du blir osäker på innehåll och syfte
- Det finns bifogade länkar där du blir osäker på innehåll och syfte

Det finns även exempel på situationer där hotaktörer utnyttjat att många organisationer använder samma standard för mailadresser i sin domän. De allra flesta anställda inom Tyresö kommun har mailadressen [fornamn.efternamn@tyreso.se](mailto:fornamn.efternamn@tyreso.se), men det finns andra betrodda toppdomäner som mailet kan komma ifrån, t ex @gmail.com, @outlook.com osv. Var därför uppmärksam på innehållet i mailet även om det ser ut att komma ifrån en betrodd avsändare, mer information i kapitel 7 Granska avsändaren.

Programfiler ska inte bifogas i e-post och för att undvika skadlig kod finns dessutom begränsningar att ta emot programfiler.

## 6.4 Sociala medier

I tjänsten ska sociala medier användas restriktivt (t.ex. Facebook, Instagram, LinkedIn) och vara godkänt av chef. Missbruk eller oaktsamhet vid internetanvändning kan leda till disciplinär påföljd.

## 7 Granska avsändaren

### 7.1 Social manipulation

Social manipulation (social engineering) är inom informationssäkerhet metoder för att manipulera personer till att utföra handlingar eller avslöja konfidentiell information. Detta görs metodiskt istället för att göra inbrott eller använda sig av teknisk manipulation. Social manipulation är något som blir vanligare och genomförs på många olika sätt så du bör vara uppmärksam om någon i din närhet visar intresse för specifika delar av ditt arbete som kan vara av känslig karaktär, var alltid säkerhetsmedveten. Kommunens informationssäkerhetssamordnare kan på begäran hålla i utbildningar i ämnet social manipulation.

#### 7.1.1 E-post

Under en lång tid har social manipulation via e-post varit den vanligaste metoden och det brukar kallas phishing eller nätfiske. Som namnet indikerar skickar angriparen ut ett bedrägligt meddelande, vanligtvis innehållande en länk till en bedräglig sida på internet eller en fil som innehåller skadlig kod, till en stor mängd mottagare, t ex medarbetare i en specifik organisation. Ett av de enklaste och mest effektiva sätten att skydda sig mot dessa angrepp är att själv söka upp det som meddelandet länkar till.

#### 7.1.2 Telefonsamtal

Social manipulation är även vanligt förekommande via vanliga telefonsamtal och då kallas det voice-phishing, eller vishing. Det är tyvärr enkelt för en angripare att på olika sätt dölja sitt telefonnummer, eller få det att se ut som att samtalet kommer från ett annat nummer, vilket brukar kallas spoofing. Sen en kort tid tillbaka finns det även lättillgängliga AI-verktyg som kan användas för att klonar röster, så att en angripare på ett mycket trovärdigt sätt kan utge sig för att vara någon annan. Det mest effektiva skyddet är att motringa, eller via en annan kontaktväg bekräfta informationen i samtalet.

#### 7.1.3 Sms

Smishing kallas det när bedrägerier genomförs via sms och det är vanligt förekommande. Meddelanden handlar ofta om försändelser av olika slag som fastnat i leverans på grund av problem med fraktkostnader eller annat. Precis som för telefonsamtal kan en angripare spoofa sitt nummer så att det ser ut att komma från en legitim avsändare. En ytterligare utmaning med bedrägerier via sms är att länkarna i meddelandet är för långa för att få plats i ett sms, vilket blir löst genom vad som kallas länkförkortare. Ofta får länkarna formatet bit.ly/12345 eller liknande och problemet är att det är omöjligt för mottagaren att veta vart länken går. På en dator kan mottagaren föra muspekaren över länken och få en förhandsvisning på vart länken leder, men en förkortad länk kommer samma adress att visas, i det här fallet bit.ly/12345.

#### 7.1.4 Videosamtal

När bilder eller video används för bedrägerier brukar det kallas deep-fakes. Det är en mer ovanlig form av phishing eftersom det kräver mer förarbete av en angripare och kan oftast bara riktas mot enskilda måltavlor. Det finns exempel på AI-verktyg som på ett mycket trovärdigt sätt kan generera både ljud och bild på en person.

## 8 Skadlig kod

Det finns många begrepp för skadliga program, ett samlingsnamn är malware – som är en förkortning av malicious software på engelska. På svenska är det vanligaste begreppet skadlig kod och då inkluderas:

- Virus – Sprider sig genom filer och program och kan orsaka skada
- Trojaner – Ser ut som tillförlitliga program men orsakar skada eller ger hackare obehörig åtkomst till information
- Ransomware – Utpressningsvirus som gör information otillgänglig genom kryptering och kräver lösensumma för upplåsning
- Spyware – Samlar in information utan att du märker det

Skadlig kod används för att skada, stjäla eller manipulera information och kommer in exempelvis genom bifogade filer i e-post, bedrägliga länkar, infekterade webbplatser eller flyttbara lagringsmedia som USB-minnen. Kommunen har både centrala skydd så som brandväggar och viruskydd, men även lokala skydd på de anslutna enheterna.

Det kan vara svårt att identifiera vart skadlig kod kommer ifrån, var därför försiktig med filer som laddas ner eller program som installeras. **Vid misstanke om virus eller annan skadlig kod, kontakta Servicedesk omedelbart.** Några bra metoder för att skydda sig är:

- Var försiktig med e-post – Öppna inte filer och tryck inte på länkar från okända avsändare. Det är bättre att själv söka upp det som skickas eller länkas.
- Se till att datorn är uppdaterad och har uppdaterat viruskydd – Alla programinstallationer och uppdateringar utförs i enlighet med Digitaliseringsavdelningens riktlinjer. Uppdateringar från betrodda källor sker med automatik.
- Ladda bara ner program från betrodda källor – undvik okända webbplatser och appar

## 9 Utanför arbetsplatsen

I Tyresö används VPN för fjärråtkomst. För att få VPN installerat behöver du ha loggat in på kommunens nät på kontoret innan du försöker ansluta till exempel hemifrån.

För att verifiera att den installerats kan du titta efter en liten ikon som ser ut som en blå sköld med en bock ✓ på, vid klockan nere till höger. Om du inte hittar den så du installera den från Applikationskatalogen (tryck Windowsflaggan och skriv Applikationskatalog). Välj att installera Forticlient.

När du sedan ansluter till exempel hemifrån så kommer VPN-programvaran att ansluta så att du kommer åt nätverksenheter och intranätet som om du satt på kontoret. När du är ansluten till VPN får ikonen, den blå skölden med bock, ett gult hänglås. Var medveten om att VPN inte på något vis skyddar din dator på öppna nätverk utan ger bara en säker kommunikationsväg till Tyresö kommuns nätverksresurser. Tänk på att:

- Du representerar Tyresö kommun i all användning av internet
- Känslig information får inte sparas på lokal disk utan ska sparas på av verksamheten anvisad plats
- Kommunens information ska skyddas från alla som är obehöriga
- Ingen annan du själv får använda din arbetsdator då du jobbar hemifrån
- Ha uppdaterat viruskydd installerat

### 9.1 Distansarbete

Från och med 1 januari 2022 gäller riktlinjen för distansarbete i Tyresö kommun. Det innebär att medarbetare kan ha möjlighet att regelbundet arbeta på distans, efter överenskommelse med ansvarig chef. Vid godkännande ska VPN i enlighet med stycket ovan användas. Mer information, mallar och instruktioner om distansarbete finns på intranätet.

### 9.2 Att tänka på vid resor och vid publika platser

Vid resa, på konferens eller hotell utsätts alltid en dator, mobiltelefon, surfplatta eller USB-minne och informationen i denna för en risk för stöld eller skada. Om en dator blir stulen eller kommer i felaktiga händer kan känslig och sekretessbelagd information spridas till obehöriga. Ha alltid uppsikt över din utrustning, var restriktiv med vilken information du tar med dig när du reser.

Säkerställ att din dator är ansluten till VPN när du ansluter till öppna nät. Lämna aldrig stöldbegärlig IT-utrustning (dator, mobil, surfplatta etc.) i bilen, på tåget, i hotelllobbyn eller bussen utan egen uppsikt. Lämna aldrig din dator ”oläst” oavsett vart du befinner dig, använd Windowsflaggan + L, alternativt

ctrl+alt+delete och ”Lås” eller ”logga ut” för att låsa datorn och använd alltid ett bra lösenord.

## **9.3 Övrigt om IT utrustning**

### **9.3.1 Stöld av IT-utrustning**

Tänk på att förlorad information kan betyda både merarbete för dig som användare och stor skada för Tyresö kommun, om informationen inte kan återskapas eller kommer i orätta händer. Vid stöld av IT-utrustning, ska rapportering göras till Servicedesk så snart stöld av utrustning upptäcks. Chef ansvarar för polisanmälan och säkerställa att Servicedesk kontaktats.

### **9.3.2 Service på IT-utrustning**

All service av IT-utrustning ska ske via Servicedesk. Se till att all information på datorn är synkroniserad till kommunens nätverk så att den inte går förlorad vid service. Service på utrustning kan i vissa fall ske hos tredjepartsleverantör. Detta innebär att utrustningen måste lämnas bort, vilket kan innebära en säkerhetsrisk. Det är inte tillåtet att själv lämna sin dator på service till extern part. Eventuell sparad information lokalt på dator och mobiltelefon kan komma att raderas beroende på vad servicen innefattar. Servicedesk genomför vid behov ominstallationer.

### **9.3.3 Kassering av IT-utrustning**

All kassering av IT-utrustning ska ske efter samråd med Digitaliseringsavdelningen, kontakta därför Servicedesk direkt. Digitaliseringsavdelningen följer gällande rutiner för kassering av utrustning och säkerställer att information på lagringsenheter raderas innan kassering.

## **10 Incidenter, rapportering och hantering**

En IT- och informationssäkerhetsincident är en händelse som kan få negativa konsekvenser för Tyresö kommun. En IT- och informationssäkerhetsincident behöver inte påverka oss omedelbart men kan med tiden få konsekvenser och leda till större incidenter. Det är därför viktigt att alla avvikande händelser rapporteras till Servicedesk. Vad är skillnaden mellan informationssäkerhet och IT-säkerhet? Det som skiljer är att det är säkerhet med olika kontext. Informationssäkerhet handlar om att undvika negativ påverkan på konfidentialitet, riktighet och tillgänglighet av information. IT-säkerhet rör hot mot IT-systemen.

Exempel på IT- och informationssäkerhetsincidenter är:

- Internt intrång och intrångsförsök
- Externt intrång och intrångsförsök

- Misstanke om virus eller skadlig kod
- Sabotage på informationsresurser och -utrustning
- Felaktig användning av IT-system
- Funktionsfel

Du ska alltid kontakta Servicedesk om du:

- Blir påverkad av liknande ovannämnda händelser för att få hjälp med bedömning för vidare hantering.
- Om du misstänker att någon använt din användaridentitet eller att du har varit utsatt för någon annan typ av IT- eller informationssäkerhetsincident, kommit åt information eller förvanskat, ska du notera när du upptäckte incidenten eller den avvikande händelsen och dokumentera alla iakttagelser i samband med detta.

Du ska alltid informera din chef vid dessa typer av händelser.

## 11 Informationsklassning

Tyresö kommun har tidigare använt sig av informationsklassningsmodellen KLASSA från SKR. Under 2025 flyttar processen till Informationssäkerhets- och dataskyddsmodule i Stratsys, dock kommer samma metodik att kvarstå.

Informationsklassning är grundläggande för ett systematiskt informationssäkerhetsarbete. Det är en process som stödjer arbetet med att leva upp till kommunens policy för informationssäkerhet genom att bestämma nivåer för konfidentialitet, riktighet och tillgänglighet för informationen som hanteras. Det går att genomföra klassningar på enskilda informationsmängder eller informationstillgångar, eller en samling av båda. För att klargöra vad det är som klassas är det viktigt att definiera klassningsobjektet. En processororienterad informationskartläggning eller en informationshanteringsplan är bra stöd för att inventera och skapa en helhetsbild över vilka klassningsobjekt en verksamhet har.

<b>Klassificering av säkerhetsaspekter (0-4)</b>	<b>Beskrivning</b>
Konfidentialitet	Informationen kan åtkomstbegränsas, vad blir konsekvenserna om obehöriga får åtkomst?

Riktighet	Informationen är tillförlitlig, korrekt och fullständig, vad blir konsekvenserna om informationen manipuleras?
Tillgänglighet	Behöriga har åtkomst till informationen när de behöver den, vad blir konsekvenserna om informationen är otillgänglig? Konsekvenserna blir ofta allvarligare ju längre tid som informationen är otillgänglig
Spårbarhet	Specifika aktiviteter som rör informationen kan spåras, vad blir konsekvensen om det inte går att se vem som gjort vad med informationen?

Syftet är främst att säkerställa tillräckliga säkerhetsåtgärder, vanligtvis i form av upphandlingskrav och/eller handlingsplaner. Det kan exempelvis vara att säkerställa att konfidentiell information endast lagras på anvisad plats, exempelvis i verksamhetssystem. Detta ger ett underlag till att få kontroll på kommunens informationstillgångar och en grund för god struktur i verksamheternas processer, informationshantering och dataflöden. Ett annat syfte är att tydliggöra vilka författningskrav som ställs på informationsmängden

Som en följd skapas möjligheter för positiva effekter i form av kontinuerlig följsamhet med lagsiftning, ökad kostnadskontroll, bättre styrning och prioriteringar i verksamheten, kortare ledtider vid förändringar, förbättrad upplevelse och förtroende till kommunens service hos medborgare och externa gränssnitt, men även ökad nöjdhet hos medarbetare.

### 11.1 Offentlighetsprincipen

Offentlighetsprincipen regleras i Sverige i grundlag, tryckfrihetsförordningen. De grundläggande reglerna om allmänna handlingars offentlighet finns i denna grundlag, och i vilken utsträckning allmänna handlingar är hemliga anges i offentlighets- och sekretesslagen. Offentlighetsprincipen innebär att myndigheternas verksamhet så långt som möjligt ska ske i öppna former, vilket innebär att allmänheten och massmedia ska ha insyn i statens, regionernas och kommunernas verksamhet. För att upprätthålla en god efterlevnad med offentlighetsprincipen är det viktigt att all informationshantering, inklusive

nyttjandet av e-post, sker i enlighet med kommunens gällande informationshanteringsplaner och rutiner för hantering av allmänna handlingar.

På kommunens hemsida (tyreso.se) finns *Information om Offentlighetsprincipen och sekretess*. 2023 beslutades en ny *Riktlinje för arkiv och informationsförvaltning i Tyresö kommun* och *Reglemente för arkiv- och informationshantering i Tyresö kommun*, även dessa finns tillgänglig på kommunens hemsida.

### **11.1.1 Allmän handling och diarieföring**

Enligt tryckfrihetsförordningen är en handling allmän om den är inkommen till eller upprättad hos kommunen. Huvudregeln är att det råder egenansvar för diarieföring, det är upp till en varje medarbetare att diarieföra de handlingar som hanteras.

## **11.2 Dataskyddsförordningen (GDPR)**

Information är inte alltid personuppgifter, men personuppgifter är alltid information. Då medborgaren står i centrum för kommunens arbete är personuppgifter kommunens enskilt största och mest skyddsvärda informationstillgång. Arbetet med informationssäkerhet står därför i nära relation till data- och integritetskyddsarbetet, som säkerställer skyddet för den personliga integriteten och de grundläggande mänskliga rättigheterna. Medveten styrning och ledning av dessa områden skapar förutsättningar att nyttja digitaliseringen på bästa sätt i strävan att utveckla verksamheten och öka nyttan för medborgarna. All information som i sig själv, eller i kombination med annan information, kan identifiera en person är att se som personuppgifter. Detta gäller för all informationsbärande media, både analogt och digitalt, och även i alla former såsom text, ljud och bild.

Personuppgifter hos en person som har skyddad identitet kan omgärdas av förstärkt skydd, var uppmärksam på detta om du hanterar denna typ av personuppgifter i din verksamhet. Är du osäker på vad som gäller för de personuppgifter som du hanterar så kontakta i första hand din chef. Du kan även kontakta dataskyddsombudaren för din förvaltning, eller kommunens dataskyddsombud.

### **11.3 Systemklassning**

Generellt sett bör klassning av system (molntjänster, applikationer osv.) undvikas, eftersom det innebär att alla informationsmängder som hanteras där får samma skyddsnivå som den mest skyddsvärda informationsmängden, vilken kan bli problematiskt på sikt.

En väldigt skyddsvärd informationsmängd, t ex sekretessmarkerade personuppgifter, skulle dra upp skyddsnivåerna och ställa krav på omfattande säkerhetsåtgärder. Om informationsmängden senare flyttas någon annanstans och tas bort från systemstödet finns en risk för överskydd om kvarvarande

informationsmängder har ett lägre skyddsbehov – med onödiga kostnader som följd. Ur ett långsiktigt perspektiv är det mer effektivt att genom informationsklassning sätta skyddsnivåer på informationsmängder, för att sedan gruppera de informationsmängder som samlas i ett system och på så sätt bedöma skyddsnivån för systemet.

Det är dock vanligt att systemstöd av olika slag samlar en stor mängd information, och olika typer av informationsmängder. Det kan i sig innebära ett ökat skyddsbehov och därför är det bra att genomföra systemklassningar. Den viktigaste delen inför en systemklassning är att sammanställa uppgifter om vilka informationsmängder som hanteras i systemet, även här kan en processororienterad informationskartläggning eller en informationshanteringsplan vara ett bra stöd.

#### 11.4 Skyddsnivå

Skyddsnivåer används för att märka information för att på ett tydligt sätt visa hur informationen får hanteras, även här är informationsklassning och informationshanteringsplan vägledande. Följande struktur gäller i Tyresö kommun.

Bedömning av skyddsnivå	Beskrivning	Exempel på information
Sekretess	Röjd sekretessklassad information kan innebära allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Inlämnade anbud innan tilldelningsbeslut. Personutredningar inom socialförvaltningen. Åtgärdsplaner inom skola.
Intern	Röjd internklassad information innebär endast försumbar negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Arbetsmaterial inför underframtagande av tjänsteskrivelse till politiken.
Offentlig	Röjd öppenklassad information innebär ingen negativ påverkan på egen eller annan	Protokoll arbetsplatsträffar

	organisation och dess tillgångar, eller på enskild individ.	
--	---	--