Piteå kommun

Instruktion för informationssäkerhet

Dokumentnamn	Dokumenttyp	Senast reviderad	Beslutsinstans
Instruktion för informationssäkerhet	Instruktion	2020-10-01	Kommunchef
Dokumentansvarig/processägare	**Version**	**Diarienummer**	**Giltig till**
Kommunledningsförvaltningen	1	20KS472	2021-12-31
Dokumentinformation	Innehåller organisation, ansvar och regler för kommunens samlade informationstillgångar avseende informationssäkerhet		
Dokumentet gäller för	Verksamheter inom Piteå kommun och Piteå kommunkoncern		

Innehållsförteckning

Piteå Kommun

1. Instruktionens roll i Piteå kommuns säkerhetsarbete

Detta dokument redovisar regler och rutiner avseende informationssäkerhet för administration och förvaltning av kommunens samlade informationstillgångar.

Dokumentet är indelat i två kapitel som var för sig beskriver roller, ansvar och rutiner för hur information i kommunens IT-system ska hanteras på ett säkert och betryggande sätt.

kap. 2.x Förvaltning.
kap. 3.x Användare.

2. Säkerhetsinstruktion för förvaltning

2.1. Organisation och ansvar

2.1.1. Övergripande ansvar

Se Riktlinjer för säkerhetsarbetet i Piteå kommun.

2.1.2. Krisledningsnämnd

Krisledningsnämnden tar över ledningen av kommunen vid en extraordinär händelse, vilket innefattar även ansvaret för IT-systemen. Detta för att kunna samordna alla resurser till prioriterade åtgärder. Kommunens plan för extraordinära händelser tillämpas.

2.1.3. Säkerhetsgruppen

Se Riktlinjer för säkerhetsarbetet i Piteå kommun.

2.1.4. Säkerhetsombud

Se Riktlinjer för säkerhetsarbetet i Piteå kommun.

2.1.5. Informationssäkerhetssamordnare

Har till uppgift att leda och samordna Informationssäkerhetsarbetet i kommunen. Informationssäkerhetssamordnaren ingår i säkerhetsgruppen.

Se Riktlinjer för säkerhetsarbetet i Piteå kommunen.

2.1.6. Systemägare

Utsedd systemägare ansvarar för att IT-systemet förvaltas på bästa sätt. Systemägaren fattar avgörande beslut om IT-systemet.

Systemägare har ansvar för att:

- initiera och föreslå den egna verksamhetens behov av IT-stöd till IT-chef i form av kortfattade, översiktliga mål och krav inom områdena. Införande, systemförvaltning, drift och avveckling.
- se till att ha skriftliga överenskommelser med IT-avdelningen gällande servicegrad och tillgänglighet på verksamhetens IT-system.
- vid införande av nya IT-system, driftgodkänna dessa i samråd med IT-avdelningen och Informationssäkerhetssamordnaren.
- ta del av kommunens informationssäkerhetsarbete som kan påverka de egna IT-systemen.
- fastställa ansvar och roller för respektive IT-system (systemansvarig, styrgrupp) samt förmedla detta till IT-chef.
- besluta om hur media med sekretessbelagd information ska avvecklas utifrån styrande lagar och förordningar.
- se till att det finns aktuella systemsäkerhetsplaner för de IT-system man förvaltar över.
- att det finns rutiner framtagna för verksamheternas beställning och avbeställning av behörigheter till IT- systemet

Systemägare, som också är informationssägare och registeransvarig, ansvarar för informationen i resp. IT-system samt för att denna information hanteras på ett ur säkerhetssynpunkt tillfredsställande sätt.

I detta ingår att besluta om:

- vilket informationsinnehåll aktuellt IT-system ska ha
- vilka uppgifter som ska tillhandahållas och hur detta ska ske utifrån vad lagar och förordningar kräver.
- behov och omfattning av loggning
- utbilda användare så att man på ett säkert sätt kan arbeta i resp. IT-system.

Se även under kap. 2.2 som beskriver kommunens rutiner inom områdena införande, förvaltning, drift och avveckling

2.1.7. Systemansvarig

Systemansvarig utses av systemägare och ansvarar för den dagliga användningen av IT-systemet. Systemansvarig samverkar med IT-avdelningen och leverantör för att säkerställa en säker och rationell drift.

Systemansvarig ansvarar bl.a. för att:

- verkställa systemägarens beslut
- ta del av kommunens informationssäkerhetsarbete som kan påverka de egna IT-systemen.
- anmäla till IT-service när personal slutar eller av annat skäl ska ha ändrade behörigheter och tillgång till IT-infrastrukturen.
- sköta användar- och behörighetsadministration för det IT-system man ansvarar över.

- hålla sig informerad om utvecklingen av IT-systemet och påtala behov av förändringar till systemägare och systemtekniker
- dokumentera och rapportera uppkomna fel, brister i systemet till berörda parter som t.ex. systemägare, leverantör, systemtekniker
- uppkomna incidenter rapporteras direkt till Informationssäkerhetssamordnaren
- medverka i planering för införandet av nya releaser/versioner tillsammans med systemtekniker och leverantör
- medverka i tester vid uppdateringar och felrättningar med systemtekniker och leverantör
- bevaka att IT-systemet hålls uppdaterat med felrättningar och säkerhetsuppdateringar.
- bevaka förändringar i IT-systemet som kan påverka verksamheten
- löpande följa upp att det egna IT-systemet stödjer verksamheten på ett bra sätt
- förmedla förslag till förändringar från användare till systemägare och systemtekniker
- se till att reservrutiner är kända och uppdaterade
- nödvändiga licenser och tillstånd finns tillgängliga
- ansvara för utbildning och support beträffande frågor om IT-systemets funktioner och användning gentemot användaren

2.1.8. Personalansvarig

För att säkerställa att endast behöriga användare använder IT-systemen måste verksamheterna anmäla till systemansvarig för resp. IT-system när personal börjar och slutar eller av annat skäl ska ha ändrade behörigheter i de IT-system som krävs utifrån den anställdes arbetsuppgifter.

2.1.9. IT-chef

IT-chefen är systemägare för de IT-system som endast IT-avdelningen har inblick i, dvs. kommunens IT- infrastruktur och har ansvaret för att IT-infrastrukturens olika tekniska delar fungerar. IT-chef utser även en driftchef som är tillika systemansvarig för IT-infrastrukturen och att sköta om driften.

IT-chefen ansvarar för att:

- se till att finns aktuella och skriftliga överenskommelser med verksamheterna gällande servicegrad och tillgänglighet på de IT-system som innefattas av IT-avdelningens driftansvar.
- det upprättas systemsäkerhetsplaner för IT-infrastrukturen och att dessa hålls aktuella och följs.
- ta del av det Informationssäkerhetsarbete som bedrivs i kommunen.
- det finns rutiner och beskrivningar för en säker driftmiljö.
- i samråd med driftchef på IT-avdelningen, se till att IT-infrastrukturen fungerar ihop med kommunens övriga IT-system.

2.1.10. Driftchef

Driftchef utser en eller flera systemtekniker per IT-system som är i drift hos IT-avdelningen. Utsedd systemtekniker ansvara för att resp. IT-system är i drift och fungerar.

Driftchef ansvarar för att:

- se till att rutiner för säkerhetskopiering och förvaring av säkerhetskopierat material följs och fungerar.
- testmiljö med infrastruktur finns tillgänglig.
- reservrutiner, serviceavtal m.m. finns och är uppdaterade, så att systemägarnas krav på längsta tillåtna avbrottstid kan tillgodoses.
- vara teknisk rådgivare till systemägare då förändringar i systemen är aktuella.
- IT-infrastrukturen hålls uppdaterad och fungerar.
- IT-infrastrukturens säkerhet motsvarar kraven från systemägare.
- stödja systemägare i framtagande av rutiner vid händelse av driftstörning.
- att IT-säkerhetsinstruktion: Drift och kontinuitet är aktuell och fungerar.
- det finns en fungerande teknisk support gentemot verksamheterna.

2.1.11. Systemtekniker

Systemtekniker tillhör IT-avdelningen och ansvarar för att driften av kommunens olika IT-system upprätthålls enligt de krav som är överenskomna mellan verksamhet och IT-avdelningen.

Systemtekniker ansvarar för att:

- följa de driftrutiner som finns för resp. IT-system som man har driftansvar över.
- tillhandahålla teknisk support till systemansvarig.
- det finns installations- och driftrutiner dokumenterade och uppdaterade för de system man är tekniskt ansvarig för.
- initiera felsökning vid driftsstörningar, vidta nödvändiga åtgärder och dokumentera dessa.
- ha en kontinuerlig dialog med systemansvarig och leverantör kring olika driftfrågor.
- ta fram avbrotts- och reservrutiner i samråd med driftchef och systemansvarig.

Ytterligare information återfinns i IT-säkerhetsinstruktion: Drift och kontinuitet

2.1.12. IT-service

Syftet med IT-service är att tillhandahålla teknisk support för användarstöd och användare i kommunens IT- miljö.

IT-service ansvarar för att:

- alla inkommande supportärenden dokumenteras och följs upp.
- se till att lösa problem på ett sådant sätt att det inte äventyrar säkerheten i kommunens IT-system.
- i de fall verksamheten vänder sig till IT-service med ärenden som kan misstänkas handla om en incident, hänvisa dessa direkt till kommunens Informationssäkerhetssamordnare.

2.1.13. IT-stöd

Alla beställningar gentemot IT-avdelningen ska expedieras av IT-stöden ute i förvaltningarna eller av dem i förväg utsedd ersättare i deras ställe. Det innefattar även beställningar av användarkonton för anställda i kommunens gemensamma kontodatabas (Active Directory).

Även kontobeställningar gentemot systemansvarig för de IT-system som den anställde behöver få tillgång till.

IT-stöden fungerar som ett bollplank, stöd och rådgivande funktion i frågor som rör IT i den dagliga verksamheten.

För mer information se dokumentet: IT-stödsrollen.

2.1.14. Användare

Varje användare ska följa gällande regler för Informationssäkerhet.

I detta ansvar ingår bl.a. att:

- ta del av och följa aktuella Informationssäkerhetsinstruktioner.
- föreslå förändringar till systemansvarig och systemägare.
- påtala egna behov av utbildning.

Ytterligare information återfinns i kap. 3 Säkerhetsinstruktioner för användare.

2.2. Regler och rutiner för vissa områden

2.2.1. Administration av användarkonton

Detta ska ske vid behov av:

- nyregistrering/avregistrering av användare
- förändring av befintliga användarbehörigheter

I beställningen ska det tydligt framgå följande uppgifter:

- vilka IT-system som användaren har behov av att komma åt
- hur lång tid som användaren ska ha åtkomst till respektive IT system
- önskade kontouppgifter (med ett lösenord som byts vid första inloggningen)
- vid avregistrering av användare, ska det framgå hur producerat material ska hanteras

Innan behörighet ges för användare ska användarstödet på förvaltningen ha sett till att användaren har tagit del av detta styrdokument samt de instruktioner som gäller för den egna arbetsuppgiften

Följande riktlinjer ska gälla för att inaktivera resp. avregistrera ett användarkonto:

- sjukskriven/barnledig (dvs. fortfarande anställd), aktivt konto
- vid längre frånvaro, dölj e-postkontot i adressboken (ta bort användaren ur $-gruppen)
- tjänstledig/vikarier/säsongsanställda (dvs. uppehåller annan anställning), inaktiverat användarkonto, går inte att logga in med

Anställning upphör
Innan anställning upphör ska användaren själv städa bland dokument som utgör arbetsmaterial i sin hemkatalog/OneDrive och i sin e-post.

När en anställning upphör inaktiveras kontot dagen efter och är låst i 30dagar för sen att raderas med tillhörande hemkatalog/OneDrive och e-post

2.2.2. Loggning och spårbarhet

Syftet med loggning är att vid en incident av något slag så ska man i efterhand kunna spåra vilka transaktioner och eller operationer som skett, när och av vem.

Det ligger på systemägarens ansvar att kontrollera om det finns behov eller krav på spårbarhet i verksamhetens IT-system.

I de system där systemägaren kräver någon form av säkerhets/transaktionsloggar så bör minst följande loggas:

- användaridentitet
- in och utloggning med datum och tidpunkt

Där lagar och förordningar sätter högre krav på loggning och spårbarhet så måste systemägaren i samråd med Driftchef ombesörja att detta efterlevs.

Varje systemägare ska även komplettera ovanstående med vilka händelser som är viktiga utifrån verksamhetens behov av loggning.

Systemägaren ska även besluta om:

- hur ofta loggarna ska analyseras
- vem som ansvarar för att analysera dessa
- hur länge loggarna ska sparas och förvaras

Systemägare i samråd med driftchef äger ansvaret att rutiner skapas för ovanstående.

Samtliga IT-system ska ha central synkronisering av alla datorklockor för att säkerställa riktigheten och spårbarheten i loggarna.

2.2.3. Kryptering

Utifrån riskanalys, informationsklassning och i de fall lagar och förordningar direkt styr, ska de IT-system som så kräver, använda sig av kryptering. Beslut om detta tas av systemägare för aktuellt IT-system.

Införande och drifttagning av detta ska ske genom skriftlig beställning av systemansvarig till IT-avdelningen.

Beställningen ska tydligt klargöra:

- vem som har rätt att läsa och redigera krypterad information.
- hur man ska hantera och lagra krypteringsnycklar.
- vilken typ av information som ska krypteras.
- vem som har rätt att besluta samt dela ut behörighet till krypterad information.
- ovanstående punkter ska bifogas som en bilaga till befintlig systemdokumentation.

2.2.4. Införande av IT-system

Innan införande av IT-system ska:

- systemägare, systemansvarig, systemtekniker samt leverantör och supportansvarig vara utsedda och dokumenterade.
- systemen testas, utvärderas och godkännas av systemtekniker och systemansvarig.

Följande ska stämmas av innan införande:

- att man gör en risk- och sårbarhetsanalys (RSA) på IT-systemet.
- att ta fram en systemsäkerhetsplan för IT-systemet.
- uppfylla den tekniska krav spec. för systeminköp framtagen av IT-avdelningen.
- att man har upprättat en dokumenthanteringsplan enligt arkivariens direktiv.

2.2.5. Avveckling av IT-system

Systemägare i samråd med leverantör och driftchef ansvarar för att informationen säkerställs från det IT-system som ska avvecklas med hänsyn till lagar och förordningar som är styrande och den egna verksamheten.

Den informationen som finns i IT-systemet ska gallras och bevaras i enlighet med verksamhetens dokumenthanteringsplan. Om sådan saknas så ska kontakt med arkivarien tas innan avveckling sker.

2.2.6. Systemutveckling

Ingen egen systemutveckling ska normalt ske inom Piteå kommuns verksamheter.

I förekommande fall där undantag från detta sker, ska samtliga punkter i kap.3 i denna skrift gällande IT-system samt nedanstående punkter beaktas:

- ägande och förvaltning av utvecklad källkod ska regleras via skriftliga avtal mellan systemutvecklare och beställare, detta innefattar även de kompletteringarna/förändringar gjorda i köpta IT-system.
- systemägaren är den som äger källkoden i egenutvecklade IT-system.
- utveckling ska bedrivas i labbmiljö som är fysiskt frånskild från driftmiljö så långt detta är möjligt
- utveckling och förändring i program ska dokumenteras noggrant och i detalj med tydlig versionshantering.
- systemägare är även ansvarig vid systemutvecklingsprojekt samt att säkerhetsåtgärderna efterlevs vid utveckling av IT-systemet.

2.2.7. Tillträdesskydd

IT-avdelningens lokaliteter ska skyddas av ett yttre tillträdesskydd för allmänna utrymmen samt ett internt tillträdesskydd för datahall samt övriga utrymmen som innehåller IT-utrusning eller känslig apparatur med koppling mot kommunens IT-infrastruktur och övriga IT-system.

Samtliga knutpunkter för kommunens stadsnät ska vara låsta i av för ändamålet avsedda dataskåp samt att skåpen ska vara placerade i låsta utrymmen, för att minimera risken av sabotage och skadegörelse.

Tillträde till IT-avdelningen och dess datahall ska fattas av driftchef. Kontroll av behörighet till känslig utrustning som berör driften ska:

- registreras och lagras på säkert och betryggande sätt i låsta utrymmen
- obemannade utrymmen ska vara låsta

Tillfälliga besökare till IT-avdelningen tas om hand av den person som är värd för besöket, vilken då ansvarar för säkerheten under besöket.

Besökare som behöver access till IT-avdelningen under en längre period ska registreras i passersystemet och ges tillträde under den tiden, godkännande ska ges av driftchef.

2.2.8. Säkerhetskopiering och lagring

När det gäller kommunens verksamhetsspecifika IT-system så ansvarar Systemägaren för att ta fram lägsta möjliga kravnivå på lagring och säkerhetskopiering, utifrån de styrande lagar och regler som berör verksamheten.

När det gäller de kommunövergripande lagringsytorna dvs. filareor samt e-post, har kommunen en grundnivå med intervall för säkerhetskopiering. Tider för längre lagring av säkerhetskopior än ovan nämnda regleras via överenskommelse mellan verksamhet och IT-avdelningen.

Tider för återställande av förlorad information i verksamhetsspecifika IT-system sker enligt överenskommelse mellan verksamhet och IT-avdelningen.

Utöver detta så ska man även ta hänsyn till verksamhetens dokumenthanteringsplan

2.2.9. Externa anslutningar

Extern uppkoppling för data/teletrafik får endast anslutas mot kommunens infrastruktur efter godkännande av Driftchef. Vilken teknik som är lämplig för detta ska utvärderas utifrån följande kriterier:

- autentiseringsmetod
- skyddsmekanismer för skadlig kod och intrång
- val av media
- vilka tjänster som ska kunna nyttjas
- behov och syfte med anslutningen

Om dataöverföring sker mellan två olika organisationer så ska skriftligt avtal finnas över de anslutningar som nyttjas och där ska framgå hur båda organisationerna samt leverantör av kommunikationsmedia säkerställer sekretess, riktighet och tillgänglighet på den information som transporteras mellan organisationerna.

Avtalet ska även innehålla tydliga ansvarsgränser mellan samtliga parter. Leverantör ska även kunna redogöra för vilka kommunikationsvägar som kommer att nyttjas, hur man säkerställer

drift, sekretess, riktighet och tillgänglighet på kommunikationslinjer eller utrustning som man ej förfogar över. Där leverantör inte kan säkerställa ovan nämnda krav måste båda organisationerna säkerställa detta på eget godtyckligt sätt.

Systemägaren ansvarar för att:

- upprätta lämpliga avtal mellan samtliga parter i samråd med IT-chef.
- det finns aktuell och uppdaterad förteckning över samtliga anslutningar
- all fjärranslutning sker enligt uppställda rutiner
- regelbundet kontrollera vilka uppkopplingar som finns mot Piteå kommuns infrastruktur
- rätt autentisering nyttjas för respektive anslutningsmetod

Förteckning över externa anslutningar bör innefatta för varje anslutning:

- telefonnummer/IP-adresser/förbindelsenummer/LIC/Plint och stativbeteckningar
- placering av utrustning, maskinnamn
- typ av anslutna utrustningar och hänvisning till teknisk dokumentation över befintliga förbindelser

2.2.10. Brandväggar

All IPbaserad trafik till och från Piteå kommun ska termineras i en, eller en klustrad, lösning av brandväggar om så är möjligt.

All administration och konfiguration ska utföras av behöriga systemtekniker utsedd av driftchef. För varje konfigurationsförändring så måste det göras en funktionstest. Med jämna mellan rum ska det även:

- utföras penetrationstester som godkänns av systemägare
- genomgång av regelverk för att säkerställa konfiguration och säkerhet
- säkerhetskopiera konfiguration och regelverk
- utföras stickprovskontroller i loggar efter kända säkerhetshål och attacker

Brandväggslösningens utformning och konfiguration ska vara dokumenterad. Det ska även finnas inbyggt och aktiverat i brandvägg, alternativt kompletterad med skyddsfunktion för skadlig kod för all trafik in och ut genom brandväggen.
Om brandväggslösningen driftas, supporteras eller underhålls av extern leverantör så ska detta regleras noga via avtal med tonvikt på ansvar, sekretess, riktighet och tillgänglighet.

Systemägare beslutar om:

- vad som ska loggas i brandväggen
- vem som ansvarar för uppföljningen av loggarna
- hur ofta uppföljning ska ske
- hur länge loggarna ska sparas

2.2.11. Distansarbete

Arbete utanför organisationens lokaler som kräver uppkoppling mot interna nätverket ska godkännas av respektive verksamhetschef samt driftchef. Dessutom ska systemägare besluta om ett IT-systems information ska få bearbetas på distans med stationär eller mobil utrustning.

Ytterligare information återfinns i kap. 3 Säkerhetsinstruktioner för användare

2.2.12. Internet

Loggning av ska ske av Internettrafiken för att möjliggöra spårning av intrång och missbruk.

Förhållningssätt till Internet och surfning återfinns i kap. 3

2.2.13. E-post

I e-postsystemet ska det finnas loggningsfunktion för inkommande och utgående e-post för att möjliggöra spårning av intrång och missbruk. Vidare ska det även finnas kvittens på all inkommande ärenden via e-post.

2.2.14. Utbildning

Informationsspridning och utbildning ska erbjudas inom Informationssäkerhetsområdet till alla anställda inom Piteå kommun och omfatta:

- säkerhetens betydelse för verksamheten
- innehållet i myndighetens styrdokument för säkerhet

Nya medarbetare ska ges någon form av introduktionsutbildning i samband med att de får behörighet till nätverket och de IT-system som de ska arbeta med.

Systemansvarig ansvarar för att:

- egna medarbetare erhåller information och utbildning om det centrala innehållet i de systemsäkerhetsplaner och policys som de är berörda av
- säkerställa att medarbetaren har tillräckliga kunskaper om säkerhetsreglerna kring de IT-system de ska arbeta med, i samband med att behörighet tilldelas.

Varje enskild medarbetare har det egna ansvaret att påtala behovet av utbildning.

Kontakta kommunens säkerhetsgrupp för information gällande utbildning som rör säkerhetsfrågor.

2.2.15. Kontinuitetsplanering

Systemkrav, rutiner och regler kring driften av kommunens IT-system ska finnas dokumenterade i säkerhetsinstruktion för drift och kontinuitet, för att säkerställa så långt det är möjligt att kommunen kan verka trotts att man drabbas av driftstörningar och avbrott.

2.2.16. Driftgodkännande

Detta avser den process som leder till att fastställa att ett IT-system uppfyller ställda säkerhetskrav.

Systemägaren är den som ska besluta om driftgodkännande. Beslut ska baseras utifrån en granskning och säkerhetsutvärdering som bygger på jämförelse mellan verksamhetens krav och vidtagna drift och säkerhetsåtgärder.

Driftgodkännande processen relateras till aktuell systemsäkerhetsplan och ska omfatta:

- avgränsningar
- granskning av säkerhetsåtgärder i IT-systemet
- utvärdering av granskningen i förhållande till systemsäkerhetsplanens krav
- redovisning av beslutsunderlag samt beslut

2.2.17. Revidering och uppföljning

Uppföljning är en viktig del i IT-säkerhetsarbetet och ska ske löpande

Revidering/uppföljningen ska omfatta att:

- beslutade åtgärder är genomförda för respektive IT-system
- årliga mål är uppfyllda
- verksamheterna uppfyller ställda säkerhetskrav
- revidering av säkerhetsinstruktioner och systemsäkerhetsplaner då behov uppstår

3. Säkerhetsinstruktioner för användare

3.1. Arbetsmaterial och handlingar

När det gäller hantering och klassning av arbetsmaterial och handlingar inom Piteå kommun så hänvisar denna instruktion till dokumentet: Anvisning för ärendeprocessen - Ärendehandbok.

3.2. Användarkonton

Som datoranvändare i kommunen så har du ett par olika användarkonton att ansvara för, beroende på vilken typ av tjänst och arbetsuppgifter du har. Användarkontona ska ses som nycklar som ger dig tillgång till information i kommunens IT-system, dvs. på samma sätt som en vanlig nyckel används för att låsa upp ett skåp eller en fastighet.

Du ansvarar för att:

- se till att ingen annan användare kan få tillgång till ditt lösenord
- glömmer du bort eller inte kan logga in med ett användarkonto så ska det anmälas till IT-service.
- vid lösenordbyte se till att använd dig av minst 8 tecken/siffror/specialtecken (mellanslag, bindestreck…) i lösenordet.
- om din tjänst eller arbetsuppgift kräver, se till att förvara uppgifter om användarkonton inlåsta i säkerhetsskåp
- logga ut ur Windows och stäng av datorn då du lämnar din arbetsplats en längre stund eller vid arbetsdagens slut.

3.3. Distansarbete från hemmet eller annan extern lokalitet

För att du som användare ska få tillgång till att arbeta på distans, ska det godkännas av din närmaste chef med ekonomiskt ansvar samt att ditt IT-stöd ska beställa tjänsten hos IT-service. Utöver detta gäller att:

- support på datakommunikation utanför kommunens nätverk eller verksamheter omfattas EJ av IT-avdelningens ansvar och sköts om av resp. leverantör.
- program som ej presenteras kan betyda att programmet inte går att köra via portal för distansarbete eller att du inte har rättigheter att köra det.

Tjänsten är ett arbetsverktyg samt kommunens egendom och ska därför betraktas som sådan vilket innebär att du inte får:

- låta andra använda distansarbetsplatsen
- låta andra använda ditt användarkonto
- via distansarbetsplatsen ladda ner och/eller skriva ut hemliga handlingar till plats utanför kommunens verksamheter om inte arbetsuppgiften så kräver.

När du lämnar din arbetsplats så tänk på att logga ut eller lås tangentbordet alternativt stäng av din datorutrustning.

Missbruk av ditt användarkonto kan leda till att användarkontot och tillika distansarbetsplatsen om sådan används, stängs av samt att disciplinära åtgärder kan komma i fråga.

3.4. Datorer och tillbehör

All datorutrustning som förvaltas av IT-avdelningen sköts och underhålls av IT-service. Detta innebär att:
Vid behov av ny datorutrustning eller uppgradering av befintlig datorutrustning så skall förvaltningens IT-stöd kontaktas som sköter om beställningar mot IT-avdelningen.

IT-avdelningen har rätt att vid behov utföra centrala uppdateringar på datorer, vilket kan innebära att datorn kan startas upp centralt samt att en eller flera omstarter av datorn kan genomföras. Vid problem med datorutrustningen så ska man i första hand kontakta IT-service.

Användare ansvarar för att bruka datorutrustningen på ett sätt som är ändamålsenligt utifrån verksamhetens behov.

Användaren av datorutrustningen ansvarar för att logga ut och stänga av sin datorutrustning vid arbetsdagens slut Det är inte tillåtet att installera program på egen hand i arbetsdatorn utan godkännande av IT-avdelningen Program som följer med datorn vid leverans eller ominstallation får inte avinstalleras eller manipuleras av användaren.

3.5. Mobila datorer och handenheter

När det gäller uppkoppling mot kommunens nätverk med bärbara datorer, handdatorer, mobiltelefoner eller andra mobila enheter med uppkopplings/synkroniseringsmöjlighet. Dessa ska vara testade, utvärderade och godkända av IT-avdelningen.

3.6. Trådlös uppkoppling

I de lokaler där trådlös datakommunikation finns tillgänglig så bör man se till att man är uppkopplad till det nätverk som är avsett för dig som användare. Att koppla upp sig på okända nätverk som hittas av din dator ska undvikas och betraktas som osäkra nätverk och kan innebära att man utsätter sig för en risk att smittas av virus eller andra intrångsförsök gentemot din dator.

3.7. Virus

Vid misstanke om virus eller andra datorproblem, koppla ur nätverkssladden och kontakta IT-service.

3.8. Incidenthantering

En incident uppstår då något onormalt och oväntat inträffar som potentiellt kan få eller kunnat få allvarliga konsekvenser för verksamheten. Det kan röra sig om händelser som innebär försummande av sekretess, informationsbortfall, avsiktlig kartläggning av nätverk, händelse som har någon form av avsiktligt driftavbrott eller avsiktligt förhindrar tillgång till data i ett IT-system dvs. sabotage.

Incidenter rör sig vanligtvis om:

- större virusangrepp som drabbar större delen av eller hela organisationen
- obehörig åtkomst till information
- missbruk av system, tjänster eller funktioner
- skadlig kod
- dataintrång eller försök till dataintrång
- dator eller annan kringutrustning innehållande viktig eller känslig information blir stulen.
- brottslig handling
- hot eller attacker riktade mot kommunen och dess informationstillgångar
- sekretessbelagd eller känslig information från IT-system hamnar på annat ställe än det som var tänkt från början, vilket kan medföra skada eller men för en medborgare, organisation eller kommunens egen verksamhet.

Förutom att incidenter bryter mot eller hotar bryta mot kommunens egna regler och förordningar, kan de vara straffbara enligt brottsbalken, vilket kan innebära att arbetsgivaren tvingas till att polisanmäla händelsen.

En incident ska följas upp genom dokumentering i form av en incidentrapport, rapporten ska ligga till grund för beslut om åtgärdsplan för att minimera att incidenten ska kunna inträffa igen alternativt som grund för fortsatt utredning.

Alla användare är skyldiga att rapportera in om man är utsatt/drabbad eller upptäcker en händelse som uppfattas skadlig gentemot anställd, kommunen som organisation, andra organisationer eller medborgare.

Alla incidenter ska snarast rapporteras till kommunens Informationssäkerhetssamordnare för utredning/åtgärd.

3.9. E-post

All inkommande e-post till ditt e-postkonto ska normalt sett betraktas som inkommande ärenden tills att du som användare värderat innehållet i varje e-postmeddelande, det är därför viktigt att du som användare kontrollerar och läser igenom din e-post dagligen. Kan du inte själv värdera innehållet bör detta utföras av verksamhetens registrator.

Det är viktigt att e-post och post inte får ligga oöppnad i flera dagar eller veckor vid semester, sjukdom eller annan frånvaro. Inom varje myndighet ska en rutin upprättas för hur post och e-post ska hanteras.

Verktyg finns för att automatiskt gallra bort spam, däremot e-post som är det minsta tveksam om det är spam eller inte, släpps e-posten igenom till användaren för manuell gallring (mappen skräppost).

Alla e-posthantering i Piteå kommun är offentlig och därför är rekommendationen att man inte bör använda den för privat ändamål.

Använd inte e-postsystemet som en lagringsplats av dokument/ärenden och bifogade dokument. All inkommande e-post som betraktas som ärenden skall skyndsamt vidarebefordras till verksamhetens registrator för registrering (diarieföring). Lämpligtvis skickas in till förvaltningsbrevlådan.

Inkommande e-post med bifogade filer bör sparas ut från e-postsystemet och sen raderas från e-posten.

Inkommande e-post med bifogade dokument där avsändaren är okänd eller där avsändaren är känd men där det inte förväntas komma sådant ifrån denne, bör inte öppnas, då det bifogade dokumentet med stor sannolikhet innehåller ett virus eller skadlig kod.

Skicka inte stora mängder bifogad information via e-post, skicka i stället en länk dit mottagaren kan gå och hämta informationen.

Använd inte e-postsystemet för att skicka e-post till alla e-post konton samtidigt, detta klassas som spam, använd istället den interna hemsidan eller andra forum för informationsspridning i stället.

3.10. Surfa på Internet

Internet är idag enskilt största orsaken till att datorer blir smittade av virus och utsatta för skadlig programkod. Att surfa på hemsidor med tvivelaktigt innehåll kan innebära att man utsätter sig själv och kollegor för virus, trojaner eller annan skadlig kod som kan vara skadligt för kommunens informationstillgångar. Dessutom så kan det störa den dagliga driften genom att det sprids i kommunens nätverk.

För att skydda sig mot sådant finns det några och väldigt viktiga punkter att känna till gällande surfning, dvs. att:

- surfning på Internet bör ske med aktsamhet och endast då arbetsuppgiften kräver sådant.
- medveten surfning till, eller nedladdning av pornografiskt, rasistiskt material är EJ tillåtet på kommunens datorer så vida inte arbetsuppgiften kräver det.
- vetskap om barnpornografiskt material i kommunägda datorer leder direkt till avstängning från användarkonto samt polisanmälan
- nedladdning av upphovsrättsligt material som t.ex. musik, filmer eller program där tillstånd eller licens saknas, är EJ tillåtet

Missbruk av ovanstående kan innebära restriktioner alternativt avstängning av användarkonto.

3.11. Hantering av USB minnen eller andra flyttbara lagringsmedier

All hantering av information på flyttbara lagringsmedier som t.ex. USB minnen, externa hårddiskar skall hanteras med varsamhet då risken är stor att man kan bli virus smittad eller att känslig information kommer på villovägar. Använd därför USB minnen endast för temporär lagring, för permanent lagring skall man nyttja de lagrings ytor som tillhandahålls via kommunens datanät.

Om behov finns av att nyttja denna typ av lagringsmedier trotts allt, tänk på att:

- göra en viruskontroll av innehållet på USB minnet innan du öppnar upp informationen, speciellt viktigt om minnet nyttjas i flera olika datorer.
- undvika att lagra verksamhetskritisk eller hemlig information på dessa minnestyper då risken är stor att information kan komma på villovägar och hemlig information röjs.
- förvara minnen innehållande hemlig information, inlåsta i säkerhetsskåp avsedda för ändamålet.
- märka minnet med HEMLIG i röd text om det innehåller sekretessbelagd information.
- ta fram bra säkerhetsrutiner för hur verksamheten ska hantera media innehållande känslig information.