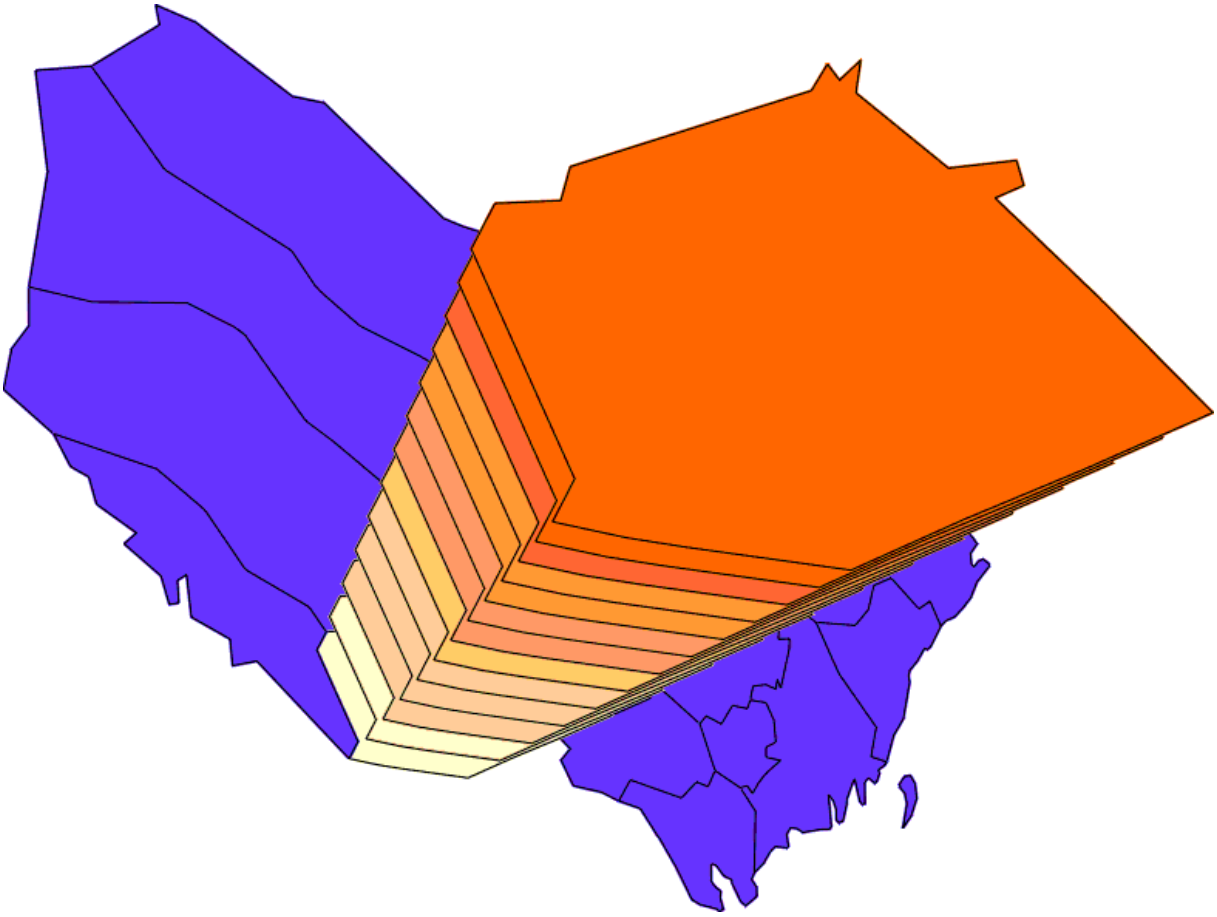
IT säkerhetsinstruktion Användare

Åsele Kommun



1.Bakgrund

Lagen om extraordinära händelser i fredstid hos kommuner och landsting.
Det innebär att kommuner och landsting måste identifiera, analysera, kartlägga och prioritera sina IT-stöd och IT-infrastruktur. Vi kommer att använda Krisberedskapsmyndigheten KBM system BITS för att analysera och prioritera viktiga it system inom kommunen, målet är att kommunen ska klara av basnivån i BITS. Innebörden av lagen innebär en striktare syn på att Vara systemägare av en tillämpning t. ex journal system och IT-infrastruktur. Användare i systemen kommer även att omfattas av tillämpningen.

Mål med IT-säkerhetsarbete

IT-säkerhetsäkerhetsinstruktion är en förutsättning för att det dagliga arbetet ska kunna säkerställas på ett fördefinierat sätt, ett regelverk som talar om hur man hanterar datorn i sitt dagliga arbete, som användare har man sin del i ett säkerhetstänkande. IT-säkerheten ska på ett tydligt sätt uttrycka ledningens mål för IT-säkerheten i kommunen samtliga verksamheter. Information i dagens samhälle är en viktig del i vår organisation för att den ska kunna fungera fullt ut vid en extraordinär händelse.

2. Inloggning

Kommunens datasystem är försedda med ett inloggningsförfarande som innebär att man måste få ett konto till det kommunala datanätet som bereds av kommunens dataavdelning, som samtidigt håller en kortare introduktion i hur systemet fungerar och är uppbyggt.
Du får sedan personligen kvittera att du tagit del av ansvaret det innebär att använda sig av kommunens datanät.

- Tillträde till förvaltningsspecifika applikationer tillhanda hålls av respektive system ägare vilket innebär att avdelningschefen måste godkänna, samt vilken behörighetsnivå innan ett konto läggs upp i systemet.

- Ditt användarkonto är personligt vilket innebär att man inte får lämna ut sin identitet till någon utomstående eller kollega. Användarnamn eller lösen ord får inte heller finnas uppsatta eller synligt i närheten av terminalen, utan skall hanteras strikt.

- Lösen ord får inte heller vara lätt att lista ut t.ex. namn på barnen, katten, hunden etc… vilket försvårar intrångsförsök, efter tre försök så låses inloggningsförfarandet, då måste du kontakta data avd. som låser upp ditt konto.

3. Hantering av information

Som användare i kommunens datasystems så tilldelas man ett visst utrymme på den gemensamma print och fileservern där man sparar sitt data på, den personliga enheten är w: den är knyten till inloggningsnamnet. Vidare så kan man vara ansluten till flera enheter beroende på vilken förvaltning man tillhör t.ex. sociala eller Kultur & Fritid.

Disketter och usb minnen är förbjudet att använda p.g.a. risken att känslig information kan komma på villovägar samt det största hotet, risken för virusspridning.

Det är inte tillåtet att spara på lokala enheter som c: d: och Usb minnen, eftersom data som sparas lokalt kan obehöriga få tillgång till, samt att ingen backup finns på de datafiler.

4. Program

Det är under inga omständigheter tillåtet att installera andra program än vad som finns på datorn vid grundinstallation gjord IT personalen. Det finns flera orsaker varför det inte är tillåtet att installera program själv bl.a. så kan det störa redan installerade program som finns på datorn vilket kan med föra driftsstörningar och haveri.

5. Internet

Kommunens datanät är ansluten till Internet via en brandvägg, som reglerar in och utgående trafik enligt uppsatta regler. Brandväggen skyddar oss mot obehöriga intrångsförsök, samt att den loggar all in och utgående trafik till kommunens datanät, vilket innebär att man kan spåra vilken dator som förorsakar olika typer av incidenter.

Internet är generellt det största hotet inom kommunens dataverksamhet eftersom användaren kan förorsaka stora driftsstörningar genom handhavande fel i sin okunnighet. Därför skall Internet bara användas till det man behöver i sitt vardagliga arbete, det kan vara att söka information inom sitt verksamhetsområde, t.ex. nya lagstiftningar, förordningar, samt att använda sig av olika sökmotorer, för ändamåls mässig informationsökning i sitt vardagliga arbete.

Det är däremot inte tillåtet att under arbetstid surfa på sådana sidor som innehåller pornografiska, rasistiska eller nazistisk karaktär. Förbudet gäller också diskriminerande t.ex. religion, kön, sexuell-läggning, nationalitet, kriminell verksamhet samt satanism.

Det är inte heller tillåtet att ”tanka ner” musik, filmer spelprogram eller andra typer av program eller skicka julkort eller filer typ Youtube ifrån Internet, eftersom det är förenat med stora risker när det gäller virus.

När du surfar på Internet, eller deltar i något diskussionsforum så tänk på att du representerar Åsele Kommun och agerar i enlighet med våra värderingar, så att det du förmedlar på nätet inte skadar kommunen. Tänk på att du lämnar spår av dig på Internet i form av organisationens

ip adress som lagras i en loggfil, denna fil visar vilka platser på Internet som kommunens medarbetare har besökt. Använd inte din vanliga användaridentitet när du är ute på Internet i olika sammanhang, utan skaffa dig en extern användaridentitet.

Hot och möjligheter med Internet.

Internet kan vara ett stort hot mot vår verksamhet om du inte hanterar informationen på ett korrekt rätt, största hotet är virus i olika varianter som följer med i filer som man sparar ner till sitt nätverk. Virus kan ställa till med olika typer av skador, från att radera all data som finns till att sänka nätverkskapaciteten så att inte det går att utföra något arbete via nätet.

Kommunen har ett antivirusprogram som är installerat på alla arbetsstationer som finns I det lokala nätverket, samt att det är installerat på file & printservern och mailservern, uppdatering av viruslistan sker med automatik så att vi hela tiden har det senaste virusskyddet.

Vid tecken på att du har blivit smittat av virus så ta kontakt med data-avd. omedelbart sådan tecken kan vara att maskinen beter sig konstig ,den kan bli långsam, eller att den ”hänger sig”.

6. E-post

E-post har idag blivit en mycket viktigt applikation som används i alla sammanhang allt ifrån kallelser till skriftväxling mellan olika parter, intern som extern.
Men med e-post så har också spridning av virus ökat lavinartat, vilket gör det till ett suveränt hjälpmedel för oseriösa personer att sprida både virus och så kallad spam, spam är oseriös skräppost som kan både innehålla virus och reklam.

- E-post som kommer till en person anställd av Åsele Kommun skall betraktas som all övrig inkommen post till kommun. Meddelande som är allmänna handlingar och som kommer med e-post skall skrivas ut och diarieföras.

- Tänk på att regelbundet radera dina meddelande som finns i din inkorg, utkorg och borttagna meddelande.

- Var selektiv med att skicka eller vidare befordra meddelande som innehåller allt för stora filer.

- Om du behöver bifoga skärmdumpar så klistra in dom i Word dokument och bifoga filen istället.

- Öppna inte meddelande eller bifogade filer som ser misstänkt eller kommer från avsändare som du inte litar på. Vidare befordra aldrig kedjebrev.

- Sprid inte din e-post adress till mindre seriösa ställen, varifrån du kan förvänta dig att få reklam ifrån sedan. Öppna inte länkar i brevet och skicka inte svar på att ni inte vill ha sådan post i forstsättning, ni bekräftar då bara att email adressen fungerar. Använd ditt email efter samma regler som gäller för Internet.

- Julkort per e-post är stora virusspridare. Var försiktig med att öppna sådana, om ni vill skicka sådana själv, gör det via vanligt email eller via en bilaga med bild som är virus testad.

- Om du misstänker att det kommit in virus via e-post systemet så kontakta data avd.

7. Incidenter

Om du misstänker att någon obehörig har använt din användaridentitet och varit inne i systemet så skall du direkt notera när du själv var inne i system sist, notera när du upptäckte intrånget. Ta sedan kontakt med data avd. för konsultation. Dokumentera alla iakttagelser och försök sedan fastställa om kvalitén på informationen har påverkats.

- Om du misstänker: datavirus, kontakta data avd.
- Om du misstänker: Sabotage, stöld, etc. kontakta data avd.

8. Extern utrustning

Bärbara datorer, handdatorer, digitala kameror som du använder utanför din ordinarie arbetsplats utgör en stor säkerhetsrisk, därför bör du tänka på följande.

- Hålla utrustningen under ständig uppsikt om du inte kan låsa in den.

- Inte lagra sekretess belagd information eller annan känslig information på externa enheterna.

- Förvara en kopia på egenhändigt skapad information.

- Komma ihåg att externa enheter ska vara försedd med virusskydd samt lösenord.

9.Extern uppkoppling

Extern uppkoppling mot det administrativa nätet är inte tillåtet, samt att kommunen inte idags läget inte har sådan utrustning som möjliggör en sådan uppkoppling, samt att det inte till dagsläget har funnits några sådan behov

10. Intern uppkopplig

Det är bara tillåtet att koppla upp kommunens egna datorer till det administrativa nätet endast i undantag kan it avd. bevilja tillstånd att koppla upp sig mot det administrativa nätet, och då skall det i första hand användas kommunens egna användas. Externa datorer får bara kopplas upp direkt mot OH-kanonen.
Skall presentationer visas ska det finnas på cd skiva.

11. Fast Telefoni

Kommunens telefoner är ett arbetsredskap och är avsedda för anställdas samtal i tjänsten. Om en anställd vid enstaka tillfällen har behov av att använda telefonen för privat bruk under arbetstid kan detta ske baserat på gott omdöme och sunt förnuft. Vid misstanke om missbruk kan närmaste chef begära en separat samtalsmätning. Åsele kommun, bedriver kontinuerliga samtalsmätningar och uttag av statistik.

Det skall vara lätt för allmänheten att finna telefonnummer till anställda inom Kommunen, det gäller både fast telefoni och mobiltelefoni.
Telefonnummer och mobilnummer skall finnas tillgängliga i den interna telefonlistan.

12. Mobiltelefoni

Mobiltelefoner är ett arbetsverktyg för ökad effektivisering, säkerhet och tillgänglighet. Kommunen tillhandahåller mobiltelefon till anställd som behöver den i sin tjänst.

1. Beslut om vem som skall ha mobiltelefon fattas av behörig chef.
2. Alla kommunens mobiltelefoner skall registreras i kommunens interna telefonlista med uppgifter om innehavare, samt mobilen IMEI nummer, numret används till spärrning av telefon vid stöld eller annan förlust av apparat.
4. Medflyttning från den stationära telefonen till mobiltelefon bör ej ske pga. kostnadsskäl.
5. Aktivera mobilsvar och tala in ett eget hälsningsmeddelande i mobilsvar. håll samtal till och från mobiltelefoner korta och sakliga.
6. Samtal i samband med bilkörning skall undvikas. Måste samtal ske i bil skall handsfree användas.
7. Vid förlust av mobiltelefon skall växeln omedelbart kontaktas som spärrar telefonen och ev. gör stöldanmälan.

Abonnemang & debitering

Mobilabonnemang kan bara beställas genom växeln för telefoni så rätt abonnemangsform och trafikavtal används. Privata samtal skall debiteras den anställde. Omdöme skall iakttas vid förvaring av mobiltelefon med tanke på stöldrisken. Användning av privat mobiltelefon i tjänsten bör undvikas.

Användning av prefix vid mobiltelefoni

Anställda som har mobiltelefon via arbetsgivaren kan erbjudas en tilläggsfunktion med prefix för användning vid privata samtal. Separat faktura skickas till den anställde för samtal som rings med prefixnummer och betalas av denne.
Beställning av prefixnummer för mobiltelefon görs via växeln.

Inköp av mobiltelefoner

Inköp av mobiltelefoner sköts centralt av data avd. Efter beställning av behörig chef.

Medgivelse

Undertecknad har läst och tagit del av IT- säkerhetsinstruktion som gäller för Åsele Kommun administrativa nät.

Åsele den

_____

Användarens Namn

_____

Namnförtydligande