Informationssäkerhetsinstruktion
Användare: Elever
(3:0:1)

Kommunalförbundet ITSAM

Revision: 20130307
Dnr: 2013/00036

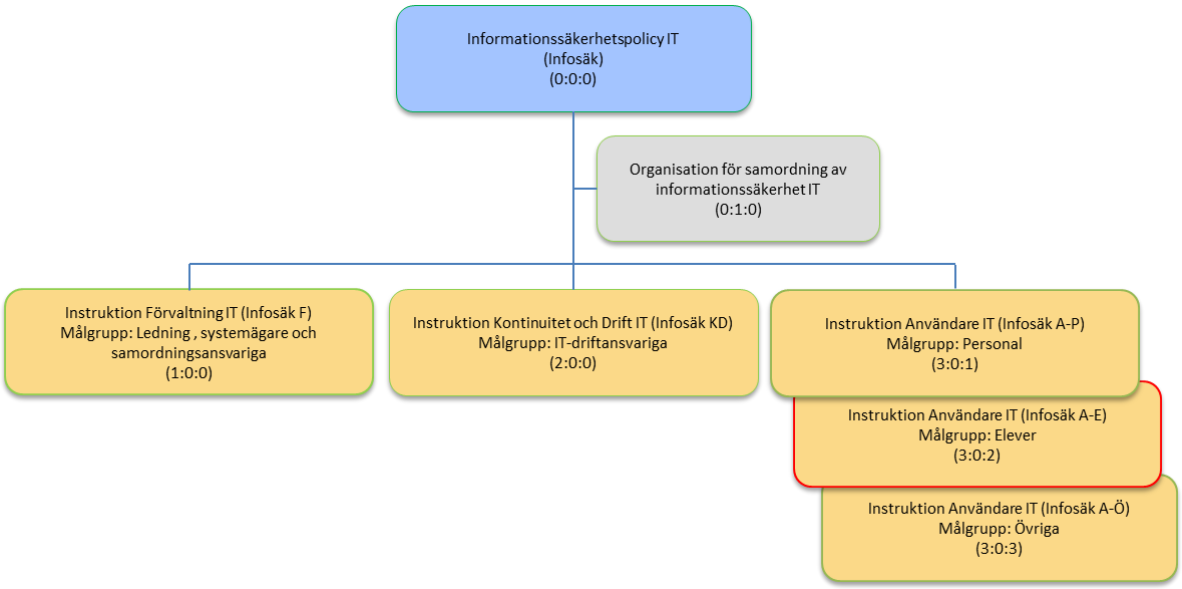
Kommunalförbundet ITSAM, Storgatan 36A, 590 36 Kisa
Tel: 0494 – 197 00, Fax: 0494 – 197 99, Org nr: 222000-2584

Innehåll

Instruktionens roll i informationssäkerhetsarbetet inom IT 3
1. Elevens ansvar 4
2. Åtkomst till information 4
2.1 Behörighet 4
2.2 Inloggning på skolans datorer 4
2.3 Val av lösenord 4
2.4 Byte av lösenord 4
3. Din datorarbetsplats i skolan 5
3.1 Utrustning 5
3.2 Programvaror 5
3.3 Reparation av utrustning 5
3.4 Återvinning av utrustning 5
3.5 När man lämnar datorarbetsplatsen 5
4. Hantering av information och data 5
5. Internet 5
6. E-post 6
7. Incidenter, virus mm 6
7.1 Allmänt 6
7.2 Virus 6
8. Studieavbrott 7
9. Gällande regler och föreskrifter 7

Instruktionens roll i informationssäkerhetsarbetet inom IT

Styrande dokument för informationssäkerhetsarbetet är övergripande informationssäkerhetspolicy IT med tillhörande underliggande policys samt dokument - Organisation för samordning av informationssäkerhet IT samt informationssäkerhetsinstruktionerna Förvaltning IT (Infosäk F), Kontinuitet och Drift IT (Infosäk KD) och Användare (Infosäk A), fördelad på grupperna Personal, Elever och Övriga.



Informationssäkerhetspolicyn syftar till att klarlägga:

- övergripande viljeinriktning och mål för informationssäkerhetsarbetet inom IT
- krav på riktlinjer för områden av särskild betydelse

Organisation för samordning av informationssäkerhet IT syftar till att klarlägga:

- IT-driftorganisationen och dess roll i informationssäkerhetsarbetet inom IT

Informationssäkerhetsinstruktion Förvaltning IT (Infosäk F) syftar till att klarlägga:

- Hur förvaltning av IT-system ska organiseras och struktureras
- IT-organisationen och det ansvar som ingår i de olika rollerna
- regler för systemutveckling, systemunderhåll och incidenthantering

Informationssäkerhetsinstruktion Kontinuitet och Drift IT (Infosäk KD) syftar till att klarlägga:

- IT-organisationen och det ansvar som finns för drift av informationssystemen
- regler för säkerhetskopiering, lagring, driftadministration och kontinuitetsplanering

Informationssäkerhetsinstruktion Användare IT (Infosäk A-P, A-E, A-Ö) syftar till att klarlägga:
hur användare ska verka för att upprätthålla en god säkerhet

Som elev räknas alla som är inskrivna och studerar vid någon av kommunens utbildningsenheter.

1. Elevens ansvar

Information är en viktig tillgång för organisationen. För att skydda denna krävs ett säkerhetsmedvetande hos alla användare. Som elev har man del i ansvaret för säkerheten i informationshanteringen.

För stöd och hjälp när det gäller användningen av skolans datorer kontaktas klassföreståndare/mentor eller skolans IT-ansvariga. Detta gäller även om man har problem med enskilda program, nätverksåtkomst eller åtkomst till sparade arbeten.

2. Åtkomst till information

2.1 Behörighet

Organisationens informationssystem är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information. Vilka behörigheter man får beror på vilken årskurs, skola och klass man tillhör.

2.2 Inloggning på skolans datorer

Innan man loggar in första gången erhålls ett unikt lösenord av klassföreståndare för åtkomst till tjänster och resurser. Lösenordet ska bytas till ett personligt lösenord efter första inloggningen. Samma förfarande gäller för enskilda informationssystem som kräver lösenord för åtkomst. Lösenord är strängt personliga och ska hanteras därefter.

Som användare lämnar man spår efter sig när man är inloggad och gör sitt skolarbete. De loggningsfunktioner som finns i systemen används för spåra obehörig åtkomst. Detta för att skydda informationen och för att undvika att man som användare blir oskyldigt misstänkt om oegentligheter skulle inträffa. Efter tre misslyckade försök att logga in spärras användarkontot. Om det händer måste kontakt tas med klassföreståndare/mentor eller skolans IT-ansvarige för att få ett nytt unikt engångslösenord. Har man glömt sitt lösenord får man även då ta kontakt mes klassföreståndare/mentor eller skolans IT-ansvarige.

2.3 Val av lösenord

För lösenord gäller att de:

- ska vara minst åtta tecken långt
- ska bestå av en blandning av versaler, gemener och andra tecken
- inte kan vara samma som de man hade tidigare

2.4 Byte av lösenord

Byte av lösenord ska:

- ske var 120:e dag för det interna nätverket (en dialogruta visas på skärmen när det är dags, lärare kan visa hur man gör om det är första gången eller om man har glömt hur man gör).
- ske omedelbart om man misstänker att lösenordet blivit röjt

Observera:

- Har man en personlig så kallad elevdator får man byta lösenord på den under eget ansvar.

3. Din datorarbetsplats i skolan

3.1 Utrustning

För den utrustning som man får använda gäller att:

- fysiska ingrepp i datorn eller annan tillhörande utrustning endast får göras av Kommunalförbundet ITSAMs utsedd personal eller av leverantören utsända servicetekniker.
- fel på datorn eller tillhörande utrustning omgående ska anmälas till klassföreståndare/mentor eller IT-ansvarig.
- alla installationer och konfigurationer enbart får utföras av Kommunalförbundet ITSAMs utsedd personal eller av utsedd lärare. Denna punkt gäller ej personliga elevdatorer där reglerna anges i datorkontraktet.

3.2 Programvaror

- Egna program får inte installeras på skolans utrustning.
- Det är inte tillåtet att kopiera skolans programvaror. Det är inte heller tillåtet att installera skolans programvaror på enheter utanför skolans administrativa ansvar. Vad som gäller för personliga elevdatorer regleras detta i datorkontraktet.

3.3 Reparation av utrustning

Vid reparation av datorer inom skolan kan information försvinna från hårddisken. Spara därför alltid viktig information på en säker plats.

3.4 Återvinning av utrustning

Vid återvinning av utrustning kontaktas Kommunalförbundet ITSAMs av skolans IT-ansvarige. Kommunalförbundet ITSAMs hjälper till med förstöring av hårddisk och annan permanent lagringsenhet.

3.5 När man lämnar datorarbetsplatsen

När man lämnar en datorarbetsplats är det viktigt att man loggar ut så att ingen annan kan komma åt egna filer eller göra saker inloggad i annans namn.

4. Hantering av information och data

De filer som lagras på skolans gemensamma utrymmen säkerhetskopieras dagligen. Personliga resurser såsom hemmakatalog mm är enheter man kan använda för lagring av egen information som används i skolan. Det som sparas i personlig hemkatalog kommer lärare och skolkamrater inte åt.

I de fall ”Gemensam” resurs finns, lagras sådan information som inte ska betraktas som privat. I de fall klassmapp finns kan alla i klassen och lärarna titta på sparade arbeten.
Om man sparar på lokala enheter såsom hårddisk, USB-minne eller liknande, görs ingen säkerhetskopiering. Filer som sparats lokala enheter såsom hårddisk, USB-minne eller liknande riskerar du att förlora om datorn går sönder. Lagra därför inte några egna filer på lokala enheter.

5. Internet

När man använder internet kan säkerheten i datornätverk och system påverkas. Mycket beroende på hur och var man surfar. Skolan räknar med att elever som i skolarbetet med lånad datorutrustning surfar på Internet, gör det endast med besök på kända och rekommenderade webbplatser.
Det är inte tillåtet att via Internet titta eller lyssna på material av pornografisk eller rasistisk karaktär. Förbudet gäller även material som anses diskriminerande eller som har anknytning till olaglig/kriminell verksamhet.

Undantag från detta kan beviljas av lärare om informationen på sådana sidor kan ha relevans för elevarbetet.

Tänk på att när man surfar på Internet, deltar i diskussioner eller gör inlägg på digitala sociala nätverk som Facebook, Twitter och liknande under skoltid fortfarande måste följa de regler som skolan har satt upp. Vid användning av Internet från skolans datorarbetsplatser eller andra av skolans lokaler lämnar man alltid spår efter sig.

6. E-post

E-post är ett bra hjälpmedel i skolarbetet men utrymmet för sparande av bifogade filer är begränsat. Tänk därför på att med jämna mellanrum radera gammal e-post i mapparna ”Inkorgen”, ”Skickat”, och ”Borttaget”. Då sparar man plats och riskerar inte att e-postkontot spärras.

- E-post med bilagor utgör ett stort hot när det gäller spridning av virus, trojaner och andra typer av skadlig kod. Klicka inte på länkar i meddelanden utan att först ha kontrollerat med avsändaren att den verkligen skickat en länk till något som inte är en virusrisk.
- E-postsystemet är ett verktyg för skolarbetet och ska helst inte användas för privat bruk.
- Om misstanke finns att virus kommit in via e-postsystemet ska man agera i enlighet med vad som beskrivs i avsnittet Incidenter.
- Kedjebrev och andra oönskade meddelanden (spam) får inte skickas vidare inom skolans e-postsystem.
- Tänk på hur man sprider sin tilldelade e-postadress.
- Om man får hotbrev eller andra kränkande meddelanden till sin e-post ska man spara det och omedelbart prata med sin klassföreståndare eller IT-ansvarig.
- Sekretessbelagd information får inte distribueras via e-post

7. Incidenter, virus mm

7.1 Allmänt

Om misstanke finns att någon använt sitt tilldelade användarnamn och lösenord eller att man varit utsatt för någon annan typ av oönskad datorhändelse ska man:

- skriva ner när man senast var inloggad (datum och tidpunkt).
- skriva ner vad som hänt och när (händelse, datum och tidpunkt).
- omedelbart anmäla det som hänt till sin klassföreståndare/mentor eller IT-ansvarig på skolan.
- kontrollera så att ingen har ändrat i eget sparat arbete.

Om man upptäcker fel och brister i de system som används ska detta rapporteras till klassföreståndare/mentor eller skolan IT-ansvarige.

7.2 Virus

Inom skolan ska samtliga uppkopplade enheter ha programvaror för viruskontroll både i klienterna och i nätverket men man kan ändå drabbas av effekter av det som kallas för skadlig kod. Om misstanke finns att dator innehåller virus ska man:

- dra ur nätverkskabeln och/eller avaktivera det trådlösa nätverkskortet, men låta datorn vara igång.

- omedelbart anmäla förhållandet till klassföreståndare/mentor eller skolans IT-ansvarige. Observera: Anmälan ska göras muntligen, inte via epost.

Läs-/surfplattor, smarta telefoner, digitalkameror, USB-minnen mm kan lätt bli virusbärare eftersom man där kan mellanlagra information mellan olika datorer. Var noga med att den dator man ansluter sådan kringutrustning till har ett uppdaterat virusskydd enligt gällande policy.

8. Studieavbrott

Vid studieavbrott ansvarar man för att:

- i samråd med klassföreståndare/mentor rådgöra om vilket av sitt arbetsmaterial som är verksamhets- eller uppdragsrelaterat och som ska sparas.
- att material av privat natur tas bort.
- att behörigheter man erhållit för åtkomst till informationssystem avbeställs via klassföreståndare/mentor enligt rutiner för detta.

9. Gällande regler och föreskrifter

Informationssäkerhetsinstruktionen Användare A-E (användarpolicyn) med tillhörande kvittens ska skrivas under av myndig elev eller i de fall eleven är omyndig av någon av elevens vårdnadshavare. Underskriven kvittens ska lämnas till klassföreståndaren/mentor. Elev och vid behov vårdnadshavare ska vid underskrift ha tillgång till ett eget exemplar av denna informationssäkerhetsinstruktion. Observera att den kan komma att uppdateras och att det alltid är den senaste uppdaterade versionen som gäller.