Informationssäkerhetsinstruktion för användare i Borlänge kommunkoncern

Beslutad av kommundirektören 2013-05-08, reviderad av kommunfullmäktige 2017-09-19, § 153

Borlänge

Metadata om dokumentet

Dokumentnamn Informationssäkerhetsinstruktioner för användare i Borlänge Kommun		**Dokumenttyp** Instruktion	**Omfattar** Koncernen
Dokumentägare Kommundirektören	**Dokumentansvarig** Informationssäkerhetssamordnare	**Publicering** Författningssamling Insidan	
Författningsstöd			

Beslutad 2013-05-08	**Bör revideras senast** Vid behov	**Beslutsinstans** Kommundirektören Kommunfullmäktige	**Diarienummer** KS2013/190 KS2017/1974
Revidering 1 2013-06-25	Revidering på grund av förändringar i kommunens IT-plattform		
Revidering 2 2017-09-19, § 153	Ändring för att anpassas kommunkoncernövergripande		

Innehållsförteckning

1 Bakgrund och användarens ansvar

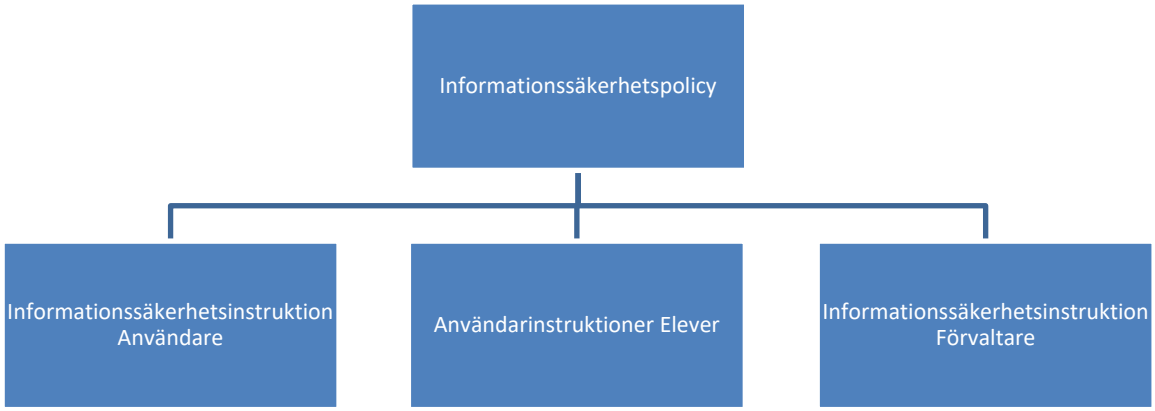
Det här dokumentet, ”Informationssäkerhetsinstruktioner för användare i Borlänge kommunkoncern” riktar sig till alla användare av koncernens information t.ex. förtroendevalda, anställda och extern personal. Dokumentet redovisar hur man som användare ska agera för att upprätthålla en god informationssäkerhet. Chef, uppdragsgivare eller motsvarande är ansvarig för att instruktionen kommuniceras till dem som berörs av den.

Koncernens alla verksamheter är beroende av att dess information är tillgänglig för rätt person vid rätt tidpunkt samt att den är riktig och därmed kan utgöra ett bra beslutsunderlag. Hoten mot våra informationstillgångar är många och för att säkerställa att informationen är skyddad finns det informationssäkerhetskrav som måste uppfyllas. Användare av kommunens information är viktiga aktörer för att säkerställa att så sker.

För att du som användare skall kunna leva upp till de säkerhetskrav som ställs på dig måste du känna till:

- vilka krav som ställs på dig
- vad du ska göra vid incidenter (avvikelser som orsakar eller kan orsaka avbrott eller störning i utrustning eller i en tjänst)
- att du kan få stöd och hjälp från din chef, systemägare, systemförvaltare och IT-kundstöd

Koncernledningens inriktning och mål för informationssäkerhetsarbetet i Borlänge kommunkoncern redovisas i en koncernövergripande informationssäkerhetspolicy. Policyn är huvuddokumentet och till det finns riktlinjer som går in på mer ämnesspecifika regler som fungerar som ytterligare stöd för användare och förvaltare i informationshanteringen. Strukturen ser ut enligt följande:



2 Terminologi

- Informationstillgångar är allt som innehåller information och allt som bär på information.
- Informationssäkerhet är säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet.
- Konfidentiell information får inte nås av eller avslöjas för någon obehörig. Oftast gäller det innehållet i en informationstillgång men ibland är även tillgångens existens hemlig.
- Riktig information innebär att informationen inte får obehörigen förändras, varken av misstag eller på grund av en funktionsstörning.
- Tillgänglig information innebär att informationen går att utnyttja av behörig användare när det behövs och så mycket som det behövs.
- Ett ledningssystem för informationssäkerhet (LIS) är ett verktyg som hjälper oss att upprätta, införa, driva, övervaka, granska, underhålla och förbättra den önskade nivån på informationssäkerhet i vår organisation.

3 Åtkomst till information

3.1 Klassning

Verksamhets- och samhällsviktig information inom koncernen ska riskbedömas och klassas av systemägare och förvaltare utifrån:

- *Riktighet;* att informationen ska vara tillförlitlig, korrekt och fullständig.
- *Tillgänglighet;* att informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet.
- *Konfidentialitet;* att informationen kan åtkomsbegränsas.
- *Spårbarhet; att specifika aktiviteter som rör informationen kan spåras.*

Det är riskerna och klassningen som avgör hur informationen ska skyddas. Då du som användare ska flytta eller spara information på annan media (ex extern hårddisk, USB-sticka eller annan nätverksplats) behöver du känna till hur den är klassad för att kunna avgöra var du får lagra den. Information kan vara klassad i fyra olika nivåer Nivå 1 (låg risk), eller Nivå 4 (hög risk).

3.2 Behörighet och inloggning

Behörighet till koncernens IT-miljö (t.ex. e-post, torg, Sharepoint) tilldelas när en person anställs i koncernen.

Din chef ansöker för din räkning om de verksamhetssystem som du behöver i ditt arbete. Systemförvaltaren för respektive system registrerar dig som användare för att du ska få behörighet till de verksamhetsspecifika system som du behöver tillgång till.Användarnamn och lösenord distribueras till dig via din chef eller systemförvaltare per e-post. Lösenordet du blir tilldelad ska bara användas första gången du loggar in och bör sedan bytas till ett lösenord som bara du känner till. Varje gång du får behörighet till ett nytt IT-system får du ett preliminärt lösenord som du vid första inloggningen ska byta. Använd aldrig någon annans inloggning

3.3 Behörighet för externa användare

Externa användare, t.ex. konsulter som behöver behörighet till koncernens nätverk och system ska via uppdragsgivaren göra en ansökan om behörighet. En sådan ansökan innebär både behörighetsansökan och biträdesavtal. Konsulten ska inte ha tillgång till mer information än hen behöver för sitt uppdrag.

3.4 Lösenord

Lösenordet som är kopplat till ditt användarnamn förhindrar obehöriga från att få tillgång till koncernens information. Vissa system/applikationer har regler för hur lösenordet ska vara konstruerat, andra tillåter ”enklare” lösenord. Tänk på att om du väljer ett enkelt lösenord underlättar du för eventuella angripare att ta sig in i kommunens nätverk och system.

Om du konstruerar ett avancerat lösenord enligt nedanstående instruktioner så är det tillåtet att använda detta lösenord i flera system/applikationer (på arbetet), under förutsättning att du förvarar det på ett säkert sätt.

Detta gäller då du konstruerar ditt lösenord:

- lösenordet ska vara *minst* 8 tecken långt.
- använd inga riktiga ord som lösenord
- använd inte heller namn på familjemedlemmar, husdjur, telefonnummer el dylikt som kan kopplas till dig personligen.
- lösenordet bör bestå av stora och små bokstäver samt siffror och specialtecken i de fall systemet/applikationen tillåter det
- du får inte använda samma lösenord i kommunens system som de du använder hemma
- återanvänd inte lösenorden
- byt lösenord minst 4 gånger per år eller omgående om du misstänker att någon annan känner till det
- lösenord är personliga och det är ditt ansvar att se till att ingen annan känner till dina lösenord
- undvik att dokumentera lösenordet (på t.ex. papper, i datafil eller mobiltelefon)

Tips!
Skapa lösenord enligt samma princip varje gång, exempelvis genom att ta en mening som är lätt att komma ihåg ”Nisse var 32 när han besökte Oslo & Bergen första gången”, skapa sedan lösenord genom att ta första bokstaven i alla ord: ”Nv32nhbO&Bfg”. Lösenordet blir relativt komplicerat men ändå enkelt att komma ihåg.

4 Din arbetsplats

4.1 Utrustning

För din dator med tillhörande utrustning gäller följande:

- om du behöver ytterligare utrustning för att kunna klara av dina arbetsuppgifter ska du anmäla detta till din chef som i sin tur beställer den utrustning som behövs.
- fysiska ingrepp får endast ske av IT-kontoret.
- fel ska omedelbart anmälas till IT-kundstöd
- bärbara datorer skall förvaras inlåsta eller tas med hem när du går för dagen
- när du lämnar din arbetsplats för dagen ska du komma ihåg att dra ned/vinkla persienner för att hindra från insyn.
- privata enheter ska anslutas till BYOD eller Gäst näten.

4.2 Program och applikationer

Arbetsgivaren tillhandahåller de program och applikationer som du behöver i ditt arbete för din dator.

- du får inte ladda ned och installera något från Internet utan att kontakta verksamheternas IT-kontoret först
- det är inte tillåtet att kopiera eller använda koncernens program utanför koncernens verksamhet
- det är inte tillåtet att använda koncernens program för mer än det du behöver i ditt arbete, såsom att söka information i verksamhetssystem för privata ändamål. Detta är att betrakta som dataintrång. Vissa verksamhetssystem lyder under hälso- och sjukvårdslagstiftning och är därmed belagda med striktare regler som bland annat påbjuder regelbundna åtkomstkontroller av användarna.

4.3 När du lämnar din arbetsplats

- logga ut och stäng alltid av datorn när du går hem för dagen.
- lås datorn tillfälligt Ctrl+Alt+Delete välj ”Lås” eller win+L.
- Om den möjligheten finns - lås dörren när du lämnar rummet

4.4 Service och kassering

Koncernen leasar datorer på 3 år, varefter din dator byts ut till en ny.

- när du byter ut/lämnar tillbaka din dator, kontrollera att det inte finns lagrade information på hårddisken C:
- När IT-kontoret fått in din gamla dator raderas allt innehåll innan den skrotas.
- all service av din dator skall utföras av IT-kontoret

5 Distansarbete

När du jobbar utanför kontoret är det extra viktigt att tänka på säkerheten. Jobbar du hemifrån bör du särskilt tänka på att:

- du ansvarar för din dator (och annan it-utrustning) när du tar den utanför koncernens lokaler. Det innebär att du ska skydda den från stöld och åverkan genom att:
  - förvara den på ett säkert sätt
  - inte lämna den obevakad i t.ex bilen om du stannar och handlar
- inte lagra arbetsrelaterad information på en privat dator
- inte lämna datorn obevakad så att ex. familjemedlemmar kan se ditt arbetsmaterial
- inte låta t.ex. familjemedlemmar använda din jobbdator eller annan koncernägd utrustning
- inte använda privat e-post till arbetsrelaterad information

Jobbar du på annat ställe utanför kontoret, exempelvis på tåg bör du tänka på att:

- Använda insynsskydd på datorskärmen om du jobbar med känslig information. Skyddet förhindrar att någon obehörig kan läsa information från din skärm, såvida personen inte sitter mitt framför skärmen.
- Om du talar i telefon, tänk på att du inte vet vem som kan lyssna, prata därför inte om saker som kan vara känsligt.

5.1 Fjärranslutning

När du jobbar hemifrån finns möjlighet att koppla upp dig mot koncernens nätverk via en fjärranslutning (VPN) som ger en säker tillgång till din hemmakatalog och de system och applikationer som du normalt når på jobbet. Jobbar du hemifrån regelbundet skall fjärranslutningen användas för att undvika att information bearbetas och/eller mellanlagras på ett osäkert ställe.

5.2 Mobila enheter

Antalet mobila enheter ökar snabbt bland kommunens användare. Många mobila enheter kan jämföras med en dator. Trots detta saknas ofta de självklara säkerhetsfunktionerna som finns i en dator, t.ex. antivirusprogram, kryptering och brandvägg. Det gör att vi måste vara extra uppmärksamma på hur vi använder och hanterar våra mobila enheter så att de, om de hamnar i orätta händer är obrukbara för upphittaren.

Du som använder en mobil enhet i ditt arbete skall tillämpa följande regler:

- Den mobila enheten ska ha ett MDM system installerat. När det installerats är det möjligt att få e-post och kalendern i telefonen
- Din enhet skall ha ett kodlås, så att du inte kan använda den utan att ange din kod. Koden skall vara en som du kan komma ihåg, men som inte går att gissa sig till eller som kan kopplas till din person. Undvik vanliga sifferkombinationer såsom 1234, 0000, osv.

6 Lagring

Var du bör lagra din information beror på vilken typ av information det är. Vissa lagringsytor är mer säkra än andra. Du bör därför klassificera informationen för att kunna avgöra var den ska lagras. Generellt gäller att iaktta extra försiktighet när det gäller användandet av externa tjänster.

Lagringsyta	**Allmän säkerhetsbedömning**	**Säkerhetskopiering**	**Lämplig för**
T: Torg på nätverket	Koncernens gemensamma lagringsyta. Den kontrolleras och IT ser till att den uppfyller alla säkerhetsregler. Det du sparar skyddas från obehörig åtkomst.	All information säkerhetskopieras.	Information som din arbetsgrupp delar. Möjlighet att skapa mappar som bara är synliga för personer med beviljad åtkomst.
SharePoint	Det är koncernensgemensamma lagringsyta. Den kontrolleras och koncernen ser till att den uppfyller alla säkerhetsregler.	Det som sparas här är skyddat mot obehörig åtkomst och all information säkerhetskopieras.	Här kan du spara arbetsmaterial som ni själva eller fler ska ha tillgång till.
H: Din personliga hemmakatalog	Den kontrolleras och IT ser till att den uppfyller alla säkerhetsregler. Det du sparar skyddas från obehörig åtkomst.	All information säkerhetskopieras.	Information som bara du själv ska ha tillgång till. Endast du har tillgång till ditt H:
C: Lokalt på din dator.	Om datorn kraschar eller blir stulen så är informationen också borta.	Det som sparas här är inte skyddat eller säkerhetskopierat. Undvik att spara här.	Anteckningar och likande som inte är känsliga.
E-postsystem	Koncernens e-postsystem är ett kommunikativt hjälpmedel för de anställda och politiker. E-post bidrar även till enklare överföring av dokument och information som är avsedd för sådan distribution.	Se dokumentet E-postinstruktion	Se dokumentet E-postinstruktion
Molntjänster	Information om hur molntjänsten ska användas och vilken information den är avsedd för ska förmedlas av ägaren av molntjänsten.	Beror på avtal med leverantören av tjänsten. För exakt information kontakta systemförvaltaren för tjänsten.	Endast information som verksamheten har kommit överens om ska lagras på den externa tjänsten.

USB, extern hårddisk etc.	Här skall du inte spara information som är känslig eller sekretessbelagd.	Det som sparas här är inte skyddat eller säkerhetskopierat. Om lagringsytan går sönder eller blir stulen så är informationen också borta.	Här får du inte spara information av känslig/sekretess karaktär, endast temporärt material som inte är av vikt. Undantaget om du använder en extern krypterad hårddisk

7 Internet

All internetanvändning loggas vilket betyder att det finns möjlighet att se vilka sidor som besökts och av vem.

- Arbetsrelaterade filer som laddas ned ska hållas till ett minimum. Vid behov kontakta IT-kundstöd för hjälp.
- Eftersom koncernenss användaradress alltid framgår när vi är uppkopplade, är det viktigt att tänka på att vi representerar koncernen i varje kommunikation på Internet. Det innebär att koncernens adress registreras offentligt på de sidor vi besöker samt att de sidor vi besöker registreras.
- Kontroversiella hemsidor ska inte besökas via koncernens datautrustning.

8 E-post

Regler för användning av e-postsystemet finner du i kommunens ”E-postinstruktion” som finns på Insidan.

9 Personuppgifter

En personuppgift är en uppgift som direkt eller indirekt går att koppla till en person som är i livet. *Vissa typer av personuppgifter betraktas som känsliga. Det är bland annat uppgifter om hälsa, etniskt ursprung och sexuell läggning.*

För att behandling av personuppgifter överhuvudtaget ska vara tillåten krävs att den som behandlar personuppgifterna har en laglig grund för behandlingen. Som användare är det förbjudet att behandla personuppgifter om laglig grund saknas.

All behandling av personuppgifter ska alltid följa reglerna i gällande lagstiftning, tidigare Personuppgiftslagen (fram till 25 maj 2018) och senare EU:s dataskyddsförordning 2016/679 (GDPR).

Mer information om personuppgiftsbehandling och kontaktuppgifter till dataskyddsombud hittar du på Insidan.

10 Incidenter

Incident är en plötslig oönskad händelse som ger eller kan ge negativa konsekvenser för verksamheten, en enskild individ eller för organisationen.

En incident ska rapporteras så snart som möjligt efter att den inträffat om information oavsiktligt eller olagligt:

- Förstörs
- Förloras
- Ändras
- Röjs
- Obehörig åtkomst

Om en incident upptäcks ska den rapporteras in via incidentrapporteringsverktyget på Insidan så snart som möjligt. Rapporten kommer då att skickas till kommunens dataskyddsombud som avgör om incidenten ska skickas vidare till tillsynsmyndigheten.

Om personuppgiftincidenten leder till att den berörda personen i fråga lider hög risk att bli drabbad av påföljder ska de berörda bli informerade, information till berörda ska ges av den asvarige för den drabbade informationstillgången.

11 Skadligkod

Koncernen har virusskydd både i klienterna och på all inkommande trafik från internet, men din dator kan ändå drabbas av virus. Om du misstänker att din dator har fått virus ska du:

- dra ut nätverkskabeln och slå av det trådlösa nätverket, och stäng av datorn.
- omedelbart anmäla förhållandet till informationssäkerhetssamordnare, IT-kundstöd eller närmste chef. Anmälan ska ske per telefon eller besök, **inte per e-post för att undvika att sprida den eventuella skadliga koden vidare.**

Koncernen har installerat skydd mot virus i e-post och bifogade filer. Även om dessa uppdateras kontinuerligt finns risk för intrång av virus och därför skall dessa rekommendationer följas:

- öppna inte okända filer
- var försiktig med e-post från okända
- var försiktig med bifogade filer i e-post även från personer du känner
- stäng av alla funktioner som öppnar filer automatiskt
- anmäl omedelbart misstänkt virus till IT-kundstöd. Anmälan ska ske per telefon eller besök, **inte per e-post för att undvika att sprida det eventuella viruset vidare.**
- låt den infekterade filen ligga orörd - spara inte ned den på nätverket.
- om du är osäker hur på du skall agera, ring alltid IT-kundstöd.

Mobila enheter t.ex. USB-minnen kan lätt bli virusbärare eftersom du kan mellanlagra information mellan olika datorer i dessa.

12 Användarens personliga integritet

Som användare av koncernens informationssystem, nätverk och utrustning behöver du känna till hur uppgifter om dig kan komma att användas av IT-kontoret. För att upprätthålla spårbarheten sparas loggar i alla system och applikationer. I loggarna kan man exempelvis utläsa när användaren varit inloggad, vilka eventuella förändringar hen gjort och vid vilken tidpunkt. Loggarna granskas regelbundet för att upptäcka missförhållanden. Systemägaren beslutar om hur ofta och på vilket sätt loggarna ska granskas.

Vid misstanke om missbruk av kommunens utrustning granskas loggarna avseende den användare eller applikation misstanken gäller. Detta föregås alltid av en diskussion med HR-kontoret och eventuellt facken. Vid misstanke om brott lämnas ärendet vidare till brottsutredande myndighet.
I syfte att optimera användandet av nätkapacitet, diskutrymme m.m. kan IT-kontoret komma att se över innehållet i hemmakataloger och torg. Enstaka filer granskas dock inte i dessa fall, utan endast det totala utnyttjade utrymmet.

13 Avslut eller förändring av anställning

När du avslutar din anställning ansvarar du för att:

- rådgöra med din chef om vilket av ditt arbetsmaterial som ska sparas och överlämnas.
- allt arbetsmaterial du framställt anses vara koncernens egendom och får inte tas med utan chefs godkännande.
- de behörigheter du fått för åtkomst i koncernens informationssystem avbeställs av din chef till systemförvaltaren.
- tömma röstbrevlådan på hälsningsmeddelande och inkomna meddelanden.

14 Rutin för efterlevnad av instruktionen

För att bibehålla en säker informationshantering är det viktigt att IT- och informationssäkerhetsutbildning är en del av introduktionen för nyanställda. Alla anställda ska även informera sig genom att läsa igenom instruktionen. Det kommer även att erbjudas webbaserade utbildningar som alla anställda, politiker och konsulter ska genomföra.