Bodens kommun

Räddnings- och säkerhetsförvaltningen
Marika Anttila, 2303
marika.anttila@boden.se

Regler

Datum
2019-10-31

Godkänd/ansvarig
Informations-
säkerhetssamordnare

Informationssäkerhetsklass: GS

Giltighetstid
Tillsvidare

Gäller för
Användare med åtkomst till kommunens information

Informationssäkerhet

Regler för användare

1. Innehåll

1. Inledning

1.1 Syfte

Information är en av kommunens viktigaste tillgångar. För att skydda dessa krävs ett säkerhetsmedvetande hos alla anställda men även extern personal som exempelvis inhyrda konsulter. Det gäller att du som enskild användare hjälper till att skydda informationen - som vi använder i både tal och skrift - genom sunt förnuft och med stöd från de regler som finns framtagna. Förutom detta dokument så kan du, om du har åtkomst till Insidan, även ta del av mer information kring informationssäkerhet på:

- Informationssäkerhetssidan på Insidan
- Kursportalen på Insidan

1.2 Målgrupp

Samtliga anställda inom Bodens kommun och även externa användare som jobbar på uppdrag av kommunen och har användarbehörigheter till kommunens IT-system och som hanterar kommunens information.

1.3 Ansvarig för dokumentet

Informationssäkerhetssamordnaren ansvarar för att se till att reglerna är aktuella och kommunicerade.

2. Ansvar

När du är anställd vid Bodens kommun eller jobbar på uppdrag av kommunen, har du en skyldighet att följa reglerna om informationssäkerhet. Det är viktigt att i du i ditt dagliga arbete tillämpar reglerna. Om reglerna inte efterlevs kan det innebära konsekvenser för din anställning eller ditt uppdrag.

3. Lösenord

Du ett användarnamn och lösenord (inloggningsuppgifter) för åtkomst till vårt interna IT-nätverk och datorer. Din chef eller din uppdragsgivare överlämnar inloggningsuppgifterna till dig. Om du misslyckas 3 gånger med att logga in, så spärras ditt konto. Kontakta Kundservice IT[1] för att få ett nytt engångslösenord. Du får inte det nya lösenordet direkt via telefon eftersom det inte går att säkerställa att det är rätt person som ringer, ni kommer överens om hur det nya lösenordet skickas via godkända vägar.

Dina arbetsuppgifter ska styra vilken behörighet du får och vilken information du får tillgång till. Din behörighet avgörs av din närmaste chef eller i samråd med uppdragsgivaren.

[1] Kundservice IT telefon (0921-6) 2720

Regler:
Skriv aldrig ner lösenordet på ex. papper. Om du måste skriva ner lösenordet, så behandla det som ett värdepapper.
Ge aldrig ut ditt lösenord till någon.
Använd inte någon annans inloggningsuppgifter.
Använd inte samma lösenord i jobbet och privat.
Du får inte använda automatisk minnesfunktion för lösenordet.
Byte av lösenord: • Vid misstanke om att lösenord är röjt.
Välj ett lösenord enligt nedanstående instruktioner: • Minst 8 tecken • Minst 1 stor bokstav • Minst 1 liten bokstav • Minst 1 siffra eller specialtecken
Lösenord får inte innehålla: - Användarens inloggningsnamn, för- eller efternamn eller delar av namnet - åäöÅÄÖ - Något av de tidigare använda lösenorden

Tips! *Bra lösenord som är enkla att minnas är att tänka ut en mening. Justera sedan stora och små bokstäver och bilda lösenordet. Exempel:*
Mening: ”Klockan 12 går sex bilar till Boden”
Lösenord: K12g6btB

4. Din arbetsplats

4.1 IT-utrustning

Den IT-utrustning som tillhandahålls av kommunen kan vara stationär eller bärbar, en s k mobil enhet. Mobil enhet avser bärbar dator, USB-minne, CD/DVD-skiva, extern hårddisk samt smart telefon och surfplatta.

Har du egen utrustning så gäller reglerna ändå, med det undantaget att IT-utrustningen inte kan felanmälas till kommunens Kundservice IT.

Regler:
Fel eller förlust av IT-utrustning ska omgående anmälas till Kundservice IT[2] eller via Servicewebben[3].

[2] Kundservice IT telefon: (0921-6) 2720
[3] System som hantera beställningar och felanmälningar, finns på Insidan

IT-utrustning och programvaror som ansluts direkt mot kommunens interna nätverk, måste godkännas av IT-kontoret.
IT-utrusning får endast kopplas upp mot publika nätverk om du använder dig av VPN-tunnel eller uppkoppling via Citrix.
Pinkoder/lösenord och automatiskt skärmlås måste användas.
Var medveten om dom risker som finns om du tar med din IT-utrustning utanför EU/EES då annan lagstiftning gäller.

4.2 Kassering av IT-utrustning

IT-utrustning som ägs av Bodens kommun, som kan lagra information måste avvecklas enligt särskilda rutiner.

Regler:
Gör en beställning i Servicewebben för kassering av IT-utrustning, exkl. mobiltelefoner.
Mobiltelefoner lämnas till medborgarservice.

5. Skadlig kod

Skadlig kod kan spridas till ens IT-utrustning om man öppnar bilagor i e-post, importerar filer eller surfar på Internet och klickar på fel länkar, inklusive sådana som finns i sociala medier.

IT-utrustning som drabbats av skadlig kod, kan om det kopplas upp i kommunens nätverk, sprida sig vidare i nätverket och orsaka stor skada.

Kommunens datorer är utrustade med skydd mot skadlig kod. Detta innebär inte fullständig säkerhet då utvecklingen inom detta område är oerhört snabb.

Har du egen IT-utrustning, så måste du se till att du har ett aktuellt skydd mot skadlig kod.

Regler:
Anslut endast godkänd IT-utrustning till kommunens nätverk. *OBS! Anslut aldrig ett USB-minne som du inte vet vad den innehåller. Kontakta istället IT-kontoret.*
Var misstänksam och undvik att klicka på konstiga länkar.
Vid misstanke om skadlig kod: • Låt IT-utrustningen vara

- Dra ur nätverkskabeln och koppla ur WIFI
- Ring Kundservice IT[4] och anmäl incident (**OBS!** Viktigt att du omedelbart ringer in och gör en anmälan).

6. Sociala medier och Internet

När du använder Internet kan säkerheten i kommunens lokala nätverk påverkas i mycket hög grad beroende på ditt beteende. Kommunen förutsätter att den som nyttjar Internet inte besöker webbplatser av tvivelaktig karaktär.

Regler:
Det är inte tillåtet att via Internet titta eller lyssna på material av pornografisk eller rasistisk karaktär. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning, etc.) eller har anknytning till kriminell verksamhet.
I specifika fall kan det dock vara motiverat att besöka sidor som normalt är förbjudna, t ex vid utredningar, omvärldsanalyser mm. Dessa specifika fall skall beslutas av närmaste chef, och dokumenteras med motiv och tillfälle i fall att händelsen senare uppmärksammas.

7. E-post

E-post är för många det vanligaste och viktigaste sättet att kommunicera internt och externt. Dock är det viktigt att tänka på att kommunikation med e-post normalt är helt öppen. Att sända e-post som inte är skyddat med kryptering, kan jämföras med att skicka vykort.

Regler:
E-post får inte användas för att skicka kommunens information med Hög skyddsnivå[5]. Är det information med Utökad skyddsnivå[6] så ska det krypteras[7].
Skriv inte någon känslig information i ämnesraden, då e-post i normalfallet är en allmän handling.
Om du har en e-post med @boden.se, så är det bara tillåtet med automatisk vidarebefordran av e-post inom kommunen, dvs adress som slutar på @boden.se. *OBS! Tänk på första regeln gällande att skicka information med Hög skyddsnivå och Utökad skyddsnivå.*
Var misstänksam och undvik att klicka på konstiga länkar, se regler för

4 Kundservice IT telefon (0921-6) 2720
5 Hög skyddsnivå kan ge allvarlig skada vid förlust, se kap Informationssäkerhetsklassning
6 Utökad skyddsnivå kan ge betydande skada vid förlust, se kap Informationssäkerhetsklassning
7 Se kursportalen för instruktioner

skadlig kod.
Kontrollera vilka som är medlemmar på sändlistor, så att du inte skickar till fel personer.
Använd inte kommunens e-post för privata ändamål.
Gallring av e-post får bara ske enligt information- och dokumenthanteringsplan.

8. Säkerhetskopiering

Det är viktigt att information lagras på rätt sätt för att den garanterat ska bli säkerhetskopierad, så att den kan återskapas i händelse av diskkrasch, oavsiktlig radering m.m. Säkerhetskopiering är extra viktigt för information med högre skyddsnivå än Grundläggande[8].

Regler:
Informationen ska i första hand lagras i verksamhetssystem. Kontakta förvaltningsledaren eller systemägaren om du är osäker på vad som får lagras i verksamhetssystemet.
Information med högre skyddsvärde[9] än Grundläggande skyddsnivå[10] bör inte sparas på flyttbara media (ex. USB-minnen, hårddiskar). På dessa görs ingen automatisk säkerhetskopiering. Om man ändå väljer att spara på flyttbara media, så ska man ha manuella rutiner för säkerhetskopiering.
Ingen information får sparas på ”Lokal disk (C:)”. På denna görs ingen automatisk säkerhetskopiering och vid eventuell ominstallation så raderas allt på ”Lokal disk (C:)”.

9. Spårbarhet och loggning

Spårbarhet innebär att man genom loggning kan identifiera vem som har gjort vad och när och följa förloppet för olika händelser.

Loggarna används för felsökning och för att utreda incidenter eller för att förhindra brott. Loggarna lagras under en viss tid, och är åtkomliga endast för en begränsad grupp administratörer.

All internettrafik och e-post loggas centralt. Kommunen har som arbetsgivare rätt att, utan att meddela användaren, gå igenom dessa loggar för att kontrollera efterlevnad av lagstiftning och riktlinjer. Vid misstanke om brott kan loggfilerna komma att lämnas ut till rättskipande myndighet utan att du som kontoinnehavare meddelas.

[8] Grundläggande skyddsnivå kan ge måttlig skada vid förlust, se kap Informationssäkerhetsklassning
[9] Skyddsvärd information är sådan information som kommunen anser är värd att skydda med hänsyn taget till konsekvensen av vad skadan kan bli
[10] Grundläggande skyddsnivå kan ge måttlig skada vid förlust, se kap Informationssäkerhetsklassning

10. Incidenter

Alla användare har skyldigheter att anmäla incidenter (avvikelser, fel eller brister) som misstänks medföra negativ påverkan på kommunens information. Det kan röra sig om tex: IT-angrepp/intrång, skadlig kod, oskyddad känslig information, stulen dator mm.

Regler:
Notera följande innan du anmäler incident: • Hur stor är påverkan, pga. incidenten (ex. hur många blir påverkade av händelsen?) • Hur bråttom är det att det åtgärdas på en gång? • När upptäckte du incidenten?
Anmäl incidenten på en gång, som en vanlig felanmälan: • Ring till Kundservice IT, telefon: (0921-6) 2720 eller • Självregistrera incidenten i Servicewebben, den hittar du på Insidan.
Är incidenten allvarlig[11], så ska du inte bara anmäla incidenten utan även meddela närmsta chef och informationssäkerhetssamordnaren.

11 Allvarlig konsekvens: kan medföra allvarlig negativ skada på egen eller annan organisation och dess tillgångar, eller på enskild individ.

11. Informationssäkerhetsklassning

Informationssäkerhetsklassning är en konsekvensbedömning och visar vilket skyddsvärde informationen har. Bedömningen görs utifrån tre säkerhetsaspekter: riktighet, tillgänglighet och konfidentialitet. Bodens kommun har en kommunövergripande modell för informationssäkerhetsklassning. Denna ska alla känna till. Ta del av modellen på Informationssäkerhetssidan på Insidan.

Säkerhetsaspekt / Informations-säkerhetsklassning	Riktighet *att vi kan lita på att den är korrekt och inte manipulerad eller förstörd*	Tillgänglighet *att den alltid finns när vi behöver den*	Konfidentialitet *att endast behöriga personer får ta del av den*
Mycket hög skyddsnivå (MHS)	**Konsekvens: Mycket allvarlig skada.** Sveriges säkerhet. Kontakta säkerhetsskyddschef.		
Hög skyddsnivå (HS)	**Konsekvens: Allvarlig skada.** Information där förlust av [*säkerhetsaspekt*] innebär **allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.		
Utökad skyddsnivå (US)	**Konsekvens: Betydande skada.** Information där förlust av [*säkerhetsaspekt*] innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.		
Grundläggande skyddsnivå (GS)	**Konsekvens: Måttlig skada.** Information där förlust av [*säkerhetsaspekt*] innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.		
Ingen skyddsnivå (IS)	**Konsekvens: Ingen skada** Informations där förlust av [*säkerhetsaspekt*] **inte medför någon** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.		

Bild: Bodens kommuns modell för informationssäkerhetsklassning

12. Hanteringsregler

Dessa hanteringsregler ska följas, och vid avvikelser så ska det förankras och beslutas av närmsta chef. Hanteringsreglerna är utifrån säkerhetsaspekten Konfidentialitet[12].

Typ av hantering	1 Grundläggande skyddsnivå - GS	2 Utökad skyddsnivå - US	3 Hög skyddsnivå - HS
Lagring av information			
Lagring på gemensam, filserver (M:/U:)	Ja, men ska avvecklas	Ska avvecklas. Har ni information lagrad här redan, så låt det ligga kvar. Avveckling ska ske, och ny lagringsplats med rätt skydd kommer att erbjudas.	Ska avvecklas. Har ni information lagrad här redan, så låt det ligga kvar. Avveckling ska ske, och ny lagringsplats med rätt skydd kommer att erbjudas.
Lagring på lös lagringsmedia (ex USB sticka)	Ja	Ja, krypterad lagringsmedia, förvaras inlåst, rutin för manuell säkerhetskopiering ska finnas	Ja, krypterad lagringsmedia, förvaras inlåst, rutin för manuell säkerhetskopiering ska finnas
Lagring på lokal hårddisk, exempelvis på datorns skrivbord, c:/	Nej, ingen säkerhetskopiering och risk för radering vid ominstallation.	Nej, ingen säkerhetskopiering och risk för radering vid ominstallation.	Nej, ingen säkerhetskopiering och risk för radering vid ominstallation.
Lagring av information i hurts/skrivbordslåda	Ja	Ja, förutsatt låst låda och att rutiner kring hantering av nycklar/kod finns och efterlevs.	Nej, säkerhetsskåp krävs, enligt SS 3492 eller värdeskåp enligt SS-EN 1143-1, grade 0-III eller valv
Lagring av information i säkerhetsskåp	Ja	Ja	Ja
Lagring av information i IT-stöd/IT-system/ verksamhetssystem	Kontakta systemägaren eller förvaltningsledaren om ni är osäkra	Kontakta systemägaren eller förvaltningsledaren om ni är osäkra	Kontakta systemägaren eller förvaltnings-ledaren om ni är osäkra
Lagring av information utanför Bodens kommun			
Lagring på användarens OneDrive	Ja	Nej	Nej

12 Med Konfidentialitet menas att endast behöriga personer får ta del av informationen.

Typ av hantering	1 Grundläggande skyddsnivå - GS	2 Utökad skyddsnivå - US	3 Hög skyddsnivå - HS
Lagring i appar Office 365 (OneNote, Teams)	Ja	Nej	Nej
Lagring på DokumentCenter	Ja	Nej	Nej
Lagring av personuppgifter hos extern part, konsulter, entreprenörer, samarbetspartners, leverantörer	Ja, förutsatt att personuppgifts-biträdesavtal finns med parten	Ja, förutsatt att personuppgifts-biträdesavtal finns med parten	Ja, förutsatt att personuppgiftsavtal finns med parten. Särskilt sekretessavtal, och speciella krav på leverantörerna
Lagring via öppna internettjänster som ”Dropbox”, ”iCloud”, ”OneDrive(publik)”, ”Google drive” m.fl.	Nej, tillgänglighet och åtkomsträttigheter ligger utom kommunens kontroll	Nej, tillgänglighet och åtkomsträttigheter ligger utom kommunens kontroll	Nej, tillgänglighet och åtkomst-rättigheter ligger utom kommunens kontroll
Lagring/kommunicering /publicering av information på sociala medier, exempelvis Facebook, bloggar, Twitter	Ja, men ta del av dom styrande dokument som gäller för sociala medier. Om det berör personuppgifter, kontakta Dataskyddsombud (DSO).	Nej	Nej
Kassering av information			
Förstöring av pappersdokument *Om det är en allmän handling så ska det finnas gallringsbeslut i information- och dokumenthanteringsplan.*	Ja, i normal pappersåtervinning	Ja, tuggas	Ja, hämtas av godkänd leverantör och ska brännas enligt rutin[13] eller tuggas
Rensning av dator och annan IT-utrustning som innehåller information där Bodens	Ja, beställs via Servicewebben (”*återhämtning av*	Ja, beställs via Servicewebben (”*återhämtning av*	Ja, beställs via Servicewebben (”*återhämtning av*

13 Rutin för sekretesshandlingar
Samla ihop sekretesshandlingarna som ska gallras i en säck, knyt ihop den. Beställ hämtning av sekretessmaterial för destruktion (bränning) med kärl. Kolla med närmsta chef vilka vi har avtal med. De har med sig kärl när hämtningen sker, ni följer med materialet in i bilen och skriver på kvitto om hämtning för leveransen till bränning. Efter bränning kommer ett digitalt destruktionsintyg av Bodens Energi AB. Därefter kommer fakturan.

Typ av hantering	1 Grundläggande skyddsnivå - GS	2 Utökad skyddsnivå - US	3 Hög skyddsnivå - HS
kommun är informationsägare *Om det finns information som är allmänna handlingar, så ska det finnas gallringsbeslut i information- och dokumenthanteringsplan.*	*utrustning*”).	*utrustning*”).	*utrustning*”).
Spridning/kommunikation av information			
Telefonsamtal/ Skype/ Teams	Ja	Restriktivt ev. samtal ska ske enskilt	Ska undvikas, ev. samtal ska ske enskilt
E-post (internt och externt)	Ja	Ja, om det krypteras.	Nej
Pappers post internt	Ja	Ja, förutsatt att den ska vara inneslutet i ett förseglat kuvert inuti internpostkuvertet, med tydlig mottagare.	Ja, förutsatt att den ska vara inneslutet i ett förseglat kuvert inuti internpostkuvertet, med tydlig mottagare.
Pappers post externt	Ja	Ja, förseglat kuvert.	REK, förseglat kuvert.
Publiceras på intranätet	Ja	Nej	Nej
Utskrift	Ja	Ja, förutsatt ”Follow-me-print”, nätverksskrivare med lösenordsskydd alt. lokal skrivare inom fysiskt skalskydd.	Ja, förutsatt ”Follow-me-print”, nätverksskrivare med lösenordsskydd alt. lokal skrivare inom fysiskt skalskydd.
Kopiera	Ja	Ja, måste godkännas av informationsägaren	Ja, i undantagsfall. Måste godkännas av informationsägare.
Skanna till mapp/USB-minne	Ja	Nej	Nej
Skanna till e-post	Ja	Nej	Nej
Sända via fax	Ja	Nej	Nej
Skicka SMS	Ja	Nej	Nej
Märkning	Ja, med: Grundläggande skyddsnivå alt. GS	Ja, med: Utökad skyddsnivå alt. US	Ja, med: Hög skyddsnivå alt. HS

13. Avslutning av anställning eller uppdrag

Information som lagrats på personliga enheter och e-post raderas efter 29 dagar.

Regler:
Rådgör med din chef om vilket av ditt arbetsmaterial som ska sparas.
Allt arbetsmaterial du framställt åt kommunen anses vara Bodens kommuns egendom och får inte tas med utan chefs eller uppdragsgivarens godkännande.
De behörigheter du fått för åtkomst till avbeställs av din chef eller uppdragsgivaren.
Töm röstbrevlådan på hälsningsmeddelanden och inkomna meddelanden, observera att det kan ligga kvar meddelanden trots att du kanske inte använder röstbrevlåda.
Töm e-posten. Kontrollera vad som får gallras, enligt information- och dokumenthanteringsplan.

14. Dokumentets förändringshistorik

Datum	Förändringsorsak	Utfärdare
2019-01-31	Fastställd version	Marika Anttila
2019-10-01	Förändringar så att det matchar externa användare i form av ex. uppdrag åt kommunen. Denna ska med som en del i sekretessavtalet och ska läsas av alla externa användare.	Marika Anttila
2019-10-31	Smärre förändringar efter remiss till samtliga förvaltningar.	Marika Anttila
2019-10-31	Fastställd version	Marika Anttila