ÄLVSBYNS KOMMUN

Användarhandbok för IT

Älvsbyns Kommun version 1.1

Dokumenttyp Handbok	Dokumentnamn Användarhandbok för IT	Fastställd/upprättad	Beslutsinstans Kommunstyrelsen	Giltighetstid
Dokumentansvarig Kanslichef	Version 1.0	Senast reviderad	Dokumentinformation	Detta dokument gäller för Anställda

Innehåll

Bakgrund

Utöver politiskt antagna styrdokument finns det dokument på verksamhetsnivå. Exempelvis rutiner, handböcker, anvisningar som innehåller handfasta råd, och beskrivningar av arbetssätt. Dokumenten reglerar det praktiska och innehåller inte sådant som ska regleras i politiskt antagna styrdokument, eller åtgärder som kräver beslut om finansiering.

Exempel på dokument som upprättas och fastställs på tjänstemannanivå är rutin, handbok, formulär, mall, manual, checklista.

Syfte

Användarhandboken ska vara första stället att leta information på, som rör kommunens IT utrustning och användarfrågor.

Användarhandboken del 1 ska fungera som kort introduktion till nyanställda, var man kan hitta olika uppgifter eller var man ska börja leta.

Användarhandboken del 2 Här hittar du instruktioner för hur du använder kommunens IT-system och utrustning på ett säkert och effektivt sätt.

Del 1 – Introduktion för nyanställda

Introduktion

Välkommen till Älvsbyns kommun.

Denna användarhandbok är avsedd att hjälpa dig att komma igång och att använda kommunens IT-system och utrustning på ett säkert och effektivt sätt.

Här hittar du instruktioner och kontaktinformation.

På kommunens hemsida, https://alvsbyn.se hittar du även personalsidan.

Där finns bland annat manualer, instruktioner och e-tjänster samt en sida för inloggning till verksamhetssystemen.

Alla nya medarbetar ska få information om gällande policys och riktlinjer som rör IT- och informationssäkerhet.

Felanmälan - Kontaktinformation

Felanmälan och supportärenden som kommunanställd gällande IT (datorer med mera) är öppen klockan 08.00 – 16.00, lunchstängt 11.30 – 12.30.

Telefon: 0929-171 00

Kontakta IT-avdelningen dygnet runt via e-tjänsten:
https://insidanalvsbyn.enamnd.se/itsupport

Inloggning

Vid anställning i kommunen erhålls ett användarkonto och initialt lösenord, som måste bytas ut vid första inloggning. Se avsnitt nedan för lösenordsregler.

Närmsta chef tillhandhåller dessa uppgifter vid anställning.

Alla verksamhetssystem man har behörighet till blir åtkomliga först när man loggat in med sitt användarkonto. Alla verksamhetssystem stöder inte automatiskt inloggning, se avsnittet Verksamhetsspecifika system nedan.

Åtkomst till IT baserade system

Visma personalsystem

För att registrera närvaro, frånvaro med mera använd personalsystemet, länk nedan.

Självservice - Medarbetare

Länken fungerar endast när du är inloggad i något av Älvsby kommuns nätverk.

Kontakta närmsta chef för vidare instruktioner.

Microsoft 365

E-post, kalender, ordbehandling, kalkyl med mera finns i Microsoft 365 plattformen. Beroende på licensform finns ytterligare verktyg för planering, skapa enkäter och olika andra samarbetsverktyg.

Teams är en viktig komponent för både intern och extern kommunikation samt att samarbeta och dela information.

Verksamhetsspecifika system

Varje verksamhet har ett eller flera specifika IT-system som du behöver tillgång till.

Vissa system stöder automatisk inloggning, Singel Sign On (SSO) men inte alla.

Din närmsta chef ansvarar för att ordna med inloggning och korrekt behörighet samt utbildning i respektive system.

Del 2 – Användarinstruktioner

Lösenordskrav

Generella lösenordskrav.

Lösenord får inte vara för korta, ska bestå av en blandning av små, stora bokstäver, siffror och specialtecken. Olika system har olika krav på kombinationer av ovanstående.

Lösenordet får inte innehålla blanksteg, eget namn, person- eller telefon-nummer eller på annat sätt vara enkelt att koppla till dig som person eller yrkesroll och därmed enkelt att gissa.

Lösenordet för inloggning på din dator måste bytas var 180:e dag. Andra regler kan gälla för verksamhetssystemen.

Tips: Använd gärna fraser eller meningar som är lätta att komma ihåg. Lösenord får inte skrivas ner på lappar som förvaras på kontoret. Använd i stället lösenords-appar i din telefon eller ”göm” lösenorden i löpande text i din analoga anteckningsbok. Observera att alla system inte klarar svenska tecken – ÅäöÅÄÖ.

Hantering av användarkonto och lösenord

Tänk på nedanstående:

> Lämna aldrig ut användarkonto eller lösenordsuppgifter. Inte till någon. Om ni ombeds göra det, till exempel vid ett supportärende hos systemleverantören, kontakta IT-avdelningen först.
> Byt lösenord om ni misstänker att någon kan ha fått kännedom om ert lösenord.
> Använd inte samma lösenord på flera olika system.
> Aktivera flerfaktorsinloggning där det är möjligt.
> Låt aldrig webbläsaren spara dina lösenord.

Med flerfaktorsinloggning menas en funktion som kräver ytterligare information från dig som användare. Dvs när du loggat in med ditt användarkonto och lösenord kräver systemet till exempel att du anger en engångskod som du får som sms eller via en app i telefonen.

Funktionen kallas också MultiFactor Authentication (MFA).

Bank-id är ett annat exempel på flerfaktorsinloggning som ger väldigt hög säkerhet.

Återställning av lösenord

Nu finns en e-tjänst som gör det möjligt att återställa ett glömt lösenord till kommunens inloggning och e-post. E-tjänsten kan också användas ifall man även glömt sitt användarnamn.

Du behöver Bank-id eller Freja-id för att använda e-tjänsten.

Från din telefon eller en dator med internetåtkomst, surfa till https://alvsbyn.enamnd.se/oversikt/overview/3306

Du hittar även länk till e-tjänsten på kommunens hemsida, under Personalsidan, Felanmälan och support.

Följ instruktionerna i e-tjänsten.

Informationshantering, lagring av data

I nuläget kan data lagras på olika ställen, i verksamhetssystem, som filer på kommunens servrar, i Microsofts365 miljö eller i form av bifogade filer i e-post. Dessutom finns lagringsytor dels i olika Teams och dess kanaler, som är specifika för varje verksamhetsområde, dels den uppsjö av övriga verktyg som ingår i Microsoft365 plattformen, till exempel Planner, ToDo, OneNote med flera.

Spara ALDRIG data på datorns skrivbord eller lokala hårddisk. Den informationen säkerhetskopieras inte och försvinner om datorn går sönder eller ominstalleras.

I bilaga Lagring av dokument finns en beskrivning av var lagring av olika dokumenttyper ska ske.

Filstruktur i den egna servermiljön.

G:\ - Här försvaras organisatoriskt gemensamma dokument och övrig information

H:\ - Här förvaras dina personliga dokument och övrigt arbetsmaterial

I:\ - Här förvaras sådan information som mindre grupper/projektgrupper arbetar med.

K:\ - Här förvaras avdelnings/arbetslags dokument och övrig information

Varje användare har dessutom tillgång till en molnbaserad lagringsyta i Microsoft365 miljön, som kallas OneDrive.

Filstrukturen i den egna servermiljön kommer att ersättas med lagring i Microsoft365 miljön. Fram till dess används ovanstående filstruktur i första hand.

Generellt ska all information som klassas som sekretess eller innehåller personinformation, och som omfattas av GDPR lagstiftningen, **endast** lagras i verksamhetssystem.

I särskilda fall kan viss sådan information lagras i ovanstående filsystem eller i Microsoft365 miljön. Beslut om så kan ske, fattas och dokumenteras av verksamhetsområdes chef i samråd med IT-avdelningen och Dataskyddsombud eller den del i organisationen som har övergripande ansvar för kommunens informationshantering. En Risk och Konsekvensanalys ska upprättas. Verksamhetsområdeschef ansvarar för att berörda medarbetare har tillräcklig utbildning för ändamålet.

Val av lagringsyta – filer utan personuppgifter

Personlig information, arbetsmaterial osv lagras på den egna OneDrive. OneDrive är åtkomlig från Utforskaren, Teams och Microsoft365 webportal. Även ToDo och OneNote är avsedda för personligt bruk och finns som appar att ladda ner på dator och telefon, kontakta IT-avdelningen för mer information.

Information som behöver delas med medarbetare och/eller extern personal lagras med fördel i en Teams kanal. Kontrollera att endast berörda användare har behörighet till Team'et.

I ett Team kan man lägga till ytterligare flikar med Planner, OneNote med flera och kan då användas för att dela information med flera användare. Information i din egen OneNote syns inte för Team-medlemmar.

Arbetstelefon

Se Policy för mobilabonnemang/telefoni, mobilsurf samt mobilt bredband för Älvsbyns kommun och dess bolag för riktlinjer gällande mobiltelefoner.

Utöver det som anges i policy gäller även följande instruktioner:

En personlig telefon, dvs den delas inte mellan olika användare på samma avdelning, ska alltid hållas säkerhetsuppdaterad.

Den ska ha ett säkert lösenord/PIN-kod, fingeravtryck eller ansiktsigenkänning för att kunna öppnas.

En personlig telefon kan användas för flerfaktorsinloggning, MFA.

En delad telefon, får INTE användas för flerfaktorsinloggning.

Privat telefon i tjänsten

Samma regler som för arbetstelefonen gäller, med undantag för att man bör undvika att använda den för sms/app-baserad flerfaktorsinloggning.

Använd Bank-id på din privata telefon som inloggningsmetod!

Användande av kommunens IT-utrustning

Hantera all IT-utrustning med varsamhet. Rapportera skada, oavsett hur den tillkommit till närmsta chef, arbetsledare eller lärare först och sedan kontaktas IT-avdelningen.

Om skadan orsakats av oaktsamhet, sabotage eller vandalism debiteras verksamheten eller den enskilde.

Telefoner och bärbara datorer får endast använda säkra internetanslutningar utanför den egna arbetsplatsen. Använd aldrig öppna WiFi-nät.

Lämna aldrig IT-utrustning olåst när du inte har den under uppsikt.

E-post och kommunikation

Älvsbyns kommun använder Outlook klienten i Microsoft365 plattformen för e-post och kalender.

Var misstänksam på all mejl som kommer utifrån. Kommunens mejlfilter tar bort de mesta skräp och bedrägerimejl men inte alla!

Om du är det minsta osäker, på om ett mejl eller en länk är tillförlitligt, kontakta IT-avdelningen.

Alla mejl som skickas utanför vår organisation får en varningstext högst upp, meningen med detta är att påvisa att det kan vara skadliga länkar och fejkad mejladress.

Mejladresser som är publika kan bli fejkade oftare, till exempel någon i den egna organisationen som mejlar sina medarbetare. Då kan bedragarna komma att fejka en adress som liknar denna och skicka ut farliga länkar till alla medarbetarna, det är då större chans att fler klickar på länken och anger information.

Får du mejl från en okänd avsändare, hovra med muspekaren över avsändaren, då visas den verkliga avsändar-adressen, kontrollera att den verkar riktig INNAN du öppnar mejlet.

Kontrollera länkar i mejlet, att de är riktiga, INNAN du klickar på dem. Bedragare använder sig ofta av sidor med snarlika adresser som ser riktiga ut, men leder till falska sidor.

Tips: Banker, försäkringsbolag eller myndigheter kommer aldrig att efterfråga inloggningsuppgifter. Du kommer heller aldrig att vinna på ett lotteri där du inte köpt en lott först!

Om du uppmanas att klicka på en länk, skicka ett mejl eller ringa ett telefonnummer till en bank, till exempel ”för att du har blivit utsatt för ett bedrägeri” - Skriv i stället in bankens webbadress själv i ett nytt webbfönster och kontakta banken den vägen, där hittar du både riktiga e-postadresser och telefonnummer.

Användning av Internet och programvaror

Kommunens utrustning får bara användas för arbetsrelaterade ändamål.

De programvaror som behövs i arbetet installeras och underhålls av IT-avdelningen.

Klicka inte på okända länkar, reklam eller annonser på NÅGON hemsida.

Kontrollera även att hemsidan är säker, adressen börjar med https:// eller visar en symbol av ett hänglås.

Se även avsnittet om användning Bank-id.

Att tänka på vid resor

Lämna aldrig din utrustning utan uppsikt.

Om du använder din laptop i offentliga miljöer – se upp med Visual hackning – det vill säga risken att någon ser vad du skriver på skärmen och ser vilka tangenter du trycker på, vilket är en av anledningarna till att enkla lösenord som till exempel 123456 inte är tillåtet. Vid behov kan sekretessfilter användas på din skärm. En produkt utöver grundutbudet, som kan beställs av verksamhetsansvarig eller motsvarande som även står för den extra kostnaden.

Använd aldrig öppna WiFi nät. Även anslutning till lösenordskyddade nätverk, exempelvis på hotell, kan medföra stora risker. Var kritiskt inställd till frågor som ställs i samband med anslutning till nätverket.

Avaktivera tjänster som du inte behöver under resan (det kan exempelvis handla om positionstjänster och Bluetooth).

Använd i stället din telefons mobilsurf för att koppla upp telefonen och datorn.

Använd ALDRIG USB-minnen som inte tillhandahållits av IT-avdelningen.

Använd egen laddare och kabel (använd inte USB uttag). På vissa hotell kan laddare och kabel finnas utplacerade i rummen, ibland riggade för att plantera skadlig kod i de enheter som ansluts.

Om du har behov av åtkomst till kommunens verksamhetssystem på resan kan du behöva ansluta via en VPN-tunnel. Det skapar en säker, krypterad, förbindelse mellan din dator och kommunens system. Kontakta IT-avdelningen för hjälp.

Om du ska resa utanför EU och behöver ha åtkomst till kommunens verksamhetssystemunder resan, kontakta IT-avdelningen innan avresa.

Kommunen tillämpar så kallad geo-blocking, det vill säga att man kontrollerar om utrustningen är ansluten till nätverk utanför ett bestämt geografiskt område.

Att använda Bank-id

Använd aldrig ditt Bank-id på uppmaning av någon annan, vi e-post, telefon eller hemsida.

Ta för vana att alltid starta ditt Bank-id innan du startar inloggningen på en hemsida! Kontrollera att det inte ligger något och inväntar ditt lösenord eller fingeravtryck, kontrollera också att det är rätt uppgifter som visas i Bank-id appen när du knappat in ditt personnummer eller skannat en QR-kod i samband med inloggning.

Att ansluta till trådlösa nät i kommunen

När du är på jobbet så använder du dig av följande:

Administrativ personal: AN-ADM, AN-ADM2 eller AN-ADM3

Politiker: Alvsbyn guest i kommunhuset

Elevdatorer: AN-EDU, AN-EDU2

Elevtelefoner, Elev-ipads och övriga enheter: ALV-Knut eller Alvakra

Larmtelefoner och övriga SOC enheter: ALV-Sabo

Förhållningssätt till sociala medier

Använder ni sociala medier i ert arbete är det viktigt att man klargör ansvar, regler och följer gällande regler för kommunens användande av sociala medier.

Se kommunens Riktlinjer för sociala medier för mera information.

Artificiell Intelligens / Maskin inlärning

AI eller maskininlärning är ett område som utvecklas snabbt. Även om möjlighet finns att själv ladda upp eller förse AI-systemet med kommunens information och nyttja olika AI modeller får inte detta ske okontrollerat. I dagsläget saknas kontroll över informationens spridning och tillgänglighet.

I de fall verksamheten har behov av att ladda upp information till ett AI-system ska beslut om detta fattas och dokumenteras av verksamhetsområdes chef i samråd med IT-avdelningen och Dataskyddsombud eller den del i organisationen som har övergripande ansvar för kommunens informationshantering.
Verksamhetsområdeschef ansvarar för att berörda medarbetare har tillräcklig utbildning för ändamålet.

Att spela in sammanträden och låta AI sammanfatta minnesanteckningar innebär att informationen laddas upp till ett AI-system och lagras därmed utanför kommunens kontroll.

AI får i nuläget användas med enbart kommersiellt tillgängligt underlag i test och experimentellt syfte, som komplement till ordinarie sökmotorer.

Separat information inom AI användning kommer att tas fram löpande eftersom utvecklingen går oerhört snabbt inom detta område.

Rapportering av IT-incidenter

Om du misstänker att något hänt i din telefon, dator eller verksamhetssystem kontakta IT-avdelningen omedelbart, via telefon i första hand, felanmäl via e-tjänsten i andra hand och stäng om möjligt av utrustningen.

Bilaga - Lagring av dokument

Lagringsplats	Förklaring	Dokument klasser			
		Arbetsmtrl	Öppen	Intern	Konfidentiell
Verksamhets-system	IT-System för lagring och behandling av information som rör en specifik verksamhet, behörighet bestäms av verksamhetsansvarig. Åtkomlig från arbetsplats eller externt via VPN-tunnel och MFA inloggning.	✗	✓	✓	✓
OneDrive	Din personliga lagringsyta. Åtkomlig från dator, telefon och webbtjänst på internet. Innehållet kan delas med kollegor.	✓	✓	✓	✗
(H:)	Din personliga lagringsyta. Åtkomlig från arbetsplats eller externt via VPN-tunnel och MFA inloggning.	✓	✓	✓	✗
Teams, Sharepoint	Delade lagringsytor i Microsoft365. Dokument och filer delas med kollegor på avdelnings, verksamhets eller organisationsnivå. Åtkomligt från dator, telefon och webbtjänst	✓	✓	✓	✓
OutLook	E-post, kalender, kontakter i Micosoft365. Åtkomligt från dator, telefon och webbtjänst	✓	✓	✓	✗
Övriga M365 appar	I huvudsak egna planerings och administrativa funktioner. Åtkomligt från dator, telefon och webbtjänst. I nuläget gäller endast Microsofts egen säkerhetskopiering, 30 dagar.	✓	✓	✓	✗
Delade mappar (G:,I:,K:)	Delade lagringsytor i kommunens egen filserver. Dokument och filer delas med kollegor på avdelnings, verksamhets eller organisationsnivå. Åtkomligt från arbetsplats eller externt via VPN-tunnel och MFA inloggning.	✓	✓	✓	✓
Alvsbyn.se inkl. personalsidan	Dokument och filer som är offentliga, samt personal sidor utan personuppgifter. Åtkomliga från dator, telefon och webbtjänst	✓	✓	✓	✗
Google drive, DropBox m.fl.	Lagringstjänst, både gratis och betalvariant. Används inte i kommunen.	✗	✗	✗	✗
Gmial, hotmail m.fl.	E-post system. Används inte i kommunen	✗	✗	✗	✗

Förklaringar

Förklaring	Symbol
Ok att använda lagringsytan	✓
Använd inte lagringsytan, undantag kan görs efter noggrann risk och konsekvensanalys	✓
Lagringsytan får ej användas	✗

Arbetsmaterial

Material som är pågående arbete, eller uppdateras löpande. Ej föremål för utlämnande av allmän handling.

Öppen

Allmänna handlingar, innehåller ej personuppgifter.

Internt bruk

Handlingar som kan bli föremål för sekretessprövning i samband med begäran om utlämnande av allmän handling. Kan innehålla icke känsliga personuppgifter.

Konfidentiell

Sekretessbelagd information eller känsliga personuppgifter.

Beakta gällande lagstiftning, GDPR, OSL, PDL, CSL.

OBS: Gäller det säkerhetsskyddsklassad information gäller särskilda regler. Kontakta informationssäkerhetsansvarig.

Bilaga – Ordlista och förklaringar

CSL – Cyber Säkerhets Lag. Dvs svensk lagstiftning för införande av EU's NIS-2 direktiv.

GDPR – General Data Protection Regulation. Regelverk som ska skydda personers integritet. Exempel på personuppgifter som omfattas av GDPR:

Personnummer, med eller utan de fyra sista siffrorna

Etniskt ursprung

Politiska åsikter

Religiös eller filosofisk övertygelse

Medlemskap i en fackförening

Hälsa

En persons sexualliv eller sexuella läggning

Genetiska uppgifter

Biometriska uppgifter som används för att entydigt identifiera en person.

MFA – Multifactor Authentication, eller flerfaktorsinloggning, det krävs mer än bara ett användarkonto och lösenord för att inloggning ska vara möjlig. Kan vara ett SMS till telefonen, en särskild app, Bank-Id med flera.

NIS, NIS2 – Network and Information Systems Security Directive

OSL – Offentlighets och sekretesslag (2009:400)

PDL – Patientdatalag (2008:355)

VPN – Virtual Private Network, innebär att man med hjälp speciell programvara på datorn kan skapa en krypterad tunnel mellan dator och verksamhetssystem