Informationssäkerhet

Stödanvisning
identitet och åtkomst

Östhammars kommun

Målgrupp	Chefer och systemförvaltare, alla kontor och verksamheter
Avsändare	Kommunledningskontoret, Digitalisering och projektledning
Dokumentansvarig	Informationssäkerhetssamordnare
Framtagen	2024-12-19
Aktualitetsprövad	2026-03-05

ÖSTHAMMARS KOMMUN
– EN DEL AV ROSLAGEN

Innehåll

Innehåll

Innehållet utgår från kommunens program och vägledning för informationssäkerhet och ger en fördjupad beskrivning över identitet och åtkomst. Stödanvisningen ska tillämpas för all hantering av identiteter och åtkomst till information men även till funktioner, tjänster och it-system. Detta inbegriper också uppkopplade ”saker”, databaser, operativsystem, styrsystem och nätverk.

Mål och syfte

Målet är en ensad process för styrning av identitet och åtkomst så att endast de personer som behöver informationen för att kunna utföra sina arbetsuppgifter ges tillgång till den. Processen inkluderar också styrning av identitet och åtkomst så att tjänster, uppkopplade ”saker” t.ex. robotar eller apparater och även Artificiell Intelligens (AI) ges tillgång till den information och de funktioner de behöver på ett lämpligt sätt.
Syftet är att svara mot externa krav, interna behov och bidra till att skydda informationen i kommunens verksamheter.

Identitet och åtkomst

Generellt

Huvudprincipen för hur identitet och åtkomst ska tilldelas utgår från att användare ska ha den lägsta möjliga åtkomst som krävs för att arbetet ska kunna utföras på ett lämpligt och riktigt sätt. Informationsklassningen sätter ramarna för hur åtkomst ska tilldelas och hanteras för olika nivåer av skyddsvärd information och funktioner. Informationsägaren är ytterst ansvarig för att godkänna tilldelning och att avbeställa åtkomst till information och regelbundet följa upp användares åtkomsträttigheter. Ju högre rättigheter en användare har eller ju mer känslig information som hanteras, desto oftare ska uppföljning ske. Särskild uppmärksamhet ska ägnas åt höga behörigheter och då användare slutar eller byter tjänst. Systemförvaltare har ansvar för att ta bort och ändra behörigheter enligt informationsägarens anvisningar.

Komponenterna som styr åtkomst

En ***användares identitet*** och ***autentisering*** är tillsammans en grundläggande kontroll av att användaren är just den som den utger sig för att vara. Kontrollen ska utföras oavsett om användaren är en person eller en tjänst/”sak” (t.ex. en robot) som behöver åtkomst till information och tjänster. Hur man kontrollerar en tjänst eller ”sak” beror på användningsområdet, men kan t.ex. innebära verifiering av certifikat, användning av API-nycklar samt granskning av leverantörens svar mot informationssäkerhetskrav (här kan ni ta hjälp av systemförvaltarteamet).
Denna kontroll av en användares identitet lägger grunden för kommunens förmåga att förhindra obehörig åtkomst och i övrigt möta de krav som ställs på informationssäkerhet i flera lagar och andra externa och interna krav. Kontrollen är på flera sätt en avgörande förutsättning för all digitalisering i kommunens verksamheter. Denna kontroll av identitet är

också en förutsättning för att organisationen ska kunna förlita sig på loggar i exempelvis utredning och felsökning.

Efter att användarens identitet är kontrollerad ska en ***behörighetsstruktur*** styra vilken information som användaren får tillgång till.
Åtkomst ges när samtliga tre komponenter har erhållits på ett korrekt sätt.

Användares identitet

Exempel på en användares identitet är användarnamn, vilket ska vara unikt och knutet till en individ, en tjänst eller en sak. Varje informationsägare ansvarar för att en identitets- och behörighetsadministration finns i systemet/tjänsten för att kunna kontrollera och styra hur identiteter skapas och hanteras. Varje informationsägare ska också tillse att en rutin följs för tilldelning respektive borttagning av användaridentiteter och behörigheter i systemet/tjänsten, så att detta sker på ett kontrollerat, säkert och spårbart sätt.
Användarkonto i kommunens Active Directory (AD) genereras via anställningen i Personec.

Autentisering – kontroll av uppgiven identitet

Både lagstiftning och kommunens informationsklassningsmodell (nivå 1-3) styr vilken bevisstyrka som krävs vid olika sammanhang och för olika typer av information. Exempel på bevis är körkort eller pass.
Stark autentisering - För nivå 3 i konfidentialitet vid informationsklassningen gäller att stark autentisering ska användas. Verksamheten ska kontrollera användarens identitet med godkänd legitimation innan åtkomst lämnas ut till användaren. Användaren ska sedan använda minst två faktorer (multifaktorsautentisering) för att få åtkomst till informationen, t.ex. tjänstekort, smartkort och en pinkod. För hantering av patientuppgifter ställer patientdatalagen krav på stark autentisering.
Multifaktorsautentisering - För nivå 2 i konfidentialitet gäller att multifaktorskontroll kan tillämpas. Men vissa lägre krav ställs på att kontrollera användarens identitet, det kan räcka att en ansvarig chef går i god för användarens identitet.
Användarnamn och lösenord - För nivå 1 i konfidentialitet gäller att användarnamn och lösenord får användas.
För nivå 0 i konfidentialitet är informationen öppen och tillgänglig för alla inom eller utanför kommunen. Därför ***ställs inga krav på identitet eller autentisering*** för dem som vill ha tillgång till informationen.

Klassningsnivå gällande konfidentialitet	Krav på autentisering
3	Stark autentisering och multifaktorsinloggning
2	Multifaktorsinloggning
1	Användarnamn och lösenord
0	Inga krav

Tabellen sammanfattar kraven per klassningsnivå

Behörighetsstruktur

En behörighetsstruktur är i grunden ett regelverk som ska styra vad en användare kan se och göra i ett system/tjänst, t.ex. baserat på deras roll i verksamheten.
En viktig princip för en behörighetsstruktur är att endast de användare som behöver tillgång till informationen för att kunna utföra sina arbetsuppgifter ska ges tillgång till den.

När informationen innehåller personuppgifter kräver GDPR särskilda regler för åtkomst för att skydda individers integritet. Dokumentationen om behörighetsstrukturen ska visa hur hänsyn tagits till känsliga och skyddade personuppgifter genom en riskanalys. Det kan exempelvis framgå om användare kan se skyddade personuppgifter eller om systemet har funktioner för att anonymisera dem
Principen för en behörighetstruktur är också viktig sett ur offentlighets- och sekretesslagen då den kräver att sekretess upprätthålls mellan självständiga verksamhetsgrenar inom samma organisation. Inom en verksamhetsgren gäller inre sekretess, vilket innebär att endast de som behöver uppgifterna för sitt arbete får tillgång till dem. Därför måste sekretessregler beaktas vid utformningen av behörigheter i IT-system, så att uppgifterna får rätt skydd.

För verksamhetssystem ansvarar informationsägaren för och beslutar om vilken behörighetsstruktur som ska gälla utifrån verksamhetens behov och roller. Beslutet ska ske i samråd med systemförvaltaren som ansvarar för att översätta kraven till den behörighetsstruktur som ska gälla för system/tjänster utifrån det systemtekniska perspektivet. För gemensam teknisk infrastruktur, exempelvis nätverk, operativsystem eller tekniska plattformar, ansvarar IT-centrum för vilka behörighetsstrukturer som ska gälla för att administrera tjänsterna.

Tilldelning av behörigheter

När behörighetsstrukturen är bestämd ska tilldelning av behörigheter följa det beslutade regelverket.

Informationsägaren beslutar därefter om vilken behörighet som är lämplig att tilldela till just sina användare. Beslutet ska baseras på vad användarna har för anställning, organisationstillhörighet och arbetsuppgifter.

Varje systemförvaltare beslutar på motsvarande sätt vilken behörighet som är lämplig att tilldela för de användare som behöver administrera tjänsterna.

Varje informationsägare och systemförvaltare ska tillse att en rutin följs för tilldelning, ändring, borttagning och uppföljning av användarnas behörigheter så att detta sker på ett kontrollerat, säkert och spårbart sätt.

Systemförvaltare ska ha kontroll över alla utdelade användaridentiteter och behörigheter kopplat till det system/tjänst som personen ansvarar för.

Användare ska utbildas om de villkor som gäller för den åtkomst de fått sig tilldelad. Systemförvaltaren för systemet/tjänsten ansvarar för att användarna utbildas om de generella villkor som gäller och följer av behörigheten som användaren tilldelats till systemet/tjänsten.

Om obehörig åtkomst ändå sker

Om en användare tar del av information som denne inte har rätt att ta del av innebär det att en obehörig åtkomst har skett. Vid händelse av obehörig åtkomst ska kommunens incidentrutin, *Stödanvisning för incident – och kontinuitetshantering*, vägleda verksamheten i vilka åtgärder som ska vidtas. Obehörig åtkomst kan även innebära att en personuppgiftsincident föreligger. En sådan incident kan behöva anmälas till extern myndighet.

Särskilt om skyddade personuppgifter

Personuppgifter kan efter beslut av Skatteverket vara skyddade. Det är av stor betydelse att skyddade personuppgifter hanteras på säkert sätt så att uppgifterna inte blir åtkomliga för någon utöver de som måste ha åtkomst till dem för att nödvändiga uppgifter ska kunna utföras. Både medarbetare och kunder (t.ex. elever, brukare) kan ha skyddade personuppgifter och kan förekomma i IT-system eller på papper.

Det är den enskilde individen som meddelar att hen har skyddade personuppgifter. När detta skett ska det finnas en rutin inom kommunen så att rätt åtgärder kan vidtas.

Det är angeläget att kommunens verksamheter hanterar skyddade personuppgifter på ett enhetligt och säkert sätt. Varje kontor måste därför göra en noggrann genomgång av sin verksamhet och upprätta anvisningar för hanteringen av skyddade personuppgifter inom den egna verksamheten om så krävs.