UTFÄRDARE ROLF SANNEBJÖRK			DOKUMENTTYP Riktlinje	
BESLUTAD AV KOMMUNSTYRELSEN	DIARE NR KS 2020/466	DATUM 2021-01-25	VERSION 1.0	DOKUMENTIDENTIFIKATION

Övergripande riktlinjer för behörigheter i Haparanda stads IT system

För att tilldelas konto och behörigheter i system krävs en anställning eller ett uppdrag för Haparanda Stad. Behörigheter tilldelas endast personer som har behov av informationen i sitt arbete samt har erforderliga kunskaper.

Användaridentitet
Användarna i som tilldelas konto och behörigheter ska ha en unik användaridentitet. Samma användarnamn ska så långt det är möjligt användas i samtliga system. Exempel på användarnamn:

{Förnamn 3 bokstäver}{Efternamn 3 bokstäver}{Löpnummer 2 siffror} Exempel: Stina Persson - STIPER01

Mer information om utformningen av användarnamn finns i dokumentet Migreringsprojekt Active Directory – Namnstandarddokument kapitel 2.

Lösenord
Lösenordet i katalogtjänsten ska vara 8 tecken långt och innehålla minst en stor och liten bokstav, en siffra samt ett specialtecken och ska bytas ut var tredje månad. Lösenord som använts får inte återanvändas under en tolvmånadersperiod. Inloggning kan göras med användarnamn eller e-postadress beroende på system.

Behörighet
Styrning av grundläggande behörighet görs via den centrala katalogtjänsten Active Directory (AD). Den grundläggande behörigheten ger användaren möjligheten att logga in i nätverket samt en e-postadress. Behörighet till verksamhetssystem tilldelas av systemägaren eller av den utsedd person. Behörighet tilldelas i de fall användaren har behov av informationen för att kunna utföra sitt arbete. Nivå på behörighet tilldelas i samråd med närmaste chef.

Rutiner om behörighetstilldelning till verksamhetssystem tas fram av respektive systemägare.

Metadata för grundläggande behörig hämtas från personalsystemet till AD. Finns det en aktiv anställning eller ett uppdrag så tilldelas grundläggandebehörighet. Upphör anställningen eller uppdraget inaktiveras kontot och där med den grundläggande behörigheten. Samtliga system bör så långt det är möjligt integreras i lösningen för att säkerställa att kontona inaktiveras i samband med att anställningen/uppdraget upphör. Behörigheter för tillfälliga konsulter/uppdragstagare hanteras manuellt.

Avslut, tjänstledighet
För personer som avslutar sin anställning / uppdrag ska samtliga behörigheter tas bort och konton ska raderas där det är möjligt. Ansvarig är närmaste chef / uppdragsgivare som meddelar systemägarna om att anställningen / uppdraget upphört. Systemägarna ska göra årliga kontroller av behörigheter i systemen.

Vid tjänstledighet, föräldraledighet eller annan längre tids frånvaro ska kontot inaktiveras. Undantag från ovan kan göras om närmaste chef gjort bedömningen att det är viktigt för verksamheten att kontot är aktivt. Detta bör meddelas HR och IT i god tid före frånvaron.

Ökad säkerhet
För att ytterligare öka säkerheten bör ett införande av tvåfaktors autentisering med smarta kort eller motsvarande göras. Tvåfaktors autentiseringen stärker säkerheten då det inte räcker med enbart tillgång till användarnamn och lösenord för att komma åt systemen. Samt att det möjliggör införandet av en single sign-on lösning.