Sikkerhetsfunksjoner for 1-faktor autentisering i Evolution

(Sti: Innstillinger → Brukeradmin → Brukere → Avansert Sikkerhet)

FUNKSJON	BESKRIVELSE AV FUNKSJON	VALG
Passord forandring	Superbruker kan tvinge en Bruker til å endre passord ved å aktivere denne funksjonen. Bruker vil ved neste pålogging bli bedt om å endre passord. Funksjonen vil bli deaktivert når nytt passord er oppdatert	<**PÅ eller AV**>
Passord utløpsdato	Superbruker kan benytte den for f.eks for temporære brukere som skal bruke systemet for en begrenset periode – frem til og med den valgte utløpsdatoen. Brukeren vil få melding(er) når det er mindre enn 4 dager frem til utløpsdato. Det vil ikke være mulig å logge på etter denne datoen.	<**DATO**>
Passord – historie sjekk	Superbruker kan velge å aktivere denne for å unngå at brukere gjenbruker et passord for ofte. Det nye passordet kan da ikke være likt de siste 5 passordene som er benyttet**.**	<**PÅ eller AV**>
Sjekk feilede login forsøk	Hvis denne funksjonen aktiveres – så vil en brukerkonto deaktiveres etter 5 feil forsøk på å logge inn. Når bruker får korrekt logget på så vil telleren av forsøk bli nullstilt.	<**PÅ eller AV**>
Passord validering	Superbruker kan aktivere denne funksjonen for å sikre at brukerpassord blir sammensatt på en slik måte at de ikke lett kan relateres til brukeren (ektefelle, hund/katt og bil etc) og ikke lett kan knekkes av utenforstående. Passordet må bestå av 6 eller flere karakterer. Passordet må inneholde minst 1 stor bokstav, 1 liten bokstav og 1 tall. Passordet må være forskjellig fra brukernavnet.	<**PÅ eller AV**>
Siste loginn utløpsperiode (i dager)	Superbruker kan definere at en brukerID som ikke er benyttet av Bruker etter et valgt antall dager kan deaktiveres ved neste forsøk på innlogging. Bruker må da kontakte Superbruker for å få aktivert sin brukerkonto.	<**ANTALL DAGER**>