Konto och enheter VIOL 3

Versionsnummer 1.0

Senast uppdaterad: 2024-12-12

BIOMETRIA

Revisionshistorik

Revisionshistoria för Konton och enheter VIOL 3.

Vid ändring av revisionshistoria ska även version och datum på första sidan samt datum i sidhuvud uppdateras.

Version	Ändring	Datum	Signatur
1.0	Första officiella version	2024-12-12	AMAGRO

Innehållsförteckning

1 Biometria-konto

Följande kontotyper stöds för att skapa ett biometria-konto.

- Office365
- Personligt Microsoftkonto (outlook.com, hotmail.com och liknande)
- Personligt Googlekonto (gmail.com)

Har man inte ett mailkonto av ovanstående typ kan man använda en godtycklig e-postadress för att skapa ett Microsoft-aktiverat konto.
Ett Microsoft-aktiverat konto använder en befintliga e-postadress (till exempel Adam.Andersson@telia.com) och ett nytt lösenord som hanteras av Microsoft.

2 Byta lösenord

Lösenordet byter du på din egen (jobb)mail. Beroende på om det är ett Google- eller Microsoft-konton kan de se olika ut. Men det du gör är att gå in i app eller webb på din mail och begär nytt lösenord.

Återställa glömt lösenord till ett Microsoft-konto - Microsoft Support

Så här återställer du Google-kontot eller Gmail - Google-konto Hjälp

När lösenordet är bytt så kan du logga in i Biometrias system.

3 Tvåstegsverifiering

För att öka säkerheten har tvåstegsverifiering införts på Biometrias tjänster, kan också benämnas MFA, multifaktorautentisering. Tvåstegsverifiering hjälper till att skydda ditt användarkonto och den information som du har tillgång till.

Om kontotypen har stöd för sin egen tvåstegsverifiering och förmedlar det när användaren loggar in kommer Biometrias tjänster inte kräva ytterligare en tvåstegsverifiering.

För att undvika onödiga problem behöver du i förväg verifiera att du har tvåstegverifiering aktiverat genom att följa denna instruktion: kontrollera tvåstegsverifiering. Har du inte tvåstegsverifiering aktiverat kommer detta att göras i samband med verifieringen.

Biometria rekommenderar appen 'Microsoft Authenticator' för tvåstegsverifiering. Läs mer här: Använda Microsoft Authenticator

Hur du beställer dina behörigheter och rollpaket finns här: Behörigheter i VIOL 3

4 Rekommendationer för Chaufförens enhet

4.1 Transportör

Enhet: Surfplatta, liggande läge (landskap)
Webbläsare: Safari och Chrome (senaste 2 versionerna)
Upplösning: 1900x1200
Uppkoppling: 4g

5 Kontohantering i chaufförens enhet

Biometria använder MFA (Multifaktorautentisering) för användandet av tjänster i VIOL3. Det innebär att en användare måste logga in med användarnamn och lösenord samt autentisera sig via ytterligare ett steg, t ex Microsoft Authenticator.

Enheterna som användare använder för att ansluta till Biometrias tjänster tillhandahålls av de olika aktörerna själva. Biometria kommer alltså inte ansvara för rutiner och hantering av dessa.

I detta dokument beskriver Biometria vad vi lämnar för rekommendation kring hur användarnas enheter hanteras. Men det är upp till företagen själva att bestämma, supportera och hantera enheterna, konton, applikationer mm på dessa enheter.

För chaufförerna delar vi in rekommendationen i två delar:

1. Chaufförer som har en egen privat enhet
2. Chaufförer som delar enheter med flera olika användare

5.1 Chaufförer som har en egen privat enhet

När man har en privat enhet som man är enda brukaren av så har man endast ett användarkonto registrerat i enheten. Då finns det ingen risk för att privat information läcker till andra användare, eller att andra användare ”råkar” använda Biometrias tjänster som någon annan person redan inloggad på enheten. För MFA autentiseringen kan användaren installera Microsoft Authenticator för att bekräfta sin identitet.

5.2 Chaufförer som delar enhet med andra

Har man har en enhet som hör till bilen och chaufförerna växlar enhet med varandra beroende på vilken bil som de kör för dagen, är det viktigt att tänka på hur man hanterar sina identiteter i enheten.

Vi rekommenderar då att man skapar en användare var på enheten, vilket då gör att man håller isär konton på enheten. Då kan respektive användare själv hantera enheten med sina appar, länkar och konfiguration utan att information läcks mellan användarna.

För mer information om hur man sätter upp flera användaren på en androidenhet se:

Engelska:
Delete, switch, or add users - Android Help

Svenska:
Ta bort, byta eller lägga till användare - Android Hjälp

Följer man rekommendationen ovan kan varje användare hantera enheten på samma sätt som om man har en egen privat enhet.