



# Proximia Privacy & Biometric Data Security

Protecting Identities Without Compromising Privacy



Proximia eliminates passwords while ensuring that biometric and credential data remain private, encrypted, and under user control. Our platform is built on Zero Trust principles and designed to meet the scrutiny of security leaders.

## 1. Biometric Privacy

- **No raw storage**  
Proximia never stores images, fingerprints, or raw biometric identifiers.
- **Encrypted templates**  
Biometrics are converted into encrypted mathematical templates that cannot be reverse-engineered.
- **Local validation**  
Biometric checks happen on the user's device (phone or camera), not in a central database.
- **No sale or monetization**  
We never sell, lease, trade, or profit from your biometric information.

## 2. Encryption Architecture

- **Encryption everywhere**  
All authentication data is encrypted at rest, in transit, and in internal system calls (TLS, rotating keys).
- **Triple-layer model**  
Local encryption → API encryption → repository encryption, ensuring credentials and biometric templates are never exposed in clear text.
- **Distributed vault**  
Sensitive data is fragmented across multiple servers with rotating secrets, reducing attack surface and preventing static credential compromise.

### 3. Operational Safeguards

- **Separation of identity & credentials**  
Users never know or handle system-generated passwords, removing phishing and reuse risks.
- **Zero-knowledge posture**  
Even Proximia administrators cannot access or reconstruct biometric or credential data.
- **Compliance alignment**  
Biometric handling meets NIST liveness detection standards and supports regulatory requirements for public sector and enterprise.

### 4. Transparency & Disclosure

- **Public biometric policy**  
Our comprehensive Biometric Data Policy is publicly available at [trust.proximia.com](https://trust.proximia.com).
- **Purpose limitation**  
Biometric data is used solely for identity verification and authentication.



### Why CISOs Trust Proximia



Removes passwords and reduces identity attack vectors.



Protects privacy by design, no exploitable biometric repositories.



Delivers strong security controls without adding friction to users.



Provides transparent policies and user control over biometric data.

**Proximia ensures security without compromise—removing passwords, protecting identities, and preserving user privacy.**



[proximia.com](https://proximia.com) | [sales@proximia.com](mailto:sales@proximia.com)  
(844) GET-PROX or (844) 438-7769

