Welcome to Incode Workforce, your company's secure and simple way to verify your identity when accessing systems or contacting IT.

Incode helps ensure that only you, not someone pretending to be you, can gain access when it matters most. Our technology protects employees and organizations from identity-based attacks such as social engineering and deepfakes while keeping your experience fast and frictionless.

More about Incode

Incode is a global leader in identity verification and authentication. Our mission is to make trust simple by helping organizations verify real people with security and ease.

Headquartered in San Francisco with global operations, Incode provides AI-powered identity verification solutions across multiple industries—including financial services, healthcare, technology, and government—working with leading companies such as Citibank, Airbnb, Amazon, and T-Mobile.

Your information and how it's protected

As part of your company's identity verification process with Incode, you will be asked to take a selfie and upload your government-issued ID.

We understand that your personal information is sensitive. Here's what happens to it and how we keep it safe.

©2025 Incode Technologies, Inc. All rights reserved.

What happens to your data

What data is collected	What data is retained	What data is deleted and when
Selfie Used for onboarding and verification.	**Basic account details** Name, work email, and employee ID from your company's IAM system (like Okta or Microsoft Entra).	**Original ID images and selfies** Deleted immediately after verification is complete.
Government-issued ID Driver's license, passport, or similar document.	**Key ID information** Limited data from your ID such as name and date of birth, used to confirm who you are.	**Temporary system data** Purged automatically once the verification session ends.
Employee details Provided by your company to confirm your identity.	**Expiration date from your ID** Used to remind your company when it's time to reverify your identity.	**Non-essential data** Deleted automatically after the default retention period (45 days, unless adjusted by your company). Data may also be deleted immediately upon request.
	Onboarding selfie Securely stored as an encrypted copy to maintain accuracy and ensure continuity when technology is updated.	
	Face template A secure, encrypted mathematical representation of your face, used only for authentication. It cannot be reverse engineered to the original image.	

Why we retain limited data

We keep only what is needed to:

- Allow you to authenticate quickly without re-verifying each time
- Help your company meet compliance and fraud-prevention standards
- Ensure consistent performance and reduce verification errors

How your data is protected

Your information is encrypted and stored in secure, access-controlled environments. Incode follows and exceeds industry standards for data security and privacy, including:

- Encryption at rest and in transit
- Strict access controls for authorized personnel only
- Regular security audits and compliance with privacy regulations

Your personal data is never shared, sold, or used for marketing purposes. It is used only to verify your identity and maintain secure access to your company's systems.

How long your data is retained

Your company determines how long we retain your information based on its security and compliance needs. The default period is 45 days, but your company may adjust this. Immediate deletion is also supported upon request. After that, all non-essential data is automatically deleted.

Questions

If you would like to know more about how your data is handled, you can reach out to your company's HR or IT administrator, or visit Incode's Privacy Policy for full details.

©2025 Incode Technologies, Inc. All rights reserved.