Security as a Company Value

Iterative Inc.'s security & compliance principles guide how we deliver our products and services, enabling people to simply and securely access the digital world.

Secure Personnel

Iterative Inc. takes the security of its data and that of its clients and customers seriously and ensures that only vetted personnel are given access to their resources.

- All Iterative Inc. contractors and employees undergo background checks prior to being engaged or employed by us in accordance with local laws and industry best practices.
- Confidentiality or other types of Non-Disclosure Agreements (NDAs) are signed by all employees, contractors, and others who have a need to access sensitive or internal information.
- We embed the culture of security into our business by conducting employee security training & testing using current and emerging techniques and attack vectors.
-

Secure Development

- All development projects at Iterative Inc., including on-premises software products, support services, and our own Digital Identity Cloud offerings follow secure development lifecycle principles.
- All development of new products, tools, and services, and major changes to existing ones, undergo a design review to ensure security requirements are incorporated into proposed development.
- All team members that are regularly involved in any system development undergo annual secure development training in coding or scripting languages that they work with as well as any other relevant training.
- Software development is conducted in line with OWASP Top 10 recommendations for web application security.

Secure Testing

Iterative Inc. deploys third party penetration testing and vulnerability scanning of all production and Internet facing systems on a regular basis.

- All new systems and services are scanned prior to being deployed to production.
- We perform penetration testing both by internal security engineers and external penetration testing companies on new systems and products or major changes to existing systems, services,

and products to ensure a comprehensive and real-world view of our products & environment from multiple perspectives.

- We perform static and dynamic software application security testing of all code, including open source libraries, as part of our software development process.

Cloud Security

Iterative Inc. Cloud provides maximum security with complete customer isolation in a modern, multi-tenant cloud architecture.

Iterative Inc. Cloud leverages the native physical and network security features of the cloud service, and relies on the providers to maintain the infrastructure, services, and physical access policies and procedures.

- All customer cloud environments and data are isolated using Iterative Inc.'s patented isolation approach. Each customer environment is stored within a dedicated trust zone to prevent any accidental or malicious co-mingling.
- All data is also encrypted at rest and in transmission to prevent any unauthorized access and prevent data breaches. Our entire platform is also continuously monitored by dedicated, highly trained Iterative Inc. experts.
- We separate each customer's data and our own, utilizing unique encryption keys to ensure data is protected and isolated.
- Client's data protection complies with SOC 2 standards to encrypt data in transit and at rest, ensuring customer and company data and sensitive information is protected at all times.
- We implement role-based access controls and the principles of least privileged access, and review revoke access as needed.

Compliance

Iterative Inc. is committed to providing secure products and services to safely and easily manage billions of digital identities across the globe. Our external certifications provide independent assurance of Iterative Inc.'s dedication to protecting our customers by regularly assessing and validating the protections and effective security practices Iterative Inc. has in place.

SOC 2 Type 2

Iterative Inc. successfully completed the AICPA Service Organization Control (SOC) 2 Type II audit. The audit confirms that Iterative Inc.'s information security practices, policies, procedures, and operations meet the SOC 2 standards for security.

Iterative Inc. was audited by Prescient Assurance , a leader in security and compliance certifications for B2B, SAAS companies worldwide. Prescient Assurance is a registered public accounting in the US and Canada and provide risk management and assurance services which includes but not limited to SOC 2, PCI, ISO, NIST, GDPR, CCPA, HIPAA, CSA STAR etc. For more information about Prescient Assurance, you may reach out them at info@prescientassurance.com

An unqualified opinion on a SOC 2 Type II audit report demonstrates to the Iterative Inc.'s current and future customers that they manage their data with the highest standard of security and compliance.

Customers and prospects can request access to the audit report **here** (add a link to a form to fill out by your partners and customers to request SOC 2 report and accept NDA terms).