Security at Autograph

Table of Contents

1. Introduction: Security at Autograph

At Autograph, security and transparency have been central pillars since day one. Our platform unifies data and workflows across HR, finance, legal, and compliance systems while maintaining stringent data security standards. Through robust security practices and third-party audits, Autograph ensures that your data is handled with care.

We prioritize the security of our customers' information by adopting industry-leading technologies and continuously enhancing our security posture through audits and risk management.

2. Security Principles

Autograph's approach to security is governed by the following key principles:

- **Least Privilege**: Users and systems are granted the minimum level of access necessary to perform their roles.
- **Defense in Depth**: Multiple layers of security mechanisms ensure that if one control is compromised, additional layers mitigate potential risks.
- **Continuous Monitoring**: We implement automated systems that provide real-time monitoring and alerting to unauthorized access or anomalies.
- **Risk-Based Security**: Regular risk assessments ensure that our security practices adapt to evolving threats.
- **Separation of Duties**: Critical tasks are divided among personnel to prevent excessive authority in any one person or system.

3. Compliance and Certifications

Autograph is committed to maintaining industry-leading certifications and compliance with global data protection laws. Our platform complies with:

- **SOC 2 Type 1**: Validated by an independent auditor as of March 2024, ensuring that our controls meet security and privacy requirements.
- **SOC 2 Type 2**: Our Type 2 certification is currently in the observation period, which will be completed by the end of 2024. In the meantime, we are happy to furnish an in-progress letter from our compliance platform if asked.
- **GDPR and CCPA Compliance**: Our practices align with the stringent requirements of the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

4. People Security

At Autograph, we believe that people are a critical line of defense in maintaining a secure environment. We prioritize robust security practices through comprehensive screening, access control, and ongoing training to ensure all personnel understand their responsibilities in protecting sensitive data.

Background Checks and Confidentiality Agreements

All Autograph employees, contractors, and vendors undergo criminal background checks before being granted access to any systems or sensitive information.

Before beginning work, all employees are required to sign confidentiality agreements that strictly prohibit unauthorized disclosure of sensitive company data. Access to critical systems and data is not granted until the employee has signed and acknowledged these agreements.

Security Awareness Training

Autograph invests heavily in security education for all employees. Every new hire must complete security awareness training within 30 days of joining the company. This training is designed to cover:

- The importance of data security and privacy.
- Key risks and vulnerabilities in the technology landscape.
- Autograph's internal security policies and best practices.

Training is not a one-time event. Employees are required to complete annual security refresher courses to stay informed of evolving threats, emerging security technologies, and any updates to company security policies.

Access Control and Regular Reviews

Access to Autograph's systems is granted based on the principle of **Least Privilege**, meaning employees are provided with only the minimum access required to perform their job functions. All access rights are regularly reviewed:

- **Semi-Annual Access Audits:** All user access to critical systems is reviewed at least semi-annually by system administrators to ensure permissions are appropriate and aligned with current job responsibilities.

- **Role-Based Access Controls (RBAC):** Access to sensitive data is granted based on job function. Elevated privileges, such as administrator access, are restricted and reviewed carefully.
- **Deprovisioning:** When an employee leaves the company or changes roles, access to all systems is revoked or adjusted within 24 hours.

Vendor and Contractor Assessments

Autograph takes a risk-based approach to managing its vendors and contractors. Each third-party service provider undergoes an initial assessment to ensure they meet our stringent security requirements. Regular evaluations are conducted to ensure continuous compliance with our standards.

5. Product Security

Autograph's product development follows a secure development lifecycle, where security is considered from the design phase through deployment.

- **Change Management**: All changes to the platform are reviewed, tested, and approved through a formal process. This ensures that no unauthorized changes are made to production environments.
- **Penetration Testing**: We engage independent security firms to conduct annual penetration tests on our platform, and any identified vulnerabilities are promptly addressed.
- **Vulnerability Scans:** Auto Graph performs internal and/or external vulnerability scans to test in-scope systems at least quarterly.
- **Encryption**: All data in transit and at rest is encrypted using industry-standard protocols (TLS 1.3 and AES-256).

6. Data Security

Data security is a foundational aspect of Autograph's overall security strategy. We implement a multi-layered approach to protect customer and internal data from unauthorized access, loss, or corruption, leveraging encryption, access controls, and robust data classification mechanisms.

Data Classification

Autograph categorizes data based on its sensitivity and criticality, ensuring that each type of data receives the appropriate level of protection. Data is classified into the following categories:

- **Sensitive Data:** This includes highly confidential information such as personal data protected under GDPR, financial information, and health-related data. Sensitive data requires the highest levels of encryption and access control.
- **Confidential Data:** Data that is not public but less critical than sensitive data. This includes internal company records, employee performance data, and some customer communications.
- **Public Data:** Data that is intended for public consumption, such as marketing materials and general company information. Public data does not require encryption.

This classification system allows Autograph to apply the appropriate security measures depending on the data type, ensuring that sensitive information is safeguarded while public data is more freely accessible.

Encryption

To protect data in all its forms, Autograph employs industry-standard encryption protocols:

- **Data at Rest:** All sensitive and confidential data stored within Autograph's systems is encrypted using AES-256 encryption, which is the highest commercially available encryption standard.
- **Data in Transit:** All data transferred between systems, whether within Autograph's internal infrastructure or between Autograph and external parties, is encrypted using TLS 1.3. This ensures that data cannot be intercepted or altered during transmission.
- **Encryption Key Management:** We use a secure key management system (KMS) to generate, store, and rotate encryption keys.

7. Infrastructure Security

Autograph's infrastructure is designed for security, resilience, and scalability. We leverage cloud-based infrastructure to provide a highly available and secure environment while implementing additional security controls to ensure the safety and integrity of customer data.

Cloud Infrastructure

Autograph's platform is hosted on Amazon Web Services (AWS), one of the most secure and compliant cloud providers available. AWS provides the foundational security features, such as physical security, network security, and redundancy, while Autograph implements additional security controls. Autograph also uses advanced monitoring and logging tools to detect and respond to potential threats.

Access Control and Network Security

Access to Autograph's cloud infrastructure is tightly controlled:

- **Multi-Factor Authentication (MFA):** Access to all critical systems requires MFA, ensuring that even if credentials are compromised, unauthorized users cannot gain access.
- **Firewall Rules and Network Segmentation:** Our cloud infrastructure is protected by multiple layers of firewalls. We implement network segmentation to limit access between different parts of our infrastructure, ensuring that a compromise in one system does not impact other systems.

Redundancy and Disaster Recovery

Autograph's infrastructure is built for redundancy and resilience:

- **Backups:** We perform backups of Sensitive, Confidential, and Public data for all in-scope production systems, including infrastructure and data stores to appropriately safeguard customer data. We configure our cloud service provider(s) (CSP) AWS, to perform backups of all data stored in the cloud on a daily basis. Backups are performed using the CSP's automated backup tool.
- **Multiple Regions:** Our platform is hosted in multiple AWS regions to ensure availability even if one data center experiences downtime.
- **BC/DR Testing:** Auto Graph tests its business continuity (BC) capabilities on at least an annual basis via a simulated tabletop exercise,and documents the results to strive for continuous improvement.

8. Monitoring and Incident Response

Autograph employs real-time monitoring to detect and respond to potential security incidents. We follow a structured incident response plan, ensuring that any detected threats are contained and resolved promptly.

- **Incident Response Team**: Our dedicated team follows predefined steps to handle incidents, including notifying affected parties where necessary.
- **Responsible Disclosure**: We welcome vulnerability reports from external parties and respond to them in a timely manner to safeguard our systems.

9. Continuity and Resilience

Autograph operates with redundancy across multiple data centers to ensure the resilience of our services. In the event of a disaster, our business continuity and disaster recovery (BCDR) plans ensure rapid recovery.

- **Data Backups**: All critical data is backed up regularly and stored in geographically dispersed locations.
- **Disaster Recovery Testing**: We perform regular tests of our disaster recovery plans to ensure they function as intended during an actual event.

10. Contact Us

For more information on Autograph's security practices or to request compliance reports, please contact us at:

Email: security@withgraph.com

Phone: 305-204-6005