ControlUp Security White Paper

Last updated: January 2022

Table of Contents

1. Introduction

- This document outlines the principles behind ControlUp's technical and organizational data security measures. These measures are provided as standard to all customers and in all ControlUp products and services, as required by the Regulation (EU 2016/679), the General Data Protection Regulation ("GDPR").
- ControlUp implements appropriate technical and organizational data security measures which are designed to meet the data protection principles effectively. ControlUp ensures that appropriate safeguards are integrated into the processing of personal data to meet the requirements of the GDPR and to protect the rights of data subjects as described below.

2. Organizational Structure

- ControlUp has a Chief Information Security Officer (CISO) who designs, develops, and deploys our technical architectures, security policies, standards, and awareness program, along with our security department.
- The ControlUp security department is divided into three main pods:
  - Research and Penetration – responsible for product security architecture and challenging applications and infrastructure to trace possible vulnerabilities.

- SecOps – responsible for the ControlUp network architecture, security controls and security monitoring.
- GRC – responsible for managing ControlUp security policies, risk, compliance, and customer inquiries. The GRC pod can be reached at privacy@controlup.com.

3. Governance and Risk Management

- Annual Risk Assessment includes information security audits managed by the CISO, using a methodology based on best security standards. Its results are presented to the steering committee and followed by management during management's security reviews.
- ControlUp has public security and privacy policies which are available to customers on request. The policies are supported by a wide range of mandatory rules on different aspects of data protection and information security.

4. Third Party Risk Management

- Prior to engagement, third-party vendors used by ControlUp are screened using third-party questionnaires and a certification review. This is to ensure that they meet ControlUp's security standards.
- Periodically, The Compliance and Security Manager reviews controls within assurance reports to ensure that they meet organizational requirements.

5. Physical Security

5.1 Production environment

- ControlUp's physical and virtual servers are hosted by Amazon Web Services (AWS) and Microsoft Azure. Access to these data centers is limited to authorized personnel only, as verified by biometric identity verification measures. Physical security measures for these data centers include: on-premises security guards, closed-circuit video monitoring, and additional intrusion protection measures. More on AWS security measures can be found here. More on Azure security measures can be found here.

5.2 Corporate environment

- ControlUp has implemented best practice measures to prevent unauthorized persons from gaining access to its resources and equipment, regardless of whether those resources are directly related to where personal data is processed or used. These measures may include all or a combination of any of the following:
    - Maintaining offices which are within facilities requiring employees and visitors to register for entry beyond the front entrance.
    - Enforcing strict measures to ensure that all visitors are accompanied, and awareness among employees to challenge any exceptions.
    - Enforcing restricted access to areas housing

communications or other technological equipment on an employee role basis.

- Utilizing a high-security card key system to control facility access.
- CCTV video surveillance monitoring of all entry and exit points.

6. Job Control

- All ControlUp employees are required to sign confidentiality agreements prior to accessing our ControlUp resources.
- All ControlUp employees are required to receive security and privacy training at time of hire, as well as quarterly security and/or privacy awareness training.
- ControlUp employees are subject to disciplinary action, including but not limited to termination, if they are found to have abused the "ControlUp Acceptable Use Policy".
- The CISO communicates with all employees on a regular basis, covering topics such as emerging threats, phishing awareness campaigns, and other industry-related security topics.

7. Production Access Control - Internal Access to Customer Data

- Access to AWS or Azure consoles are managed by complex password-protected user accounts.
- MFA is enforced while accessing our production and development environments.
- Role-based access controls are implemented in a manner consistent with the principle of least privilege.
- Access is granted according to a strict formal procedure, and is periodically reviewed.

8. Network and Infrastructure Controls

8.1 Network and Infrastructure Security

- Remote access must be via SSL VPN using two-factor authentication.
- ControlUp regularly updates its network architecture schema and maintains an understanding of the data flows between its systems.
- Firewall rules and access restrictions are established and reviewed for appropriateness on a regular basis.
- Our Wi-Fi internal corporate LAN is separated from the guest Wi-Fi, and encrypted by certificate-based authentication.

8.2 Vulnerability and Patch Management

- ControlUp establishes a vulnerability and patch management process for our systems which includes technical vulnerability assessments, patch testing, patch deployment and verification.

8.3 Encryption

- **Data in Transit** - Customer Data is encrypted during transmission using up-to-date versions of TLS (1.2 or higher).
- **Data at Rest** - Customer data is stored in encrypted databases with strong encryption algorithms.

8.4 Laptop and Server Protection

- ControlUp uses best-of-breed EDR software on all employee laptops and in the production, corporate and QA servers.
- ControlUp implements protections on end-user devices and monitors for those devices to achieve compliance with the security standard. This includes requiring password protection, a screen saver, and patch management.

9. Monitor and Control

- ControlUp uses an intrusion detection system and other security monitoring tools on the production environment. Notifications from these tools are sent to the ControlUp Security Department SIEM (Security Information and Event Management) so that they can take appropriate action.
- Employee access to the production environment is logged, monitored and audited.

10. Segregation Controls

- The ControlUp architecture provides effective and logical application data separation for different customers. This is done via customer-specific and unique "Organization IDs" and enables the use of customer and user role-based access privileges. This virtual segmentation is being tested by well-known security companies via gray and black box penetration testing.
- In addition to virtual customer data segregation, ControlUp leverages many aspects of AWS capabilities to meet or exceed the security of customers' on-premises physical separation requirements. These include:
    - Unified authentication and authorization.
    - Rich monitoring and logging.
    - Encrypting data at-rest and in-transit.
    - Host and instance isolation.

- Separate environments for different functions, especially for testing, QA and production.

11. Secure Development Life Cycle

11.1 Product Security

- ControlUp's software security practices are measured using industry-standard security models.
- The ControlUp software development life cycle (SDLC) uses applicable OWASP Top 10 standards and includes many activities intended to foster security. These include:
- Defining security requirements.
- Design (threat modeling and analysis, security design review).
- Development controls (static analysis, manual peer code review).
- Testing (dynamic analysis).
- Deployment controls (such as change management and canary release process).

11.2 Code Assessments

- ControlUp platforms are continually monitored and tested using processes designed to proactively identify and remediate vulnerabilities. We regularly conduct:
  - Automated source code analysis designed to find common defects.
  - Peer review of all code prior to being pushed to

production.

- The ControlUp Security Research team constantly reviews and challenges the code for vulnerabilities.
- Third-party application security assessments and penetration tests are performed annually.

11.3 Change Management

- To maximize data confidentiality, integrity and availability, ControlUp manages changes to the production systems very carefully. Our change control procedures are designed to ensure that changes potentially impacting customer data are documented, tested, and approved before deployment.

11.4 Privacy by design

- ControlUp incorporates privacy by design principles for systems and enhancements at the earliest stage of development. We also educate all employees on security and privacy on an annual basis.

12.Availability Controls

12.1 System Availability

- The infrastructure for ControlUp platforms is designed to minimize service interruption due to hardware failure, natural disaster, or other catastrophes. Features include:
    - **State-of-the-art cloud provider**: ControlUp uses Amazon Web Services and Microsoft Azure, which are trusted by thousands of businesses to store and serve their data and services.
    - **Backups**: ControlUp performs backups which are tested regularly.
    - **Disaster recovery and continuity plan**: ControlUp has a disaster and business continuity plan that enables the company to respond quickly and remain resilient in the event of most failure modes, including natural disasters and system failures.

12.2 Incident Response

- ControlUp maintains an incident response procedure which is designed to promptly and systematically respond to any security and availability incidents that may arise.
- In the event of a personal data breach, ControlUp will notify customers up to 72 hours after becoming aware of the personal data breach.

13. Compliance

- ControlUp conducts regular internal and external audits of its security, led by the Security and Compliance Manager.
- ControlUp complies with GDPR and is certified to the following standards:
  - SOC 2
  - ISO 27001
  - ISO 27018
  - ISO 27017
  - FIPS
  - CSA

Conclusion

- We take security seriously at ControlUp because every customer using our service expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers, and we work hard to maintain that trust.