Alvius Data Security

Contents

Contents	**2**
Introduction	**3**
Asset Protection and Resilience	**3**
Operational Security	**3**
Secure Development	**4**
Supply Chain Security	**5**
Secure User Management	**5**
Identity and Authentication	**5**
External Interface Protection	**5**
Data in Transit Protection	**6**
Secure Service Administration	**6**
Audit information for Users	**6**
Secure Configuration of Employee Devices	**6**
Home and Mobile Working	**6**
Malware Prevention	**6**

Introduction

Alvius's data security policies, procedures and processes are modelled on the UK Government's National Cyber Security Centre (NCSC)'s 'Principles for Cloud Security', the NCSC's '10 Steps to Cyber Security', ISO 27001 standards and SAFECode's Fundamental Practices for Secure Software Development.

Alvius's technical management team is continuously examining the system architecture, platforms and ways in which we protect our client's and user's data. We conduct periodic internal and external monitoring, following a lifestyle approach, to ensure continued adherence to best practise through a risk-based approach, to ensure good information security governance, and to ensure that we conform to all applicable legal and regulatory requirements.

Wherever possible we apply recognised sources of security management good practise, as detailed above. We promote a risk management culture within the organisation to ensure that everyone understands the importance of security, is aware of the security risks faced by the organisation, and the practicalities that are involved in ensuring that the organisation manages client and user data safely, responsibly and securely.

Asset Protection and Resilience

The Alvius system runs on Amazon Web Services (ISO 27002 and 27001 certified and G Cloud approved), which maintains responsibility for physical security as well as secure equipment disposal (following NIST 800-88 procedures) and overwriting of storage before reallocation for the hardware used to operate the system.

All data is stored on data centres within the UK. Our primary database is deployed across multiple availability zones (clusters of data centres) using synchronous logical replication with automatic failover to ensure system resilience. Databases are object storage are also encrypted at rest using AES-256 encryption.

Alvius' system is hosted on Amazon Web Services (AWS), using a Virtual Private Cloud (VPC) architectural model. This ensures that services within the Alvius VPC are private by default and cannot be accessed over the internet.

Sensitive fields are encrypted at the edge of the network through a CDN. This uses asymmetric encryption using a public-private key pairing to encrypt the field such that only privileged parts of the applications can decrypt it. Similarly files are encrypted using individual symmetrical encryption keys.

Operational Security

We operate on a weekly deployment cycle which includes bug fixes and incremental feature releases. All code commits must pass a series of stages before they are deployed to the production environment. There is an initial code review performed by a senior developer and all new code is reviewed automatically by a static code monitoring tool.

A release candidate of a series of code changes are packaged together and tested using a web application scanner for security vulnerabilities as well as a test suite of automated tests. These tests include API tests, unit tests and end-to-end browser-based tests which perform acceptance tests on expected functionality as well as on permissions and data visibility.

The production environment is monitored by a web application scanner, and the underlying infrastructure is analysed by a vulnerability detector which analyses server logs and the platform is monitored by an intrusion detection system. Open-source dependencies that are used by the platform are continuously monitored for known vulnerabilities and are patched accordingly. Application secrets are encrypted at rest and retrieved programmatically by the applications in order to securely store keys and allow for the easy rotation of them.

Secure Development

Security is a fundamental consideration during the design, building and testing phases of development.

During the design phase, as per SAFECode Fundamental Practices, the following principles are adhered to:

- **Economy of mechanism:** keeping the system as simple as possible
- **Fail-safe defaults:** access and permissions are denied by default
- **Complete mediation:** user access to every field for every object must be authorised
- **Least privilege:** every user should have the fewest permissions and access to do their job
- **Least common mechanism:** minimize the amount of code that is used by more than one role type
- **Psychological acceptability:** ensuring that the user interface encourages secure behaviour for users
- **Compromise recording:** ensuring that systems are auditable and therefore record any instances of compromised data access
- **Defense in depth:** design a system so that multiple layers of security prevent unauthorised activity on the system
- **Fail securely:** the system should be designed to remain secure even if it crashes or fails in some way
- **Design for updating:** systems are constantly evolving and new vulnerabilities will emerge which means systems should be easy to update

During the development process, code is scanned using static scanners for potential vulnerabilities and insecure coding practises. Automated testing and web application scanning is used to test code prior to deployment to ensure security (see Operational Security).

Supply Chain Security

Our supply chain has been selected taking into account their track record of resilience and high security standards. Our due diligence provides us with the assurance that this will remain the case on an ongoing basis.

When selecting a cloud-based technology supplier, we conduct due diligence on areas such as their market reputation, ISO and similar certifications, customer support levels, and their standard Service Level Agreements (SLAs). For software suppliers wherever possible we use open-source software with a proven track-record and an active development community, rather than relying on proprietary software provided by a single supplier. We assess all suppliers on a 6-monthly basis, to determine whether the service we have received has been satisfactory, as well as whether there are any additional risks in the supplier relationship. This includes legal risks such as GDPR, service delivery, financial or contractual risks.

Secure User Management

Alvius provides administrative access to clients to manage their user accounts through a management interface. Role-based access control policies can be configured by the client to ensure adherence to the principle of least privilege.

Identity and Authentication

The authentication system used by Alvius is PCI DSS, SOC, and ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO 9001 compliant.

Users can use multi-factor authentication to secure their account, using SMS or a Time-based One-time Password (TOTP) generator, such as Google Authenticator. The system uses adaptive authentication, detecting unusual sign-in activity, such as sign-in attempts from new locations and devices and requiring an additional authentication method for additional security. The system also supports federated authentication through common identity management standards such as OpenID Connect, OAuth 2.0, and SAML 2.0.

External Interface Protection

A Web Application Firewall sits in front of the Internet Gateway to the VPC to regulate and limit public access to the system. In addition, the system is protected from Distributed Denial of Service Attacks (DDoS) using an automatic detection and mitigation system to minimise

downtime and latency of attacks. Dynamic Application Security Testing is used to monitor the security of the public-facing access points into the system.

Data in Transit Protection

Wherever possible, communications between systems occur through private connections that do not occur over the internet and use private IP addresses for additional security. Where data transfer over the internet is necessary, TLS 1.2+ is enforced for all connections.

Secure Service Administration

Alvius's set-up conforms to the direct service administration model. Full-administrative access is limited to a subset of the technical management team.

Audit information for Users

Audit logs containing system activity is recorded and can be provided to clients for auditing purposes in standard open file formats.

Secure Configuration of Employee Devices

To ensure that the devices that Alvius employees' devices are secure, we use modern operating systems, web browsers and applications that are regularly updated. User devices are secured through a centralised-device management system which enforces policies such as file-system level encryption, device application layer firewalls, and regular system and application updates. An inventory is maintained of all hardware and software owned by the company.

Home and Mobile Working

Employees' devices' file systems are encrypted at rest using XTS-AES-128 encryption with a 256-bit encryption key. Connections to systems are made using TLS or SSH, and Virtual Private Networks (VPNs) are also used for certain tasks to ensure a secure, private, connection.

A cloud-based password management system is used to ensure that user credentials are not stored on the user's device, and devices can be remotely wiped to protect data in cases of loss or theft. Removable media devices are controlled to prevent malicious introduction of malware or loss of information. Employees must only use formally issued removable media and the disposable of such devices are managed centrally in line with the Alvius 'Data Disposal Procedures and Policies'.

Malware Prevention

Alvius employees' email has anti-malware and anti-phishing protection which blocks attachments that have malicious content and quarantines emails that have signs of a phishing attack to

prevent the email from reaching the user's inbox. Employees' devices comes installed with modern web browsers that block malicious websites. In addition, employees are educated on the importance of vigilance when it comes to preventing a malware or other cyber attacks from occurring.

Managing User Privileges

User privileges are limited based on the principle of 'least privilege', and are regularly audited to ensure that no user has unnecessary access to systems. Employees must use a password manage to ensure that secure, unique, passwords are used for credentials across different platforms. Two-factor authentication is mandatory for all core systems.