AIRLOCK
DIGITAL

Security Overview Whitepaper

APRIL 2023

[SEC=CONFIDENTIAL]

Organizational security

We have an Information Security Management System (ISMS) in place which takes into account our security objectives and the risks and mitigations concerning all the interested parties. We employ strict policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data.
Employee background checks

Each employee undergoes a process of background verification. We hire reputed external agencies to perform this check on our behalf. We do this to verify their criminal records, previous employment records if any, and educational background. Until this check is performed, the employee is not assigned tasks that may pose risks to users.

Security Awareness

Each employee, when inducted, signs a confidentiality agreement and acceptable use policy, after which they undergo training in information security, privacy, and compliance. Furthermore, we evaluate their understanding through tests and quizzes to determine which topics they need further training in. We provide training on specific aspects of security, that they may require based on their roles.

We educate our employees continually on information security, privacy, and compliance in our internal community where our employees check in regularly, to keep them updated regarding the security practices of the organization. We also host internal events to raise awareness and drive innovation in security and privacy.
Dedicated security and privacy teams

We have dedicated security and privacy teams that implement and manage our security and privacy programs. They engineer and maintain our defence systems, develop review processes for security, and constantly monitor our networks to detect suspicious activity. They provide domain-specific consulting services and guidance to our engineering teams.

Internal audit and compliance

We have a dedicated compliance team to review procedures and policies in Airlock Digital to align them with standards, and to determine what controls, processes, and systems are needed to meet the standards. This team also does periodic internal audits and facilitates independent audits and assessments by third parties.

Endpoint Security

All workstations issued to Airlock Digital employees run up-to-date OS version and are configured with anti-virus software. They are configured such that they comply with our standards for security, which require all workstations to be properly configured, patched, and be tracked and monitored by Airlock Digital's endpoint management solutions. These workstations are secure by default as they are configured to encrypt data at rest, have strong passwords, and get locked when they are idle. Mobile devices used for business purposes are enrolled in the mobile device management system to ensure they meet our security standards.

Physical security

At workplace

We control access to our resources (buildings, infrastructure and facilities), where accessing includes consumption, entry, and utilization, with the help of access cards. We provide employees, contractors, vendors, and visitors with different access cards that only allow access strictly specific to the purpose of their entrance into the premises. Human Resource (HR) team establishes and maintains the purposes specific to roles. We maintain access logs to spot and address anomalies.

At Data Centres

At our Data Centres, a co-location provider takes responsibility of the building, cooling, power, and physical security, while we provide the servers and storage. Access to the Data Centres is restricted to a small group of authorized personnel. Any other access is raised as a ticket and allowed only after the approval of respective managers. Additional two-factor authentication and biometric authentication are required to enter the premises. Access logs, activity records, and camera footage are available in case an incident occurs.

Monitoring

We monitor all entry and exit movements throughout our premises in all our business centres and data centres through CCTV cameras deployed according to local regulations. Back-up footage is available up to a certain period, depending on the requirements for that location.

Infrastructure security

Network security

Our network security and monitoring techniques are designed to provide multiple layers of protection and defence. We use firewalls to prevent our network from unauthorized access and undesirable traffic. Our systems are segmented into separate networks to protect sensitive data. Systems supporting testing anddevelopment activities are hosted in a separate network from systems supporting Airlock Digital's production infrastructure.

We monitor firewall access with a strict, regular schedule. A network engineer reviews all changes made to the firewall every day. Additionally, these changes are reviewed once in every six months to update and revise the rules. Our dedicated Network Operations Centre team monitors the infrastructure and applications for any discrepancies or suspicious activities. All crucial parameters are continuously monitored using our proprietary tool and notifications are triggered in any instance of abnormal or suspicious activities in our production environment.

Network redundancy

All the components of our platform are redundant. We use a distributed grid architecture to shield our system and services from the effects of possible server failures. If there's a server failure, users can carry on as usual because their data and Airlock Digital services will still be available to them.

We additionally use multiple switches, routers, and security gateways to ensure device-level redundancy. This prevents single-point failures in the internal network.

DDoS prevention

We use technologies from well-established and trustworthy service providers to prevent DDoS attacks on our servers. These technologies offer multiple DDoS mitigation capabilities to prevent disruptions caused by bad traffic, while allowing good traffic through. This keeps our websites, applications, and APIs highly available and performing.

Server hardening

All servers provisioned for development and testing activities are hardened (by disabling unused ports and accounts, removing default passwords, etc.). The base Operating System (OS) image has server hardening built into it, and this OS image is provisioned in the servers, to ensure consistency across servers.

Intrusion detection and prevention

Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents.

Data security Airlock Digital

Secure by design

Every change and new feature is governed by a change management policy to ensure all application changes are authorised before implementation into production. Our Software Development Life Cycle (SDLC) mandates adherence to secure coding guidelines, as well as screening of code changes for potential security issues with our code analyser tools, vulnerability scanners, and manual review processes.
Our robust security framework based on OWASP standards, implemented in the application layer, provides functionalities to mitigate threats such as SQL injection, Cross site scripting and application layer DOS attacks.

Data isolation

Our framework distributes and maintains the cloud space for our customers. Each customer's service data is logically separated from other customers' data using a set of secure protocols in the framework. This ensures that no customer's service data becomes accessible to another customer.
The service data is stored on our servers when you use our services. Your data is owned by you, and not by Airlock Digital. We do not share this data with any third-party without your consent.

Encryption

In transit: We have a standard based on guidance from Australian Cyber security centre, which is similar to NIST, details of the standard for encryption in transit can be found here

At rest: We have a standard based on guidance from Australian Cyber security centre, which is similar to NIST, details of the standard for encryption at rest can be found here

Data retention and disposal

We hold the data in your account as long as you choose to use Airlock Digital Services. Once you terminate your Airlock Digital user account, your data will get deleted from the active database during the next clean-up

Identity and Access control

Access Administration

A formal user registration/de-registration and access provisioning process is implemented to assign or revoke access rights to Airlock Digital IT assets.

Privileged Access Management

Administrative access rights to manage Airlock Digital IT assets must be reviewed and approved by the Chief Technology Officer.

A separate administration account to the user’s regular account must be assigned to personnel administering Airlock Digital information assets.

- Multi-factor authentication must be implemented and enforced for all administrator account logins.

- Administration accounts must not be used to access to email or web-browsing functionality nor be used to perform day-to-day activities.

Administrative access

We employ technical access controls and internal policies to prohibit employees from arbitrarily accessing user data. We adhere to the principles of least privilege and role-based permissions to minimize the risk of data exposure.

Access to production environments is maintained by a central directory and authenticated using a combination of strong passwords, two-factor authentication, and passphrase-protected SSH keys. Furthermore, we facilitate such access through a separate network with stricter rules and hardened devices. Additionally, we log all the operations and audit them periodically.

Operational security

Logging and Monitoring

We monitor and analyse information gathered from services, internal traffic in our network, and usage of devices and terminals. We record this information in the form of event logs, audit logs, fault logs, administrator logs, and operator logs. These logs are automatically monitored and analyzed to a reasonable extent that helps us identify anomalies such as unusual activity in employees’ accounts or attempts to access customer data. We store these logs in a secure server isolated from full system access, to manage access control centrally and ensure availability.

Detailed audit logging covering all update and delete operations performed by the user are available to the customers in every Airlock Digital service.

Vulnerability management

We have a dedicated vulnerability management process that actively scans for security threats using a combination of certified third-party scanning tools and in-house tools, and with automated and manual penetration testing efforts. Furthermore, our security team actively reviews inbound security reports and monitors public mailing lists, blog posts, and wikis to spot security incidents that might affect the company's infrastructure.

Once we identify a vulnerability requiring remediation, it is logged, prioritized according to the severity, and assigned to an owner. We further identify the associated risks and track the vulnerability until it is closed by either patching the vulnerable systems or applying relevant controls.

Malware and spam protection

We scan all user files using our automated scanning system that's designed to stop malware from being spread through Airlock Digital's ecosystem. Our custom anti-malware engine receives regular updates from external threat intelligence sources and scans files against blacklisted signatures and malicious patterns. Furthermore, our proprietary detection engine bundled with machine learning techniques, ensures customer data is protected from malware.

Airlock Digital supports SPF and DKIM to verify that messages are authentic. We also use our proprietary detection engine for identifying abuse of Airlock Digital services like phishing and spam activities. Additionally, we have a dedicated anti-spam team to monitor the signals from the software and handle abuse complaints.
From your end, we strongly recommend scheduling regular backups of your data by exporting them from the respective Airlock Digital services and storing it locally in your infrastructure.

Disaster recovery and business continuity

Application data is stored on resilient storage that is replicated across data centres. Data in the primary DC is replicated in the secondary in near real time. In case of failure of the primary DC, secondary DC takes over and the operations are carried on smoothly with minimal or no loss of time. Both the centres are tier 3 datacentres

We have power back-up, temperature control systems and fire-prevention systems as physical measures to ensure business continuity. These measures help us achieve resilience. In addition to the redundancy of data, we have a business continuity plan for our major operations such as support and infrastructure management.

Incident Management

Reporting

We have a dedicated incident management team. We notify you of the incidents in our environment that apply to you, along with suitable actions that you may need to take. We track and close the incidents with appropriate corrective actions. Whenever applicable, we will identify, collect, acquire and provide you with necessary evidence in the form of application and audit logs regarding incidents that apply to you. Furthermore, we implement controls to prevent recurrence of similar situations.

Vendor and Third-party supplier management

We evaluate and qualify our vendors based on our vendor management policy. We onboard new vendors after understanding their processes for delivering us service, and performing risk assessments. We take appropriate steps to ensure our security stance is maintained by establishing agreements that require the vendors to adhere to confidentiality, availability, and integrity commitments we have made to our customers. We monitor the effective operation of the organization’s process and security measures by conducting periodic reviews of their controls.

And how both our customers and Airlock Digital can collaborate as well as take up individual responsibility towards cloud security and privacy