cloudPWR

SECURITY OVERVIEW

SECURITY AND DEVELOPMENT PRACTICES
PUBLISHED 10.20.2020

https://cloudpwr.com/security
INFO@CLOUDPWR.COM206.588.6861

Data Security & Access

CloudPWR's AIRLIFT platform supports a variety of customers and use cases. Security is a very important consideration; we have broken this subject down into several sections for customers to review. This information is meant to provide a general overview. Proprietary information with greater detail is available under non-disclosure agreement.

Infrastructure

Our infrastructure is designed to provide redundancy and scalability. This approach provides strong resiliency to disaster scenarios. We utilize AWS Security policies to restrict access between application server layers. Access is secured by using authentication keys and a single point of access for maintenance. The solution utilizes a centralized full stack monitoring service and provides full system and access log support. The monitoring service is fully automated and provides notification when it identifies system issues.

We provide three environments to separate production data workload from testing and development loads. These environments run in separate instances using databases and connections unique to each instance.

Our sandbox environment allows for any fictitious testing data for training or testing of the application while maintaining the same application constraints and ability to configure the same security and application settings. No provision is provided to copy production data into the sandbox environment except basic account information (account name, basic settings etc.) and one set administrator on the production account for administering the sandbox.

Security Compliance

Our controls meet or exceed those expected by the Federal Information Security Management Act (FISMA) for Moderate Impact Systems and as the most current release of National Institute of Standards and Technology (NIST) Special Publications SP 800-53.

Our service, AIRLIFT, can be hosted on tier one cloud service providers We currently support AWS, Azure and Google Cloud Platform (GCP). For example, we support Amazon Web Services (AWS) using Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3) and Amazon Virtual Private Cloud (VPC), which have all received FISMA Moderate authorization and accreditation from the General Services Administration.

Software Development

Our application is built with current best practices and is consistent with NIST SP 800-64 including:

- Tracking issues and features in development and their security implications
- Keeping the development team aware of current security threats as well as the latest secure coding techniques, quality control and code review before code is merged into the production repository
- Maintaining secure development environments
- Using unit tests and security tools to verify the security correctness of the application code

Our application does not contain any of the OWASP top 10 vulnerabilities and verifying this status is part of our regular security testing process.

Independent Security Audits

We contract with independent security audit firms to provide quarterly penetration testing to validate our cybersecurity posture. This includes a review of our code base and testing for known vulnerabilities and threat vectors.

We contract with independent auditors to provide Type II Security and Operational Controls validation, also known as SOC 2 compliance.

Updates & Patches

All software patches to software utilized in the infrastructure of our application are managed through a central orchestration system with configuration files that are managed through source control. It is an agent-based system that provides us with inventory management and patch management for all of our application servers. This system allows us to manage the exact software installed on each of our servers as well as test deployments of new patch sets and ensures the security of patch sets using built-in OS tools. We also do not allow for any form of automated patching through OS services or third-party tools and restrict and monitor user access to initiate patch sets.

Audit Logs

Our application provides audit logging of all data changes in the system to a separate logging point that cannot be altered from within the application. Logs are rotated, compressed, encrypted and archived for later analysis if necessary. All hosts have their system time synchronized via NTP to UTC. Our application also provides access logs of all information recording the date and time of access, the user accessing the data, the data accessed as well as IP address. Our central logging service to provide notifications of unusual activity monitors all relevant logs.

Security Policies

cloudPWR maintains a set of security and privacy control policies that address the controls discussed in NIST SP 800-53. We can provide additional information for the specific controls and policies as required by customer.

Access Policy:

Sets policies and procedures for access controls including account management and enforcement, identification and authentication policies and processes that uniquely identify organization users, and physical and environmental procedures.

Disaster Recovery Policy:

Outlines contingency plans for handling incidents as well as training and maintaining relevant procedures.

Operations Policy:

Provides awareness and training of security issues, sets a policy for systems maintenance and applying patch sets, maintains a policy for acquiring, allocating, documenting and evaluating system resources and capacity, and sets standards for development processes, standards, tools and training.

Security Policy:

Proscribes regular security assessments conducted both internally and externally, requires auditing and accountability for data and systems configurations, includes a policy for protecting both digital and non-digital media, outlines a security plan including system and data security, maintains a policy in regard to personnel security, provides a procedure for risk assessment and screening, proscribes conducts regular application risk assessments and vulnerability scans, has policies and outlines systems that protect system data and communications, and maintains policies and systems for maintaining system and data integrity including monitoring, alerts and validation.

System Configuration & Change Management practices

cloudPWR maintains a Configuration Management Policy that addresses procedures and policies for managing information system configurations as well as setting the roles and responsibilities for configuration management.

This policy includes maintaining a baseline configuration of information systems including an automated system to manage patch sets as well as the configuration of information systems. This automated system's configuration is maintained in version control to facilitate rollbacks of configurations if necessary.

All proposed changes to the configuration are documented in our version control system and reviewed by relevant staff and approved before being deployed. All changes go through testing and validation during the proposal process to ensure they do not interfere with system operations. During validation security impacts are evaluated.

Our configuration management system also maintains the inventory of system components, keeping this inventory up to date as system configurations change. Additional controls are provided in our hosting environment and configuration to ensure that no unauthorized or duplicate systems are present.

Use of Production Data

It is cloudPWR company policy that no data may be copied, moved, or transmitted from a production system for any purpose without the knowledge of the client. No production data is ever to be used in development, testing, quality assurance, or security evaluation. Access to production data is limited to only customer service, troubleshooting, or quality assurance tasks and is to be limited to only data necessary to complete the task in question.

Communication Policy in the Event of Breach

Our incident response plan includes preventative steps previously mentioned including conducting security risk assessments at regular intervals, using our patch management process to ensure host security, data center security controls and server topology that ensures network security, as well as user training.

We continuously monitor for incidents using file integrity checking software, monitoring operating system, application and network logs, keeping current with news about the latest vulnerabilities and exploits, and encouraging proactive communication from our staff and persons outside the organization about incidents.

Additionally, we keep a log of all incidents including: the incident status, a summary of the incident, all pertinent supporting information collected, actions taken by our incident handling team, and a list of parties that need to be contacted about the incident including clients.

Upon discovery of a security incident it is cloudPWR policy that all relevant parties, including clients, be notified in a timely manner with information regarding the incident including functional impact, information impact and effort needed to recover from the incident.

Disaster Recovery Plan

cloudPWR maintains a disaster recovery plan that includes an alternate facility in a distinct geographic region with redundant infrastructure to allow for fast recovery from a primary facility failure. We utilize streaming database replication over encrypted connections to provide minimal downtime and with a minimum loss of data. We also make full database backups every

24 hours that are encrypted and stored on a redundant back system in the case of a catastrophic failure.

Role-Based Data Access Rights

Our system provides user and administrator roles and permissions that can restrict privileges to any desired levels. We further provide fine-grain Object Security Policy that allows for selectively granting or revoking specific permissions to users or groups

System Time-out and Re-authentication

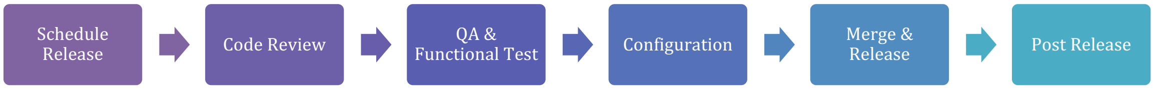
Our application allows for setting the inactivity time-out to a specific period based on customer requirements. No unsaved data is retained between authenticated sessions. Reading and/or updating data is considered system activity and extends the timeout.

Error Notifications of Failed Transactions

The application logs all failed requests and provides messages to the user describing the error that occurred.

Software Development

1. At a high level, our release management process follows a standard agile deployment process as outlined below. All code is managed in GitHub for code collaboration, review and code management.



   a. **Schedule Release:** Release date is scheduled. Customers are notified of upcoming release and any outages.

   b. **Code Review:** Code Reviewer reviews code looking for and coding bugs or other issues. If there are problems with the code, the Reviewer should comment on the differences and send it back to the coder. When the Reviewer decides the code is ready the issue should have the "code review" label removed and be labelled as "ready for QA."

c. **QA and Functional Test:** When a new release is being prepared, a new development branch is created from the last release. Issues that are ready for QA are merged into the QA branch. Any database updates required for the release are run against the QA database server.

d. **Configuration:** Developers confirm they have a checked-out copy of the private configuration's repository from the bastion server. Any necessary configuration updates follow the same code review process.

e. **Merge and Release:** Once all issues for the release are QA Pass they are merged into the master branch. A new metatag is created for the release and pushed into the repository.

f. **Post Release:** Verify availability and functionality of the production server. Write any release collateral (release notes, blog posts, press releases).

2. Operational and maintenance communication strategies for downtime and upgrades are based on the following methods:

   a. Coordination with customer System Administrators via email and phone.

   b. Within the AIRLIFT user interface, we can also include a link to upcoming system maintenance events, frequently asked questions, training material and new feature release description and schedule.

   c. The ability to subscribe to group email list for announcements.

Thank you for taking the time to read this summary of our security and development practices. Customer data and application security is a priority concern for our development and operations teams. Further review of SOC-II Audit Report and other security sensitive information can be made available under non-disclosure agreement.