Positioning Universal

Technical and Organizational Measurements Statement

Document Version: 1.1
Approved on: March 21, 2019
Approved by: Brad Bitterman

Updated on: August 5, 2020 for Positioning Universal

Table of Contents

Introduction

This Positioning Universal Technical and Organizational Measures Statement (TOMS) measures and controls the technical and organizational security measures implemented by Positioning Universal to protect the IoT devices and data customers entrust to us as part of their relevant Positioning Universal service. These documents are a high-level overview of Positioning Universal' technical and organizational measures. Positioning Universal may change these measures from time to time to adapt to the evolving security landscape and where required will notify customers of these changes.

Permitted Use

This document may only be used for your internal purposes in connection with Positioning Universal' products and services. This document undergoes frequent updates. Unless this statement forms part of your or your organization's contractual arrangements with Positioning Universal, it should not be copied or duplicated without the express written permission from Positioning Universal.

Positioning Universal Platform

Positioning Universal is a Device Management SaaS solution that provides secure bi-directional communication between IoT devices and the cloud, creating seamless integration between sensors and business applications. It includes secure provisioning, data transformation, analytics and software update features as well as connectors into dozens of third-party systems.

Access Control

In the context of users performing administrative actions, the Positioning Universal platform is accessed by a customer or support technician using a web-based portal for the administration of their devices in the field, or by a Positioning Universal Cloud Engineer to administrate each environment directly.

Positioning Universal implements suitable measures to prevent unauthorized access into the Positioning Universal platform. This is accomplished by:

- Positioning Universal authentication (using a unique username and password) to authenticate users into the system all over TLS.
- Positioning Universal does not allow the use of common passwords (derived from a live list of many of the most common passwords used).
- Positioning Universal portal user's credentials are stored encrypted and require tokenized access issued by an identity management system.
- MFA is required for site admins to log in and administrate the Positioning Universal platform.
- All activity a site admin undergoes within Positioning Universal is logged and can be viewed by any approved users within Positioning Universal.
- Only authorized Positioning Universal employees are able to connect and log in to all hosted databases for troubleshooting purposes, all of which are fully audited and logged within the audit log.

Identity Management

Positioning Universal employs an identity and access management system to authenticate and authorize Positioning Universal platform users. This takes the form of tokenized access with time expiration for a user accessing a web-based administrative portal, or via an identity provider with MFA, for a cloud engineer performing administrative tasks.

Positioning Universal Platform User Policy

Positioning Universal has implemented policies to ensure specific users have access to specific areas within the network and systems. This is achieved by, but not limited to:

- Positioning Universal Platform Users:
  - Positioning Universal platform users are granted limited credentials.
  - Any unused or inactive Positioning Universal platform user credentials are automatically disabled after 90 days.
  - Positioning Universal platform users are segregated from infrastructure administration accounts.
- Positioning Universal Employees:
  - Only authorized Positioning Universal employees are granted the ability to gain access to secure areas within the Positioning Universal environment.
  - Positioning Universal Platform Operations personnel are required to pass a site administration training and to have a separate user account tied to MFA.
  - All Positioning Universal employees undergo regular security awareness training.
  - All Positioning Universal Infrastructure access rights follow the principle of least privilege.
  - All Positioning Universal employees are subject to overarching Flex, Inc. security policies and training.
  - A formal termination process is immediately followed for any terminated employee, to ensure all access rights and permissions are no longer available to the terminated employee.

Positioning Universal Platform Access Monitoring

Positioning Universal implements proper measures to monitor access restrictions to Positioning Universal' System Administrators and to ensure that they act in accordance with instructions received.

This is accomplished by:

- Individual appointment of trusted site administrators
- Role based access control (RBAC)
- Activity logging
- Just-in-time access to critical assets
- Implementation of platform monitoring with an automated response process, of threshold alerts, using runbooks

Availability

The Positioning Universal Platform Operations team is responsible for 24/7/365 monitoring of the platform. Various tools and automation are employed to govern and actively report on the availability of the platform.

Operations Monitoring

Multiple data sources are monitored through tools and automation specifically employed for the Positioning Universal platform.

Positioning Universal provides the Platform Operations team with sensitive alerting surrounding an abnormal rise in data points that may include exception volume, resource dependency failures, and availability.

Positioning Universal captures time period trends automatically to draw an analysis of differing data points between “normal” and “abnormal” periods of performance.

Disaster Recovery

Positioning Universal implements suitable plans, measures and arrangements to ensure business continuity, including:

- Multi-location data center services
- Multiple source network providers (Data Centers)
- Availability of cloud backup storage.
- Multi-tiered, cloud-based monitoring (multiple sources, third party providers with built-in redundancies)
- Disaster recovery plans for server failure – enables switching to redundant hardware

Critical platform data assets are backed up daily to allow for in-place or new geo-region, based restoration. Geo-redundancies also exist for various infrastructure resources to support intra-zone within a region or regional datacenter failure. Furthermore, some resources have built-in redundant instances to take advantage of failover, supporting High Availability.

Confidentiality

Positioning Universal holds data protection, integrity, and confidentiality with the utmost importance. To ensure confidentiality, industry standard security controls are employed to prevent any data from being read, copied, transferred, or altered by unauthorized individuals.

In addition to the security controls, Positioning Universal does not collect personal information other than the user’s first and last name, email address, and an optional telephone number. This information is used only for Positioning Universal Platform accounts. No other personally identifiable information, personal health information or personal financial information is collected, stored, or processed.

Data in Transit

Encryption is enforced for all communications between platform components including the data pipelines. Transport Layer Security (TLS) is used with the minimum version being 1.2. All weak ciphers such as DES encryption are disabled where applicable.

Data at Rest

All storage containers that hold telemetry data and configuration information are encrypted when at rest. Industry standard encryption such as AES-256 is used to encrypt data at rest.

User Rights

Users of the Positioning Universal platform have the ability to view and correct the information the platform holds related to their login account. Also, Users can request that their account is deleted which will remove their information from the system permanently.

IoT Device Security

Internet of Things devices that connect to the Positioning Universal platform are required to use modern encryption and authentication mechanisms. In addition to the security controls enforced by the platform, Positioning Universal’ security measures provide manufacturers an additional layer of threat assessment which assists in reducing device-side risks.

Provisioning

All IoT devices that connect to and communicate with the platform are required to undergo a provisioning process. This is a two-step process:

1. All devices must be imported and whitelisted in the Positioning Universal Platform. Device information used for whitelisting comes directly from the device manufacturer and contains immutable device identification material.
2. All devices must be securely activated in the platform during the initial identification and authentication.

Authentication and Secure Communications

Device authentication is handled using industry standard cryptography. Positioning Universal supports two authentication mechanisms: token based using HMAC or mutually authenticated TLS.

All device communications with the platform are encrypted using TLS.

Risk Management

As part of Positioning Universal' risk management process, Positioning Universal continually performs threat modeling and security reviews.

Vulnerability Management

Positioning Universal uses advanced, cloud-based security features to secure its platform. Positioning Universal conducts systematic vulnerability testing (continuous scanning) on all its production servers to ensure that no potential security or privacy risks are created.

Positioning Universal' vulnerability testing occurs automatically on all production systems including servers, web applications, and containers. Positioning Universal' threat management system allows for 24/7 monitoring, threat modeling, and threat classification.

All authenticated scans are pre-scheduled to avoid service interruption, and no third-party port scans or annual penetration testing is allowed without the approval of Positioning Universal' management team.

Vulnerabilities requiring mitigation through patching follows Positioning Universal' patch management procedures, inclusive of:

- Dashboards identifying patch required (along with CVE/CVSS associated)
- Execution of patch (who is executing, specific patch, date performed, process to minimize production service interruptions, communication of maintenance windows)
- Follow-up reporting to affirm mitigated vulnerability

Anti-Virus / Anti-Malware

Positioning Universal ensure that its assets are protected against malware and spyware. Positioning Universal uses anti-virus and anti-malware programs to mitigate internet threats and remove them upon discovery. Positioning Universal' anti-malware program is capable of identifying and containing modern forms of malware.

Penetration Testing

Positioning Universal utilizes industry-recognized independent third-party services to conduct vulnerability assessments, configuration reviews, and penetration tests of networks, systems, applications and databases involved in the Positioning Universal Platform. Testing is performed annually.

Audits

Positioning Universal conducts periodic audits on its policies and internal processes associated with its platform security and infrastructure access. This includes incident response, patch management, user policy, and server monitoring. In addition, regular training on procedures and testing is conducted for all applicable employees.

Incident Management

Positioning Universal relies on an incident response lifecycle to determine strategic responses needed for each phase of an incident and allocates resources to the incident leading to resolution and accountability of the process. The end goal in Positioning Universal' IoT Cyber Security Incident Response is to preserve Positioning Universal' IoT assets by minimizing and avoiding system and data security losses.

Positioning Universal' Cyber Security Incident Response is based on the National Institute of Standards and Technology Special Publications (NIST SP) Subseries 800, Computer Security and are reviewed annually.

Vulnerability Disclosure

Positioning Universal considers the security of its systems a top priority. However, no matter how much effort put into system security, there can still be vulnerabilities present.

Should a vulnerability be discovered, steps can be taken to address it as quickly as possible. Positioning Universal asks for you to help us better protect our clients and our systems.

Please do the following:

- E-mail your findings to Positioning UniversalSecurity@Flex.com. Encrypt your findings using Positioning Universal' PGP key to prevent this critical information from falling into the wrong hands.
- Do not take advantage of the vulnerability problem you have discovered.
- Do not reveal the problem to others until it has been resolved.
- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties, and
- Do provide enough information to reproduce the problem so Positioning Universal will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be enough, but complex vulnerabilities may require further explanation.

Positioning Universal' promise:

- Positioning Universal will respond to your report within 3 business days with an evaluation of the report and an expected resolution date.
- Positioning Universal will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission.
- Positioning Universal will keep you informed of the progress towards resolving the problem.
- Positioning Universal will recognize researchers and their discoveries with a mention on the Positioning Universal Security web page unless they would like to remain anonymous.
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The amount of the reward will be determined based on the severity of the leak and the quality of the report.

Positioning Universal strives to resolve all problems as quickly as possible and would like to play an active role in the publication of the problem after it is resolved.

References

Description	Link
NIST SP 800-52	https://csrc.nist.gov/publications/detail/sp/800-52/rev-1/final
NIST SP 800-53	https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

Contact

Please direct your questions, feedback or any other information to support@positioninguniversal.com