1. Security Policy Overview.

1.1. ForgeRock's Commitment to Security. ForgeRock is committed to achieving and preserving the trust of our Customers, by providing a comprehensive security program that carefully considers data protection matters across our suite of products and services, including any Customer Data submitted by Customers to the ForgeRock Service.
1.2. Covered Services. This documentation describes the certifications held by ForgeRock, and the administrative, technical, and physical controls applicable to the ForgeRock Service. This documentation does not apply to free trial services made available by ForgeRock.
1.3. Architecture, Data Segregation, and Data Processing. The Service is operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The ForgeRock architecture provides an effective logical data separation for different customers via Customer-specific "Organization IDs" and allows the use of Customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, such as for testing and production. ForgeRock has implemented procedures designed to ensure that Customer Data is processed only as instructed by the Customer, throughout the entire chain of processing activities by ForgeRock and its sub-processors.

2. Security Controls and Information Security Management Program.

2.1. Security Controls. The Service includes a variety of configurable security controls that allow ForgeRock customers to tailor the security of the Service for their own use. ForgeRock personnel will not set a defined password for a user. Each Customer's users are provided with a token that they can use to set their own password in accordance with the applicable Customer's password policy. ForgeRock strongly encourages all customers, where applicable in their configuration of the Service's security settings, to use the multi-factor authentication features made available by ForgeRock.
2.2. Information Security Management Program. ForgeRock maintains a comprehensive Information Security Management System ("ISMS") program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of ForgeRock's business; (b) the amount of resources available to ForgeRock; (c) the type of information that ForgeRock will store and process; and (d) the need for security and protection from unauthorized disclosure of such Customer Data. The ISMS is documented and updated based on changes in legal and regulatory requirements related to privacy and data security practices and industry standards applicable to the Service and reviewed at least annually. ForgeRock's ISMS is designed to:

(a) Protect the integrity, availability, and confidentiality, of Customer data in ForgeRock's possession or control;
(b) Protect against any anticipated threats or hazards to the integrity, and availability, and prevention of unauthorized disclosure of Customer Data by ForgeRock or its agents;
(c) Protect against unauthorized access, use, alteration, or destruction of Customer Data;
(d) Protect against accidental loss or destruction of, or damage to, Customer Data; and
(e) Safeguard information as set forth in any local, state or federal regulations by which ForgeRock may be regulated.

2.3. Security Standards. ForgeRock's ISMS includes adherence to and regular testing of the key controls, systems and procedures of its ISMS to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing includes, but is not limited to, the following:

(a) Internal risk assessments;
(b) ISO27001; and
(c) AICPA Trust Services Criteria for Security, Availability, and Confidentiality per SOC 2 Report; and
(d) NIST guidance.

2.4. Security Audit Report. ForgeRock provides its Customers, upon their request, with a summary of ForgeRock's then-current external audit report such as the ISO27001, or, SOC 2 Report, including information as to whether the security audit revealed any material non-conformities in the ForgeRock Service.
2.5. Assigned Security Responsibility. ForgeRock assigns responsibility for the development, implementation, and maintenance of its ISMS, including:

(a) Designating a security official with overall responsibility; and
(b) Defining security roles and responsibilities for individuals with security responsibilities within ForgeRock.

3. Relationship with Sub-processors. ForgeRock conducts reasonable due diligence and security assessments of Sub-processors engaged by ForgeRock in the storing and/or processing of Customer Data ("Sub-processors"), and enters into agreements with Sub-processors that contain provisions similar or more stringent than those provided for in this security documentation.

1. Disciplinary Policy and Process. ForgeRock maintains a disciplinary policy and process in the event ForgeRock personnel violate the ISMS.

1. Access Controls.

5.1. Access Control Policies and Procedures. ForgeRock has in place policies, procedures, and logical controls that are designed:

(a) To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;
(b) To prevent personnel and others who should not have access from obtaining access; and
(c) To remove access in a timely basis in the event of a change in job responsibilities or job status.

Additionally, ForgeRock institutes:

(d) Controls to ensure that only those ForgeRock personnel with an actual need-to-know will have access to any Customer Data;
(e) Controls to ensure that all ForgeRock personnel who are granted access to any Customer Data are based on least-privilege principles;
(f) Controls to require that user identifiers (User IDs) shall be unique and readily identify ForgeRock person to whom it is assigned, and no shared or group User IDs shall be used for ForgeRock personnel access to any Customer Data; and
(g) Password and other strong authentication controls that are made available to ForgeRock customers, so that customers can configure the Service to be in compliance with NIST guidance addressing locking out, uniqueness, reset, expiration, termination after a period of inactivity, password reuse limitations, length, expiration, and the number of invalid login requests before locking out a user;

5.2. Physical and Environmental Security. Physical and environmental security controls are managed by Google as explained in https://www.google.com/about/datacenters/data-security/. ForgeRock Identity Cloud is fully deployed within the Google Cloud Platform.

5.3 Special Access by ForgeRock. If ForgeRock determines, in its reasonable discretion, that a Customer environment is impacting the availability or performance of the identity platform due to Customer's misconfiguration or a security incident, ForgeRock may use restricted Special Access accounts to access the relevant Customer environments. In the event ForgeRock need to enter a customer environment, ForgeRock shall use reasonable efforts to contact the Customer prior to any action being taken. ForgeRock reserves the right to effect access without customer consent when contact attempts fail and action is required to preserve service for one or more customers. In the event of a Special Access to a customer environment, the customer will receive a full report stating: (i) when access took place; (ii) what actions were taken, including any contact or exposure to customer data; and (iii) a post event review summarizing any impact on the customers environment and root cause analysis of the incident.

6. Data Encryption.

6.1. Encryption of Transmitted Data. ForgeRock uses Internet-industry-standard secure encryption methods designed to encrypt communications between its server(s) and the Customer browser(s), and between its servers and Customer's server(s).

6.2. Encryption of At-Rest Data. ForgeRock uses Internet-industry standard secure encryption methods designed to protect stored Customer Data at rest. Such information is stored on server(s) that are not accessible from the Internet.

6.3. Encryption of Backups. All backups are encrypted. ForgeRock uses disk storage that is encrypted at rest.

7. Disaster Recovery. ForgeRock maintains policies and procedures for responding to an emergency or a force majeure event that could damage Customer Data or production systems that contain such Customer Data. Such procedures include:

(a) Data Backups: A policy for performing periodic backups of production file systems and databases to meet the Recovery Point Objective described below;
(b) Disaster Recovery: A disaster recovery plan for the production environment designed to minimize disruption to the Service, which includes requirements for the disaster plan to be tested on a regular basis, currently four times a year;
(c) RPO / RTO: Recovery Point Objective is no more than two (2) hours and Recovery Time Objective is no more than one (1) hour;
(d) Business Continuity Plan: A process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

8. Secure Development Practices. ForgeRock adheres to the following development controls:

(a) Development Policies: ForgeRock follows secure application development policies, procedures, and standards that are aligned to industry-standard practices, such as the OWASP Top 10 and SANS Top 20 Critical Security Controls; and
(b) Training: ForgeRock provides employees responsible for secure application design, development, configuration, testing, and deployment appropriate (based on role) training regarding secure application development practices.

9. Data Integrity and Management. ForgeRock maintains policies that ensure the following:

(a) Segregation of Data: The Service includes logical controls, including encryption, to segregate Customer Data from that of other customers; and

(b) Back Up/Archival: ForgeRock performs full backups of the database(s) containing Customer Data no less than once per day and archival storage on no less than a weekly basis on secure server(s) or on other commercially acceptable secure media.

10. Vulnerability Management. ForgeRock maintains security measures to monitor the network and production systems, including error logs on servers, disks and security events for any potential problems. Such measures include:

(a) Infrastructure Scans: ForgeRock performs daily vulnerability scans on all infrastructure components of its production and development environments. Vulnerabilities are remediated on a risk basis. ForgeRock installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible;
(b) Application Scans: ForgeRock performs daily (as well as after making any major feature change or architectural modification to the Service) application vulnerability scans. Vulnerabilities are remediated on a risk basis. ForgeRock installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible;
(c) External Application Vulnerability Assessment: ForgeRock engages third parties to perform network and application vulnerability assessments and penetration testing on at least an annual basis ("Vulnerability Assessment"). Executive reports from ForgeRock's then-current Vulnerability Assessment, together with any applicable remediation plans, will be made available to customers on written request.

Vulnerabilities are remediated on a risk basis. ForgeRock installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible.

12. Penetration Testing
Customer may perform load testing that is representative of expected production volumes in the staging environment. Customer may perform penetration testing of their own environment in line with the requirements of the ForgeRock Identity Cloud Penetration Testing & Load Policy located at https://backstage.forgerock.com/docs/idcloud/latest/product-information/penetration-and-load-testing-policy.html;

11. Change and Configuration Management. ForgeRock maintains policies and procedures for managing changes to production systems, applications, and databases. Such policies and procedures include:

(a) A process for documenting, testing and approving the promotion of changes into production;
(b) A security patching process that requires patching systems in a timely manner based on a risk analysis; and
(c) A process for ForgeRock to perform security assessments of changes into production.

12. Secure Deletion. ForgeRock maintains policies and procedures regarding the deletion of Customer Data in compliance with applicable NIST guidance and data protection laws, taking into account available technology so that Customer Data cannot be practicably read or reconstructed. Customer Data is deleted from Google's Data Centers using secure deletion methods including digital shredding of encryption keys and hardware destruction in accordance with NIST SP800-88 guidelines as described in https://cloud.google.com/security/deletion/.

13. Intrusion Detection. ForgeRock monitors the Service generally for unauthorized intrusions using traffic and activity- based monitoring systems. ForgeRock may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug- ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to help customers detect fraudulent authentications, and to ensure that the Service functions properly.

14. Incident Management. ForgeRock has in place a security incident response plan that includes procedures to be followed in the event of any unauthorized disclosure of Customer Data by ForgeRock or its agents of which ForgeRock becomes aware to the extent permitted by law (such unauthorized disclosure defined herein as a "Security Breach"). The procedures in ForgeRock's security incident response plan include:

(a) Roles and responsibilities: formation of an internal incident response team with a response leader;
(b) Investigation: assessing the risk the incident poses and determining who may be affected;
(c) Communication: internal reporting as well as a notification process in the event of a Security Breach;
(d) Recordkeeping: keeping a record of what was done and by whom to help in subsequent analyses; and
(e) Audit: conducting and documenting a root cause analysis and remediation plan.

ForgeRock publishes system status information on the ForgeRock website. ForgeRock typically notifies customers of significant system incidents by email to the listed admin contact, and for availability incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and ForgeRock's response.

15. Security Breach Management.

15.1. Notification. In the event of a Security Breach, ForgeRock notifies impacted customers of such Security Breach without undue delay and, where required, within time limits defined by law. ForgeRock shall cooperate with the customer's reasonable request for information regarding such Security Breach, and ForgeRock provides regular updates on any such Security Breach and the investigative action and corrective action(s) taken.

15.2. No Acknowledgement of Fault by ForgeRock. ForgeRock's notification of or response to a Security Breach shall not be construed as an acknowledgement by ForgeRock of any fault or liability with respect to the Security Breach.

15.3 Remediation. In the event of a Security Breach, ForgeRock, at its own expense shall:

(i) investigate the actual or suspected Security Breach

(ii) where a breach impacts a customer, provide any affected customer with a remediation plan, to address the Security Breach and to mitigate the incident and reasonably prevent any further incidents,

iii) remediate the effects of the Security Breach in accordance with such remediation plan, within ForgeRock's scope of control and

(iv) reasonably cooperate with any affected customer and any law enforcement or regulatory official investigating such Security Breach.

16. Logs. ForgeRock provides procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports. ForgeRock: (i) backs-up logs on a daily basis, (ii) implements commercially reasonable measures to protect such logs from unauthorized modification or erasure, and (iii) retains such logs in compliance with ForgeRock's data retention policy. If there is suspicion of inappropriate access to the Service, ForgeRock has the ability to provide customers log entry records to assist in forensic analysis.

17. Human Resources Security

17.1 Employee Selection

To the extent reasonable, and permissible under Applicable Law, ForgeRock shall where appropriate, conduct, have conducted or otherwise require, background checks proportionate to the role for ForgeRock personnel performing services under the Agreement including professional references and criminal background checks.

17.2 ForgeRock Personnel Security Management

17.2.1 ForgeRock shall maintain an acceptable use policy governing the use of computing resources including, without limitation, all ForgeRock Systems, that is communicated to appropriate ForgeRock Personnel.

17.2.2 ForgeRock shall require ForgeRock personnel performing services under the Agreement to maintain valid non-disclosure obligations or other confidentiality agreements as deemed reasonably necessary by ForgeRock.

17.3 ForgeRock personnel Termination and Separation

17.3.1 ForgeRock shall have a process that governs the secure return of ForgeRock Systems and Customer Confidential Information for separated ForgeRock personnel.

17.4 Training and Awareness

17.4.1 ForgeRock shall require that all ForgeRock personnel complete upon hire and, at least annually thereafter, ForgeRock's security awareness training including awareness of ForgeRock's related policies and maintain records of such training completion.