FORGEROCK

ForgeRock Security Schedule for On Premise Customers

This Information Security Requirements Exhibit X (this "Exhibit") is incorporated into the agreement between ForgeRock and the entity identified in the applicable Order Form ("Customer") that governs Customer's use of the ForgeRock Software or Services (the "Agreement"). To the extent the terms and conditions of this Exhibit conflict with the terms or conditions in the Agreement, the terms of this Exhibit shall control unless expressly stated otherwise. Capitalized terms used but not otherwise defined herein shall have the meanings ascribed to them in the Agreement.

1 Defined Terms

1.1 Definitions

1.1.1 As used in this Exhibit, "Applicable Law" means all legal, regulatory or industry requirements applicable to performance under the Agreement or ordering document including the data protection or privacy laws of any applicable jurisdiction.

1.1.2 "Commercially Reasonable Efforts" means, in addition to the implied duty of good faith and fair dealing, at least those diligent measures that people experienced in the relevant subject area would generally regard as sufficient to constitute reasonable diligence for regulated financial institutions in relevant circumstances. In no circumstance shall techniques, tools or protocols publicly known to be deprecated or otherwise compromised be considered reasonable or secure under this definition.

1.1.3 "Disaster" means any sudden, unplanned catastrophic event that compromises ForgeRock's ability to provide the Services including, without limitation, any other critical functions, processes, or services for some unacceptable period of time causing ForgeRock's management to invoke their recovery plans.

1.1.4 "Disaster Recovery" means the collection of resources and activities to re-establish the delivery of the Services and the recovery and restoration of data lost by reason of the Disaster.

1.1.5 "ForgeRock System" means any physical or electronic system including, without limitation, applications, information stores, and infrastructure systems, used for storing, processing, or transmitting Customer Confidential Information.

1.1.6 "Intrusion Detection System" or "IDS" means any ForgeRock System that monitors a network or systems in real time for malicious activity or policy violations with such malicious activity or violations being reported either to an administrator or collected centrally using a security information and event management (SIEM) system that combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

1.1.7 "Malware" means software programs designed to damage or perform other unwanted actions to or within any ForgeRock Systems. Such examples may include viruses, worms, Trojan horses, keystroke loggers and spyware.

1.1.8 "Multi-Factor Authentication" or "MFA" means authentication through verification of at least two of the following types of authentication factors: (i) knowledge factors, such as a username/password, or (ii) possession factors, such as token or text message on a mobile device, or (iii) inherence factors, such as a biometric characteristic.

1.1.10 "Recovery Point Objective" or "RPO", also referred to as the "Maximum Data Loss", means the targeted point in time from which it is necessary to recover Customer data in ForgeRock's infrastructure and systems, and quantifies and the permissible amount of such data loss following an interruption caused by a Disaster, measured in hours.

1.1.11 "Recovery Time Objective" or "RTO" means the targeted elapsed time between the point of the interruption of the Services caused by a Disaster up to the point where the Services must be acceptably functional to Customer, measured in hours.

1.1.12 "Risk-Based Authentication" or "RBA" means any non-static authentication system which detects anomalies or changes in the normal use patterns of an individual and requires additional verification of the individual's identity when such deviations are detected, such as using challenge questions.

1.1.13 "Security Incident" means any actual or reasonably suspected misuse, compromise, or unauthorized, accidental or unlawful acquisition, destruction, loss, alteration, disclosure, or access to Customer Confidential Information under the possession, custody, or control of ForgeRock Personnel including any circumstance pursuant to which Applicable Law requires either notification to be given to affected parties or other activity in response to such circumstance.

1.1.14 "Site" means any physical premise or ForgeRock Systems utilized by ForgeRock Personnel in performance of Services under the Agreement.

1.1.15 "Site Visit" means the physical or other access to Sites by Customer personnel, each a "Site Visitor".

1.1.16 "

1.1.17 "Customer Confidential Information" means any data that is stored by ForgeRock on behalf of a customer within ForgeRock Systems during the fulfilment of a contract.

2 Information Management and Risk Management

2.1 Information Security Program

2.1.1 ForgeRock shall have and maintain a holistic information risk management program that complies with Applicable Law, incorporates reasonable and appropriate administrative, operational, technical, physical and organizational measures that are designed to preserve and protect the confidentiality, integrity and availability of Confidential Information. This program shall identify the organization's critical information, the threats associated with such information and maintain documented controls designed to mitigate anticipated risks for the same.

FORGEROCK

3 Access Control

3.1 ForgeRock Management of Access Control to ForgeRock Systems

3.1.1 For user accounts managed by ForgeRock that grant access to ForgeRock Systems that require material changes to such access, ForgeRock shall effect such changes in a timely manner.

3.1.2 For user accounts managed by Customer and utilized by ForgeRock Personnel that grant access to Customer ForgeRock Systems, ForgeRock shall notify the appropriate Customer security and access administration personnel of material changes to such access in a timely manner.

3.2 Encryption of Customer Confidential Information

3.2.1 ForgeRock shall use Commercially Reasonable Efforts to ensure that Customer Confidential Information is encrypted at rest and in transit.

3.3 Multi-Factor Authentication

3.3.1 For access to cloud-based or hosted ForgeRock Systems containing Customer Confidential Data, ForgeRock Systems shall, where possible, support Multi-Factor Authentication as a requirement for logon.

4 Incident Response Policy and Management

4.1 Response and Reporting

4.1.1 ForgeRock shall maintain an incident response plan and an incident response team with defined roles and responsibilities that are each periodically reviewed and authorized by appropriate management.

4.1.2 ForgeRock shall use Commercially Reasonable Efforts to anticipate, detect, evaluate, and respond to a Security Incident in a timely manner.

4.2 Incident Management and Forensics

4.2.1 ForgeRock shall use Commercially Reasonable Efforts to maintain relevant documentation related to Security Incidents including issues, outcomes, and remediation activities.

4.2.2 ForgeRock shall use Commercially Reasonable Efforts to maintain the integrity and chain of custody of relevant information related to Security Incidents and ensure that such information is preserved in a manner consistent with Applicable Law.

5 Secure Operations

5.1 Operational Management

FORGEROCK

5.1.1 ForgeRock shall use Commercially Reasonable Efforts to physically or logically segregate Customer Confidential Information from other non-Customer data within ForgeRock Systems.

5.1.2 ForgeRock shall use Commercially Reasonable Efforts to physically or logically segregate production, test and development Systems for which ForgeRock is responsible unless agreed to otherwise in writing by the Parties prior to such use.

5.1.3 ForgeRock Systems used in the provision of Support Services shall be securely configured, maintained, and retired from use using Commercially Reasonable Efforts and incorporating, to the extent applicable, any legal, regulatory, and compliance requirements deemed necessary by ForgeRock in ForgeRock's reasonable judgment.

5.2 Anti-Malware

5.2.1 ForgeRock shall have an anti-Malware policy that requires Malware-detection software to be installed and enabled on ForgeRock Systems that interact with Customer Confidential Information and prohibits disabling such anti-Malware controls without appropriate authorization.

5.2.2 ForgeRock Systems shall be configured to automatically check for and automatically implement new anti-Malware signatures on a reasonable frequency.

5.3 Vulnerability and Patch Management

5.3.1 ForgeRock shall use Commercially Reasonable Efforts to maintain effective vulnerability and patch management processes for ForgeRock Systems.

5.3.2 ForgeRock shall use Commercially Reasonable Efforts to evaluate and effect appropriate remediation activities including the timely application of patches to impacted ForgeRock Systems in a risk-prioritized manner informed by such vulnerability detection processes.

5.4 Logging and Monitoring

5.4.1 ForgeRock shall use Commercially Reasonable Efforts to log user actions related to ForgeRock Systems with the following requirements: (i) user and administrative actions, (ii) account privilege changes, (iii) all access attempts, (iv) configuration changes, (v) access to Customer Confidential Information, and (vi) changes to firewall and network access control systems.

5.4.2 Such logs for shall be retained for an appropriate length of time and at least for the minimum retention period under Applicable Law and readily available for review by appropriate ForgeRock Personnel.

5.5 Intrusion Detection Systems (IDS)

5.5.1 Using Commercially Reasonable Efforts, for ForgeRock networks through which Customer Confidential Information traverses, ForgeRock shall utilize Intrusion Detection Systems and regularly update IDS signatures based on new threats which shall be applied in a timely risk-prioritized manner.

6 Remote Access to Internal Customer ForgeRock Systems

6.1 Administrative Requirements for Remote Access

6.1.1 ForgeRock shall require that remote users have valid non-disclosure obligations or other confidentiality agreements in force for such personnel prior to allowing such remote access.

6.1.2 ForgeRock shall maintain reasonable oversight of ForgeRock Personnel's use of such access.

6.1.3 Upon reasonable request, ForgeRock shall make available to Customer a complete list of ForgeRock Personnel accounts that have remote access privileges to Customer Systems.

6.1.4 Upon request by Customer, ForgeRock Personnel that have remote access to Customer Systems shall have confidentiality obligations which shall be acknowledged by signature.

6.1.5 Privacy training and information security training shall be completed by ForgeRock Staff prior to performance of Services and as required thereafter.

6.2 Technical Requirements for Remote Access

6.2.1 ForgeRock shall establish such connections through a mutually agreed facility between Parties and shall originate from ForgeRock's approved IP addresses and only through the use of ForgeRock's appropriately managed and approved devices.

6.2.2 ForgeRock shall utilize Commercially Reasonable Efforts to maintain the security of its ForgeRock Systems establishing such remote connections by appropriately applying the latest applicable security patches in a timely and risk-prioritized manner.

7 Disposal, Return and Retention of Customer Confidential Information

7.1 Disposal Requirements for Customer Confidential Information

7.1.1 Except as otherwise specifically required by Applicable Law or permitted by this Agreement, upon termination or expiration this Agreement and Customer's written request, or upon the reasonable written request of Customer, ForgeRock shall sanitize in a manner designed to make forensically unrecoverable by standard forensic technologies, using Commercially Reasonable Efforts, all Customer Confidential Information from all ForgeRock Systems, data retentive devices or any other media containing such Customer Confidential Information.

7.1.2 If ForgeRock discards or otherwise discontinues its use of media utilized at any time for the storage or processing of Customer Confidential Information, such media shall

be made forensically unrecoverable in accordance with the relevant terms of such obligations as such obligations are set forth in the Agreement including this Exhibit.

7.1.3 Upon written request by Customer, ForgeRock shall represent its performance of applicable secure disposal obligations (e.g., NIST800-88 guidelines) by providing written attestation to appropriate Customer personnel in a timely manner. Notwithstanding any other provisions in the Agreement, Customer shall retain the right to assess, to its satisfaction, ForgeRock's performance of ForgeRock's secure data disposal obligations as such obligations are set forth in the Agreement and this Exhibit.

7.2 Return of Customer Confidential Information

7.2.1 Upon request by Customer, ForgeRock shall return copies of any Customer Confidential Information in its custody, including in printed or physical form, to Customer in a format deemed usable by Customer.

7.3 Retention of Customer Confidential Information

7.3.1 Each Party shall be entitled to retain copies of the other Party's Confidential Information as may be required by the Party's record retention policy, audit requirements, or otherwise required to comply with Applicable Law, court order, warrant, subpoena, or other valid request carrying the force and effect of law, provided that (a) further processing, use or disclosure of such Confidential Information is limited to the purpose described in this Section and for no other purpose, (b) during such retention each Party agrees to treat such Confidential Information in accordance with the terms of the Agreement, and (c) such Confidential Information shall be retained only for such period as required by the purpose for which such Confidential Information was retained, as set forth in this Section and promptly returned, rendered permanently inaccessible, or destroyed in accordance with this provision upon the expiration of retention requirement. In no event shall ForgeRock withhold any Customer Confidential Information as a means of resolving any dispute between the Parties.

8 Information Contingency

8.1 Backup and Recovery

8.1.1 ForgeRock shall have policies and procedures for governing backup media that contain Customer Confidential Information which provide that:

8.1.1.1 Customer Confidential Information shall be retained for such period stipulated in the Agreement or other governing written agreement between Parties;

8.1.1.2 Such backups and replicas of data stores shall be treated with the same care and control as the stores in which such original information resides;

8.1.1.3 Access to such backup media shall be restricted to formally authorized ForgeRock Personnel and its access logged.

8.2 Business Continuity and Disaster Recovery Planning

8.2.1 ForgeRock's provision of Support Services shall be subject to an approved Business Continuity and Disaster Recovery (BC/DR) plan which is regularly reviewed by appropriate management.

8.2.2 To the extent applicable, such BC/DR plan(s) shall contain an appropriate strategy to meet the recovery objectives of Customer Confidential Information or the Services.

8.3 Business Continuity and Disaster Recovery Plan Requirements

8.3.1 The Business Continuity and Disaster Recovery (BC/DR) plan shall:

8.3.1.1 Include a mechanism designed to ensure the confidentiality, integrity, and availability of Customer Confidential Information during a Disaster;

8.3.1.2 For Support Services, meet the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) mutually agreed between Parties, but in no case longer than 48 hours for RTO and 12 hours for RPO unless otherwise specified in the Agreement or relevant Ordering Document;

8.3.1.3 Identify the technical and non-technical recovery actions and requirements that ForgeRock needs to perform when a Disaster is declared and when a recovery plan is executed; and

8.3.1.4 Identify the restoration procedure to switch production operations between primary and recovery sites and provide the corresponding validation process for such procedure.

8.3.2 Notwithstanding anything to the contrary in the Agreement, a *force majeure* event shall not excuse ForgeRock from its performance of its Disaster recovery obligations under ForgeRock's BC/DR plan or as such obligations are set forth herein.

8.4 Testing Requirements

8.4.1 ForgeRock shall conduct appropriately scoped BC/DR tests at least annually and address findings related to its performance of the BC/DR plan as they relate to the recoverability of Customer Confidential Information to meet the specified recovery objectives.

8.4.2 Upon request from Customer, ForgeRock shall provide to Customer a report, in a mutually agreeable format, after such relevant recovery exercises, that identifies the findings related to the recoverability of Customer Confidential Information and ForgeRock's actions, taken and planned, to address such findings.

8.4.3 Upon Customer's reasonable request, ForgeRock shall reasonably cooperate with any continuity risk or business impact analysis conducted by Customer to the extent applicable.

8.4.4 In lieu of the provisions contained hitherto in this Exhibit, upon Customer's reasonable request, ForgeRock shall furnish to Customer such relevant third-party reports that sufficiently demonstrate assurance of the design and effectiveness of such testing and recoverability provisions to Customer's satisfaction.

FORGEROCK

9 Secure Development

9.1 Application Development Requirements

9.1.1 ForgeRock shall have and comply with a secure software development life cycle (SDLC) process that governs the development, testing, and maintenance of all applications used by Customer for storing, processing, or transmitting Customer Confidential Information or that comprise a component of the Service.

9.1.2 For such applications, threat modeling, including identification of threats during design, and application security testing, including code scanning and manual penetration testing, shall be conducted for each major code release.

9.1.3 ForgeRock's application development and maintenance processes shall provide for continual testing of vulnerabilities within such applications with a commitment to provide patches on a schedule commensurate with the perceived risk associated with such corresponding vulnerabilities without adversely impacting the availability of related ForgeRock Systems.

9.1.4 To the extent ForgeRock utilizes open-source software on ForgeRock Systems or to deliver the Services, ForgeRock shall perform security due diligence activities using Commercially Reasonable Efforts with respect to the selection, acquisition, and maintenance of such open-source software to ensure appropriate risk mitigation practices including, without limitation, the application of timely security patching and vulnerability management oversight.

10 Human Resources Security

10.1 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.

10.2 ForgeRock Personnel Security Management

10.2.1 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.

10.2.2 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.

10.3 ForgeRock Personnel Termination and Separation

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

FORGEROCK

10.4 Training and Awareness

10.4.1 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.

11 Compliance and Reporting

11.1 Regulatory Compliance

11.1.1 ForgeRock shall use Commercially Reasonable Efforts to comply with Applicable Law. Such compliance efforts shall be designed, managed, and regularly evaluated for effectiveness by qualified ForgeRock Personnel.

11.2 External Information Security Assessment and Certifications

11.2.1 Using Commercially Reasonable Efforts, ForgeRock shall have a reputable third party conduct an information security assessment upon the introduction of a new product or service, and for every major change to an existing product or service.

11.2.2 Up to once annually upon Customer's request, ForgeRock shall make available, and all information reasonably necessary to demonstrate compliance with its privacy, compliance, and information security obligations under the Agreement and this Exhibit. Such information may include Customer's information security questionnaire, SOC 2 Type II, ISO 27001 or other relevant compliance reports or certifications including high-level reports, in a mutually agreeable format, of external information security assessment findings to the extent such findings relate to ForgeRock Personnel's ability to safeguard Customer Confidential Information applicable to ForgeRock's performance of its obligations under the Agreement.

ForgeRock shall use Commercially Reasonable Efforts to correct any material control deficiencies identified through such examinations, as described in this Exhibit, in a timely risk-prioritized manner.