ForgeRock Identity Cloud Acceptable Use Policy

This Acceptable Use Policy ("**AUP**") describes activities that are prohibited on the ForgeRock Identity Cloud. The aim of the AUP is for the protection of ForgeRock, its representatives, services and customers.

1. Abuse. Customer shall not, directly or indirectly, and may not authorize any third party to use the ForgeRock Identity Cloud to engage in, foster, promote or solicit unlawful, illegal, fraudulent, infringing, invasive, defamatory, irresponsible or abusive behaviour. This includes but is not limited to:

a. Conduct that is likely to breach any applicable laws, codes or regulations applicable to the parties or others;

b. Allowing unauthorised use or access to, monitoring of, or interference with the ForgeRock Identity Cloud;

c. Collecting, transmitting or using information, or distributing software which covertly gathers or transmits information about a user; or

d. Use of the ForgeRock Identity Cloud in a way that unnecessarily interferes with the normal operation of the ForgeRock Identity Cloud or the equipment or systems used by ForgeRock to provide the ForgeRock Identity Cloud.

2. High-Risk Activities, HIPAA, and PCI. Customer shall not, directly or indirectly, and may not authorize any third party to use the ForgeRock Identity Cloud to:

a. Conduct any High-Risk Activities, defined as uses such as the operation of nuclear facilities, air traffic control or other transportation systems, or life support systems, where the use or failure of the ForgeRock Identity Cloud could lead to death, personal injury, or environmental damage; or

b. Process any personal health information or information including any data that may be subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), unless Customer and ForgeRock execute an Order Form for the relevant Identity Licenses that includes or references the relevant Business Associate Agreement; or

c. Process any payment or credit card information or information that may be subject to Payment Card Industry standards.

Customer shall ensure that the data identified above is not processed by the ForgeRock Identity Cloud or otherwise provided to ForgeRock. In the event that such data is processed by the ForgeRock Identity Cloud or provided to ForgeRock, Customer shall be responsible for any costs associated with identifying and removing such data, and to the extent applicable Customer shall indemnity ForgeRock pursuant to the terms and conditions of the Agreement.

3. Web and Mail Requirements. For any emails sent by Customer using the ForgeRock Identity Cloud or for any web site interface into the ForgeRock Identity Cloud, Customer shall:

a. Post a Privacy Notice to end users of the ForgeRock Identity Cloud that complies with Applicable Law.

b. When emailing ensure that the appropriate lawful basis for communications exists with the intended recipient and that records of the lawful basis have been created. This includes but is not limited to Consent, Opt in or Opt out records;

c. Provide a clear notice stating where to address complaints or correspondence regarding use of the ForgeRock Identity Cloud or receipt of emails generated by the ForgeRock Identity Cloud;

d. Not engage in any mass email, promotions, advertising or spam using the ForgeRock Identity Cloud that is contrary to Applicable Law.

4. Breach of this AUP. If Customer breaches the terms and conditions set forth in this AUP, including Customers unintentional failure to use reasonable security measures or as a result of authorised or unauthorised access by third parties related to Customer with or without Customer knowledge, then ForgeRock may suspend or terminate Customer's access to the ForgeRock Identity Cloud as set forth in the Agreement. No credit or remedy under any service level agreement for interruption of service is available for AUP breach.