Service Description
for
Governance & Lifecyle Cloud Service

*** IMPORTANT INFORMATION – PLEASE READ CAREFULLY ***

The use of the Governance & Lifecyle ("G&L") Cloud Service described herein is subject to and expressly conditioned upon acceptance of the: (i) Terms of Service between RSA and Customer or, if the parties have no such agreement in place, the Terms of Service for RSA Cloud Offerings currently located at https://www.rsa.com/standard-form-agreements/ (the "Terms of Service"); (ii) the Data Processing Addendum for RSA Cloud Offerings located at https://www.rsa.com/standard-form-agreements/ (the "DPA), and (iii) the applicable ordering document covering Customer's purchase of a subscription or subscriptions to the G&L Cloud Service from RSA or an RSA authorized reseller, the terms of which are incorporated herein by reference (such Terms of Service, DPA, ordering document, and this Service Description are, collectively, the "Agreement").

This Service Description is a legally binding document between you (meaning the individual person or the entity that the individual represents that is purchasing subscriptions to the G&L Cloud Service for its internal use and not for outright resale ("Customer")) and RSA (which means (i) RSA Security USA LLC, if Customer is located in the UnitedStates, Mexico or South America; (ii) the local RSA sales affiliate if Customer is located outside United States, Mexicoor South America and in a country in which RSA has a local sales affiliate; or (iii) RSA Security & Risk Ireland Limited or other authorized RSA entity as identified on the RSA quote or other RSA ordering document if Customer is located outside the United States, Mexico, or South America and in a country in which RSA does not have a local sales affiliate). Unless RSA agrees otherwise in writing, this Service Description and the Agreement governs Customer's use of the G&L Cloud Service except to the extent all or any portion of the G&L Cloud Service is subject to a separate written agreement set forth in a quotation issued by RSA.

By proceeding with the use of the G&L Cloud Service or authorizing any other person to do so, you are representing to RSA that you are (i) authorized to bind the Customer; and (ii) agreeing on behalf of the Customer that the terms of the Agreement shall govern the relationship of the parties with regard to the subject matter of the Agreement and are waiving any rights, to the maximum extent permitted by applicable law, to any claim anywhere in the world concerning the enforceability or validity of the Agreement. If you do not have authority to agree to the termsof this Service Description or the Agreement on behalf of the Customer, or do not accept the terms of this Service Description on behalf of the Customer, immediately cease any further attempt to use the G&L Cloud Service for any purpose.

This Service Description governs the provision by RSA of the RSA cloud offering known as "G&L Cloud Service" to which Customer has purchased a valid subscription, therefore. Notwithstanding anything to the contrary in the Agreement, in the event of a conflict between the Terms of Service and/or ordering document and this Service Description, the terms of this Service Description shall prevail solely with respect to the subject matter hereof. Capitalized words used in this Service Description and not expressly defined herein will have the meaning stated in the Agreement.

Service levels and operational procedures are standardized for all customers.

1. DEFINITION

1.1 "**Applicable Laws**" means all applicable local, state, national, and foreign laws, treaties, and regulations, including but not limited to, those related to data privacy, international communications, and the transmission of technical or personal data.

1.2 **"Content"** means User Attributes and any other data, materials, or information uploaded by Customer into the Service Offering, but not including any Sensitive PII.

1.3 "**Personal Information**" means any information that could directly or indirectly identify an individual.

1.4 "**Sensitive PII**" means any Personal Information that is "sensitive" by nature or deemed "sensitive" by any Applicable Laws (such as social security numbers, credit card data, drivers' license numbers, national ID numbers, bank account numbers, and health/medical information).

1.5 "**Service Offering**" means the G&L Cloud Service.

1.6 "**Term**" means the term of Customer's subscription to the G&L Cloud Service as set forth in the applicable ordering document.

1.7 "**User**" means Customer's employees, contractors, partners, and/or other individuals whose access to Customer's network and applications will be managed by the Service Offering.

1.8 "**User Attributes**" means the following information, but not limited to, regarding each User: first name, last name, email address, title, and unique identifier.

2. SCOPE OF SERVICES.

During the Term, RSA will provide Customer with access to and use of the Service Offering via the internet in accordance with the service levels set forth in Exhibit 1 hereof and as further described therein. Customer's access anduse of the Service Offering will be subject to all those restrictions stated in the Agreement.

3. SERVICE OFFERING.

The Service Offering delivers a cloud-hosted Identity Governance and Administration platform and operational services providing for, among other things:

- Visibility and insights across cloud and on-premises applications to help ensure appropriate levels of User access and quickly address risky access;
- Ensuring appropriate User access with access reviews & certification campaign management for compliance adherence;
- Removing inappropriate User access and reduce risks by implementing access and segregation of duty policies;
- Automatically and cost-effectively provisioning and de-provisioning User access in a timely fashion using Joiner-Mover-Leaver policies;
- A simple, easy to use access requests and approval process for Users; and
- Ensuring User access alignment and simplification of access for reviews, requests, and polices leveraging role mining and management.
- Deployed as a single or multi-tenant cloud environment to ensure versatility in Customer cloud offerings.

The Service Offering is offered in different package levels – small, medium and large tiers. Customer's accepted orderfor the Service Offering will state which package (tier) has been selected by Customer.

Supplemental Software provided with the Service Offering is governed by the End User License Agreement located at https://www.rsa.com/standard-form-agreements/. Supplemental Software will be listed on the applicable ordering document.

4. ACCOUNT ACCESS.

RSA will deliver to Customer Login Credentials ("**Account Access Information**") necessary for Customer to access the Service Offering in accordancewith the Agreement. Thereafter, Customer will create and manage Login Credentials for each authorized user of the Service Offering. Customer is responsible for all activity occurring under such Account Access Information and shall abide by all Applicable Laws in connection with Customer's use of the Service Offering.

5. CUSTOMER RESPONSIBILITIES.

Customer will provide RSA with the cooperation, access, and detailed information reasonably necessary for RSA to implement and deliver the Service Offering, including, where applicable, one (1) employee who has substantial computer system, network management, and project management experience satisfactory to RSA to act as project manager and as a liaison between RSA and Customer. RSA will be excused from its failure to perform any obligationunder this Service Description to the extent such failure is caused by Customer's delay or failure to perform its responsibilities under this Agreement. Customer shall use reasonable and appropriate safeguards to protect its Content.

6. CUSTOMER ATTRIBUTES.

RSA only requires access to User Attributes in order to provide the Service Offering to Customer. While Customer may elect to upload additional Content into the Service Offering other than User Attributes, no other Personal Information is required in order for the Customer to access or use the Service Offering. Customer acknowledges and agrees that it shall not provide to RSA or upload into the Service Offering any Sensitive PII. During the Term, Customer grants to RSA a limited, non-exclusive license to use Content solely for all reasonable and necessary purposes contemplated by this Service Description and for RSA to provide the Service Offering. Customer, not RSA, shall havesole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness and intellectual property ownership or right to use of all Content. RSA shall use reasonable and appropriate administrative, technical and physical safeguards to protect the security, integrity and confidentiality of Content. However, for clarity, Customer acknowledges and agrees that: i) the Service Offering is not intended or designed to securely host and store any Sensitive PII, and ii) Customer shall not modify or use the Service Offering to store any such Sensitive PII or provide RSA with access to any Sensitive PII.

7. RSA OBLIGATIONS.

A. General

RSA is committed to maintain and continually improve cyber/information security to meet our responsibilities to our

customers and regulators and to reduce operational loss, or reputational damage through cloud infrastructure provider, supply and maintain adequate heating/cooling; electrical power; server hardware; network infrastructure and bandwidth; physical security and access controls; and professional fire detection/suppression capability necessary to provide the Service Offering.

B. Security Best Practices

Security industry best practices will be followed as noted in Exhibit 2, which shall follow the following domains:

1.1 Protect

RSA incorporates continual improvement in security policies, controls and processes to enable the confidentiality, integrity and availability of the Service Offering. We foster a strong security culture with establishment of a proactivesecurity posture against cyber threats by influencing internal and external stakeholders (including their third party vendors) to manage evolving threats.

1.2 Detect

RSA ensures security defenses are continuously assessed, monitored, and tested to remain effective and detect cyber security events affecting, or with the potential to affect the Service Offering.

1.3 Respond

RSA follows a consistent and effective approach that guarantees the constant detection of incident, respond to, and manageeffects of any actual or suspected security incidents relating to information systems, including communication on security events and weaknesses.

1.4 Recover

RSA ensures continual preparedness and improvement for the recovery and restoration of the major services in a timely manner to maintain business functions in the event of major disruption or during adverse situations.

C. Maintain

During the Term, RSA reserves the right for Application Upgrades to make modifications, including upgrades, patches, revisions or additions to the Service Offering subject to the terms set forth in Exhibit 1.

8. TERM

The Term shall be specified in the Customer's accepted Order for the Service Offering, and subject to the Terms of Service for RSA Cloud Offerings currently located at https://www.rsa.com/standard-form-agreements/.

9. DATA CAPS

Customer shall be subject to a limit on data usage (the "Data Cap"). The Data Cap shall be 500GB of data for production instances of G&L and 300GB of data for development instances. Customer acknowledges and consents that, upon reaching 90% of the Data Cap, RSA will increase Customer's Data Cap by 500GB increments and bill Customer accordingly. If proper payment is not made for increased Data Caps within thirty (30) days of invoice date, RSA shall have the right to disable Services until payment is made.

10. SUPPLEMENTAL SOFTWARE.

10.1 Mobile Lock. RSA Mobile Lock detects critical threats to a mobile device and restricts the user's ability to authenticate until the threat issue is resolved. It allows IT to establish trust by verifying mobile devices across the attack surface, systematically protecting against threats, and securing any device to mitigate those threats. With RSA Mobile Lock, IT can investigate a threat without delay, preventing risk while the issue is being resolved. As more people increasingly rely on personal devices to authenticate, RSA Mobile Lock helps manage device security in real time and maintain the security of the RSA mobile app they rely on to authenticate.

10.2 Risk AI. Risk AI is a multifactor authentication add-on that strengthens ID Plus and password-based systems by applying knowledge of the client device and user behavior to assess the potential risk of an authentication request. If the assessed risk is high, the user is challenged to further confirm his or her identity. The highest level of dynamic risk-based authentication adds in machine learning algorithms to allow for a self-enhancing security environment that learns to identify threats and risks common to a specific customer's environment over time.

10.3 Web Proxy. Web Proxy is a trusted connection method that allows ID Plus to protect applications that do not support SAML and do not contain the sign-in forms required to configure HTTP Federation. These are internally developed applications (by Customer) that did not previously restrict access by requiring sign-in credentials. Our Web Proxy offering allows for these applications to be protected as a part of ID Plus.

10.4 ID Verification. ID Verification is designed to support remote and hybrid work environments by providing a seamless and secure digital onboarding experience. As part of RSA My Page, our identity verification solution integrates through an application connector to identity verification vendors such as ID Dataweb, ensuring high assurance and efficiency. With a no-code, standards-based configuration, it's an ideal tool for IT and security leaders to streamline operations and enhance security.

EXHIBIT 1
CLOUD SERVICE LEVELS

I. SERVICE LEVELS FOR PRODUCTION INSTANCE.

This Section I of Exhibit 1 applies to Customer's Production Instance of the Service Offering. For purposes of this Exhibit 1, "**Production Instance**" means solely Customer's production instance of the Service Offering's cloud computing environment. The Production Instance shall have 99.5% or higher Availability on a monthly basis (the "**Production Availability Standard**"), calculated as set forth below. "**Availability**" means, subject to the exclusionsbelow, solely the availability of the cloud components of the Service Offering and does not apply to any componentsof the Service Offering that are not delivered by RSA over the internet as part of the Service Offering (e.g., SupplementalSoftware) or other RSA products, software, services, solutions, maintenance, or support services.

A. PRODUCTION INSTANCE INTERRUPTIONS.

1. **Measurement.** Production Downtime, as defined below, is measured from the RSA-confirmed commencementtime of a Production Downtime event to the time the Production Instance is operational.
2. **Exclusions.** Unavailability of the Production Instance shall not be considered Production Downtime to the extentthat it is caused by one or more of the following factors:
   (i) Customer's or any of its user's actions or inactions (e.g., inadvertently turning off Customer's access to the Service Offering);
   (ii) Customer's failure to perform any of its obligations under the Agreement;
   (iii) Routinely Scheduled Maintenance, Service Updates or Emergency Maintenance. "EmergencyMaintenance" means unscheduled or emergency maintenance. Total maintenance not to exceed 900 minutes per month;
   - **Routine Maintenance -** Service update maintenance window, as published, for non-featured enhancements such as bugfixes, security updates and platform maintenance. These updates are routine, and no advanced notice is provided.
   - **Service updates -** Notifications will be provided at least 14 days inadvance.
   - **Emergency Maintenance -** Notifications will be provided at least 24 hours in advance for any emergency maintenance.

   (iv) Issues with or lack of network connectivity between the IT systems of Customer to the Service Offering.
   (v) The written request or consent by Customer's representative to interrupt the Production Instance; and
   (vi) Force Majeure Events which shall mean strikes, riots, insurrection, terrorism, fires, natural disasters, actsof God, war, governmental action, cyberattacks, pandemics, epidemics, or any other cause which is beyond the reasonable control of RSA.

RSA shall be solely responsible for establishing the extent to which Production Downtime is caused by one or more of the above factors.

B. PRODUCTION INSTANCE SERVICE LEVEL STANDARD AND MEASUREMENT.

1. **General.** Availability for each elapsed calendar month is calculated as follows:
   M = total number of minutes in the elapsed calendar month;
   Y = actual total minutes of (a) Scheduled Routine or Service Maintenance, and (b) Emergency Maintenance.
   N = actual authorized Availability in minutes for the elapsed month which is calculated as follows:N = [(M – Y) x 99.5%]
   X = the number of minutes the Production Instance is authorized to not be available in the elapsed month and which is calculated as follows:
   X = M - N
   D = the number of minutes in the elapsed month that the Production Instance is not available ("**Production Downtime**").
   If D > X Customer will qualify for a service credit as follows.

   If RSA fails to meet the Production Availability Standard in any two months within a three month rolling period (commencing from the month where the Production Availability Standard first failed), then RSA shall issue to the Customer a service credit (a "**Service Level Credit**") in an amount equal to the percentage by which RSA missed the Production Availability Standard of the total fees received for the Service Offering for each of the months during which such failures were measured. However, notwithstanding the foregoing, in no event shall Service Level Credits exceed five percent (5%) of the total Fees received for the Service Offering for such months. The Customer must request a Service Level Credit from RSA in the event that a Service Level Credit isdue. The remedies specified in this Section I.B.1. shall be the Customer's sole and exclusive remedies for the failure of RSA to meet the Production Availability Standard.
2. **Credit Request and Payment Procedures.** To receive a Service Level Credit, Customer (for logging/tracking purposes) must make a request by sending an email to securid.service.credit.request@rsa.com. Each request in connection with this Section I.B. must include the dates and times of the failure to meet Production Availability Standard and must be received by RSA within five (5) business days after receiving the report described under Section

I.C. below. If the failure to meet Production Availability Standard is confirmed by RSA,Service Level Credits will be applied within two billing cycles after RSA's receipt of Customer's credit request.Service Level Credits are not refundable and can be used only towards future billing charges.

C. SERVICE LEVEL REPORTING.

Customer may access RSA's monthly reports of Availability at https://www.rsa.com/secure/.

D. GENERAL OBLIGATIONS.

RSA will use commercially reasonable efforts consistent with generally accepted industry standards and best practices of leading companies in the critical data storage and security industry to: (i) protect the Production Instance and supporting infrastructure controlled or maintained by RSA; (ii) monitor the Production Instance and supporting infrastructure controlled or maintained by RSA for problems; (iii) identify root causes; (iv) correct problems; and (v) minimize recurrences of missed Availability for which it is responsible; (vi) back-up and retain customer data per RSA standard practices. Should a Force Majeure Event result in unavailability of the Service Offering, RSA will focus its efforts on restoring availability of the Service Offering first to the Production Instance, and then to the Non-Production Instance.

II. NON-PRODUCTION INSTANCE.

This Section II of Exhibit 1 applies, if applicable, to Customer's Non-Production Instance of the Service Offering. "**Non-Production Instance**" means the computing environment, applications, and security associated with the Service Offering allocated by RSA for customers to access and use in execution of their business development and/ortesting processes. A Non-Production Instance is provided to Customer, at RSA's sole discretion, for testing and development before commencing the Production Instance(s). Customer acknowledges that Non-Production Instancesare at-risk services given that they are in support of Customer development, user acceptance testing, pre-production staging, and preview(s) of upcoming Service Offering changes to the Production Instance. As such, the Service Offering provided in the Non-Production Instance is not subject to any availability standard and is not eligible for credits on future charges as a result of failure to meet or exceed the Production Availability Standard for the Production Instance.

EXHIBIT 2

INFORMATION SECURITY AND BUSINESS CONTINUITY PLANNING FOR G&L CLOUD

I. ADHERENCE TO STANDARDS OF PROTECTION.

RSA will apply commercially reasonable efforts to carry out the procedures set forth in this Exhibit 2 to protect the Production Instance. In fulfilling its obligations under this Exhibit 2, RSA may, from time to time, use methods or procedures ("**Processes**") similar to and substantially conforming to certain terms herein. RSA shall ensure that any such Processes are no less rigorous in their protection to Customer than the standards reflected in this Exhibit's termsset forth below and shall provide safeguards no less protective in all material respects than those in this Exhibit 2.

A. Definitions.

1. **"Authorized Persons"** means RSA's employees, contractors, or other agents who need to access Customer's environment to enable RSA to perform its obligations under the Agreement, and who are boundby confidentiality and other obligations sufficient to protect Content in accordance with the terms and conditions of the Agreement.
2. **"Encryption"** is a process of using an algorithm to transform data into coded information in order to protect confidentiality.
3. **"Firewall"** is an integrated collection of security measures used to prevent unauthorized electronic access to a networked computer system.
4. **"Intrusion Detection Process"** (or "**IDP**") is a method of reviewing system events and Processes in near real time and, without unreasonable delay, alerting management to known patterns of behavior that indicatean intrusion is occurring or is likely to take place soon.
5. **"Security Incident"** means unauthorized or unlawful access to Content within the possession (e.g., the physical or IT environment) of RSA or any Authorized Person.
6. **"Breach"** means any Security Incident which has led to the loss of, acquisition of, use of, or disclosure of Content within the possession (e.g., the physical or IT environment) of RSA or any Authorized Person.

B. Breach Notification and Remediation.

In the event RSA becomes aware of a Breach as the result of a Security Incident, RSA shall, in the most expedient time possible under the circumstances, notify Customer of the Security Incident and shall, subject to Applicable Lawsor a governmental request, provide Customer with details to the extent available about the Security Incident, includinghow it occurred and how RSA will address the Security Incident. In the event of a Breach, RSA and Customer shall cooperate in good faith to resolve any privacy or data security issues involving Content, and to make any legally required notifications to individuals affected by the Security Incident. In the event of a Breach, RSA shall:

1. **Breach Notification.** Within seventy-two (72) hours after becoming aware of the Security Incident, notify Customer of the approximate date and time of the Security Incident and a summary of known, relevant factsand actions taken to rectify the Processes and address the Security Incident's effects.
2. **Breach Remediation.** Promptly implement reasonable measures necessary to address the security of RSA's systems and the security of Content. If such measures include temporarily restricting access to any information, network, or systems comprising the Service Offering in order to mitigate against further breaches, RSA shall promptly notify Customer of the restricted access, in advance of such restriction whenpossible but in all cases as soon as possible under the circumstances. RSA shall cooperate in good faith withCustomer to allow Customer to verify RSA's compliance with its obligations under this clause.

C. Independent Control Attestation and Testing.

RSA shall employ independent third-party oversight as follows:

1. **Attestation.** At least annually and at its own expense, RSA shall ensure that an audit of the hosted environment where Content is stored, processed, or transmitted by RSA is conducted according to appropriate industry security standards by an independent third party auditor and that such audit will result in the generation of an industry standard audit report (for example, SSAE-18 SOC2, Type II, ISO 27001, or similar) ("**Audit Report**"). Customer may request a copy of the most recent Audit Report from RSA in writing no more than once annually.
2. **Penetration Testing.** At least annually and at its own expense, RSA shall engage a third-party testing service provider for network penetration testing of the RSA infrastructure and systems used to provide the Service Offering. Customer may request a copy of the executive summary of the most recent penetration testing report from RSA in writing no more than once annually.

D. Data Security.

RSA shall use commercially reasonable efforts to carry out the following procedures to manage Content as follows:

1. **Information Classification.** If Customer discloses Content to Service Provider or if Service Provider accesses Content as permitted by the Agreement, Content shall be classified as Confidential Information andhandled in

accordance with the terms hereof.

2. **Encryption of Information.** When necessary, industry-standard encryption techniques (for example, public encryption algorithms such as, RC5, IDEA, RSA and AES) shall be used at cipher strengths no less than 256-bit or equivalent for Content. RSA shall use industry standard authentication practices to authenticate parties and secure messages and/or communications involving Content. Data shall be encrypted while in transit by TLS 1.2 or higher. All data is encrypted at rest at the volume level.
3. **Cryptographic Key Management.** RSA shall ensure that cryptographic keys are managed securely in accordance with control requirements and procedures which are consistent with industry best practices and shall ensure that Content is protected against unauthorized access or destruction. RSA shall ensure that if public key infrastructure (PKI) is used, it shall be protected by 'hardening' the underlying operating system(s) and restricting access to certification authorities.
4. **Event Logging.** For systems directly providing the Service Offering to Customer, RSA shall maintain logsof key events that may affect the confidentiality, integrity, and/or availability of the Service Offering to Customer and that may assist in the identification or investigation of material incidents and/or security breaches occurring in relation to RSA systems. Audit logs shall be retained for at least 180 days, other logsfor at least 90 days. Logs shall be protected against unauthorized changes (including, amending or deletinga log).
5. **Removable Media.** "**Removable Media**" means portable or removable magnetic and/or optical media, including but not limited to hard disks, floppy disks, USB memory drives, zip disks, optical disks, CDs, DVDs, digital film, memory cards, magnetic tape, and other removable data storage media whether owned by Customer or RSA. The use of Removable Media is prohibited unless authorized by Customer in writing.
6. **Media Disposal and Servicing.** In the event that functional storage media used in connection with the Service Offering must be disposed of or transported for servicing, RSA shall ensure Content is not accessiblefrom such media. Non-functional media shall be aggregated in a secure area until enough of it exists to warrant destruction by a contracted, bonded third party of RSA's choosing, and a certificate of destruction shall be supplied to RSA by such third party promptly upon its destruction.
7. **Customer Data Retention**. In the event that an on-premises database extract is used to upload Content into Customer's Production Instance, such extract will be retained by RSA for a maximum of up to 30 days whileused to restore into Customer's Production Instance. After successful restore, such database extract will be deleted by RSA.

E. Computer & Network Security. RSA shall use commercially reasonable efforts to carry out the followingprocedures to protect Content:

Server Security. Computer systems comprising the Service Offering shall be dedicated solely to the provision of the Service Offering and not used by RSA for development and/or testing unless required to fulfil obligations within this Agreement. The Server shall be protected through the following means:

a) Secure Configuration. Server operating systems shall be hardened per established hardeningguidelines which are in alignment with industry best practices.
b) Endpoint protection. Shall be deployed to detect and prevent malicious software or user actions.
c) Patching. Operating system regularly patched for security flaws upon vendor provided remediations.

1. **External Network Segment Security.** Data entering the Service Offering's network from external sourcesshall pass through Firewalls to enforce secure connections between internal and external systems. The Service Offering's connections to the Internet shall (a) have appropriate security measures and controls applied, and (b) include an IDP that monitors data within the external network segment and information coming to Firewalls. RSA shall disable unnecessary network access.
2. **Internal Network Segment Security.** Data in transit within the Service Offering shall leverage appropriate segmentation to allow least access required to operate Service Offering services.
3. **Network and Systems Monitoring.** RSA shall actively monitor its networks and systems used to provide the Service Offering to detect deviation from access control policies and actual or attempted intrusions or other unauthorized acts.
4. **User Authentication.** RSA shall implement Processes designed to authenticate the identity of its system users through the following means:
   i. User IDs. Each user of a system containing Content shall be assigned a unique identification code ("**User ID**").
   ii. Passwords. Each user of a system containing Content shall use a unique password whose length, complexity, and age should be governed in accordance with industry best practices.
   iii. Multi-Factor Authentication for Remote Access. Remote access to systems containing Content shall require the use of multi-factor authentication for systems administrative access.
   iv. Deactivation. RSA User IDs shall be automatically deactivated after a technologically enforced number of unsuccessful log-in attempts. Interactive sessions shall be restricted or timed out after a technologically enforced period of inactivity. User IDs for RSA Personnel with access to Content shall be deactivated promptly upon changes in job responsibilities that render such access unnecessary and

during termination of employment.

5. **Account Access.** RSA shall provide account access to RSA Personnel on a least-privilege, need to know basis.

F. System Development.

1. **Development Methodology and Installation Process.**
   a) Documented Development Methodology. RSA shall ensure that development activities for RSA - developed software used in the provision of the Service Offering are carried out in accordance witha documented system development methodology.
   b) Documented Deployment Process. RSA shall ensure that new systems and changes to existing systems used in the provision of the Service Offering are deployed in accordance with a documented process.
2. **Testing Process.** RSA shall ensure that all reasonable elements of a system (e.g., application software packages, system software, hardware and services) shall be tested at all relevant stages of the systems development lifecycle before applicable system changes are promoted to the Production Instance.
3. **Content in Test Environments.** RSA shall ensure that Content are not used within RSA test environments without Customer's prior written approval.
4. **Secure Coding Practices.** RSA shall have secure development practices for itself and require the same of its subcontractors, including the definition, testing, deployment, and review of security requirements.

G. General Security.

1. **Point of Contact.** RSA shall designate an account manager with whom Customer may coordinate as an escalation point beyond typical Service Offering customer support avenues available to Customer.
2. **Cloud Hosting Facilities.** RSA shall ensure that the cloud provider(s) RSA engages to host the Service Offering use industry best standards for physical security of their data centers such as barrier access controls(e.g., the use of guards and entry badges) that provide a physical environment secure from unauthorized access, damage, and interference.
   Additional requirements specific to Authorized Persons' access to the Service Offering:RSA shall ensure any Authorized Persons' access shall be protected by:
   a) Two-Factor Authentication. Two-factor authentication shall be required for any access to the Service Offering; and
   b) Limited Access. Authorized Persons shall have limited access to the Service Offering environmentonly to the extent required by job function in support of the Service Offering.
3. **Change and Patch Management.** RSA shall use commercially reasonable efforts to ensure that changes (including but not limited to emergency fixes, application patches, firmware updates, and similar) to its applications and infrastructure associated with the Service Offering are tested, reviewed, approved, and applied using an industry standard change management process that accounts for risks to RSA, its customers, and other such factors as RSA deems relevant.
4. **RSA Personnel.**
   a) Background Screening. RSA shall perform background checks in accordance with RSA screening policies on all RSA employees and consultants who are or will be supporting the Service Offeringunder this Agreement, to the extent permitted by Applicable Law.
   b) Training. RSA personnel involved in the provision of the Service Offering shall receive appropriate ongoing security awareness training. Such security awareness training shall be provided to RSA personnel being engaged in the provision of the Service Offering or prior to RSA personnel being given access to Customer's environment.

II. CONTINUITY AND DISASTER RECOVERY PLANNING.

RSA shall ensure that the Service Offering disaster recovery and continuity of operations contingency policies and procedures are in place that to facilitate the implementation of the contingency planning associated policies and controls forthe Service Offering necessary to perform RSA's obligations under this Agreement. RSA shall:

1. require a remote contingency site with adequate security and capacity to provide the Service Offering in accordance with the obligations of this Agreement;
2. require Processes designed to ensure that Content and other data necessary for the performance of the Service Offering are automatically copied to a remote contingency site;
3. include a description of the recovery process to be implemented following the occurrence of a disaster;
4. detail key Processes, personnel, resources, services and actions necessary to ensure that Service Offering continuity is maintained;
5. include a seventy-two (72) hour recovery time objective ("**RTO**") in which the Service Offering shall be recovered following notification that disaster recovery event is declared; and
6. allow for the recovery of Content at the remote contingency site in accordance with a twenty-four (24) hour recovery point objective ("**RPO**").

A. Testing. At least annually and at its own expense, RSA will perform disaster recovery, continuity of operations

assessments. Upon reasonable request, RSA will provide an overview consisting of the date(s), scope, and outcome (on a succeed or fail basis) of the last test.

B. **Notification.** In case of a Force Majeure Event that RSA reasonably believes will impact the Service Offering or its ability to perform its obligations under this Agreement, RSA shall, to the extent possible, promptly notify Customer of such Force Majeure Event via RSA's notification system located at https://status.gl.securid.com/. Such notification shall, as soon as such details are known, contain:

1. a description of the Force Majeure Event in question;
2. the impact the Force Majeure Event is likely to have on the Service Offering and RSA's obligations underthis Agreement;
3. the operating strategy and the timetable for the utilization of the contingency site; and
4. the timeframe in which RSA expects to return to business as usual.