Service Description
for
ID Plus

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

The use of ID Plus 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 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 ID Plus from RSA or a 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 ID Plus 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 United States, Mexico or South America; (ii) the local RSA sales affiliate if Customer is located outside United States, Mexico or 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 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 ID Plus except to the extent all or any portion of ID Plus is subject to a separate written agreement set forth in a quotation issued by RSA.

By proceeding with the use of ID Plus 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 this Agreement shall govern the relationship of the parties with regard to the subject matter of this 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 this Agreement. If you do not have authority to agree to the terms of 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 ID Plus for any purpose.

This Service Description governs the provision by RSA of the RSA offering known as "ID Plus" 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. SCOPE OF SERVICES.

During the term of Customer's subscription to ID Plus as set forth in the ordering document (the "**Term**"), RSA will provide Customer with access to and use of ID Plus (the "**Service Offering**") in accordance with the subscription level selected in the Order and this Agreement as further described therein. Customer's access and use of the Service Offering will be subject to all those restrictions stated in the Agreement.

2. SERVICE OFFERING.

The Service Offering provides four levels of multi-tenant, cloud and hybrid solutions, tailored to fit every identity and access management requirement. All can be flexibly deployed in the cloud, on-prem or hybrid with an open, extensible identity platform. ID Plus strikes a balance of modernizing to cloud and minimizing cybersecurity risks – all while ensuring convenience and continuity for users. The four subscription levels are as follows:

	ID PLUS SUBSCRIPTION PLANS			
	ID Plus C1	**ID Plus E1**	**ID Plus E2**	**ID Plus E3**
Deployment Models	**Cloud-Only**	**Cloud / Hybrid / On-Prem**	**Cloud / Hybrid / On-Prem**	**Cloud / Hybrid / On-Prem**
Cloud Service (CAS)	✓	✓	✓	✓
Identity Router (IDR)		✓	✓	✓
Authentication Manager (AM)		✓	✓	✓
Server license (Enterprise Edition)		✓	✓	✓
Software tokens (SID 820)		✓	✓	✓
On-demand authentication		✓	✓	✓
Up to 15 replica servers		✓	✓	✓
Virtual appliance		✓	✓	✓
Hardware appliance		Add-On	Add-On	Add-On
Multi-Factor Authentication	**Cloud-Only MFA**	**Hybrid MFA**	**Hybrid MFA + SDK**	**Hybrid MFA + SDK**
FIDO	✓	✓	✓	✓
Mobile Push	✓	✓	✓	✓
Biometrics	✓	✓	✓	✓
Apple Face ID / Touch ID	✓	✓	✓	✓
Windows Hello	✓	✓	✓	✓
OTP	✓	✓	✓	✓
QR Code	✓	✓	✓	✓
SMS / Voice	Add-On	Add-On	Add-On	Add-On
Hardware Token (SID700/DS100)	Add-On	Add-On	Add-On	Add-On
3rd party authenticators	✓	✓	✓	✓
RSA Mobile SDK			✓	✓
Offline authentication		✓	✓	✓
On-prem MFA failover		✓	✓	✓
Single Sign-On	**Basic**	**-**	**Enhanced**	**Enhanced**
Application Limits	*unlimited applications*		*unlimited applications*	*unlimited applications*
Portal Rebranding & Customization	-		✓	✓
Custom Domain / URL	-		✓	✓
Contextual Access	**Static**	**Static**	**Adaptive**	**Risk-Based**
Static Rules	✓	✓	✓	✓
User group	✓	✓	✓	✓
User role / attribute	✓	✓	✓	✓
Network (IP range)	✓	✓	✓	✓
Adaptive Access		Add-On	✓	✓
Country		✓	✓	✓
Trusted location		✓	✓	✓
Known device		✓	✓	✓
User agent		✓	✓	✓
Authentication source		✓	✓	✓
Risk AI		Add-On	Add-On	✓
Risk Engine 2.0		✓	✓	✓
Identity Confidence scoring		✓	✓	✓
Risk AI dashboards & analytics		✓	✓	✓
Threat Aware Authentication		✓	✓	
Integrations	**Web Standards**	**Web + Agents/RADIUS**	**Web + Agents/RADIUS**	**All Integrations**
Federation	✓	✓	✓	✓
SAML 2.0	✓	✓	✓	✓
OpenID Connect (OIDC)	✓	✓	✓	✓
RADIUS		✓	✓	✓
Agents		✓	✓	✓
Desktop login (Windows, macOS)		✓	✓	✓
Server login (Windows, Linux)		✓	✓	✓
Custom web server (IIS, Apache)		✓	✓	✓
Native (ADFS, Citrix, EPIC, etc.)		✓	✓	✓
RSA Authentication API (REST)		✓	✓	✓
Web Proxy			Add-On	✓
Trusted headers			✓	✓
Password vaulting			✓	✓
Kerberos/IWA			✓	✓
NTLM			✓	✓
Workflows	**Standard**	**Standard**	**Advanced**	**Advanced**
Self-service enrollment	✓	✓	✓	✓
Help desk / admin-assisted	✓	✓	✓	✓
Credential management	✓	✓	✓	✓
Password reset	✓	✓	✓	✓

Emergency access	✓	✓	✓	✓
Custom workflows (Admin API)			✓	✓
ID Verification (BYOL)			✓	✓
ID Verification	Add-On	Add-On	Add-On	Add-On
Directory	**Cloud-Only**	**Cloud/On-Prem**	**Cloud/On-Prem/Custom**	**Cloud/On-Prem/Custom**
ID Plus Cloud Directory	✓	✓	✓	✓
Active Directory / LDAP		✓	✓	✓
Azure AD (Entra ID)	✓	✓	✓	✓
AM Internal Database		✓	✓	✓
Custom user stores (SCIM)			✓	✓
			✓	✓
Mobile Lock**	Add-On	Add-On	Add-On	**Included***
40+ mobile threat vectors	✓	✓	✓	✓
Custom threat profiles	✓	✓	✓	✓
ML dashboards & analytics	✓	✓	✓	✓
Support	**Basic 9x5 Support**	**Enhanced 24x7 Support**	**Enhanced 24x7 Support**	**Premium 24x7 Support****
Online community access	✓	✓	✓	✓
Live technical support	9x5 support	24x7 support	24x7 support	24x7 support
Premium support	-	Add-On	Add-On	✓
Customer Success Engineer***	**Included**	**Included**	**Included**	**Included**
Guided cloud modernization	✓	✓	✓	✓
Expert technical insights	✓	✓	✓	✓
Personalized success path	✓	✓	✓	✓
Product roadmap deep dives	✓	✓	✓	✓
Help Desk Live Verify		Add-On	**Included**	**Included**
Bi-directional trust*****		✓	✓	✓
Protection across all channels & transactions		✓	✓	✓
API built for your workflows		-	✓	✓

*Mobile Lock is included in New E3 contracts executed post 10/16/2023.
**Mobile Lock is not currently FedRAMP authorized for any ID Plus subscription package.
***Premium Support is included in New E3 contracts executed post 10/16/2023.
****Customer Success availability for ID Plus subscription plans is based on an annual spend matrix. Customer Success Manager support will be provided to customers actively utilizing our cloud solutions. Contact Sales for more information.
*****Patent pending for bi-directional capabilities.

The Service Offering is designed to protect cloud and/or on-premises web applications, third party single sign-on (SSO) solutions, and on-premises resources. Customer's accepted Order for the Service Offering will state which package 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 Hardware provided with the Service Offering is governed by this Agreement and the Product Warranty and Maintenance Table located at https://www.rsa.com/standard-form-agreements/. Supplementals will be listed on the applicable ordering document and may include, but is not limited to, Risk Based Policy, Web Proxy, Mobile Lock and DS100 Subscription.

3. ACCOUNT ACCESS.

RSA will deliver to Customer an application administrator user ID, password, and other account information ("**Account Access Information**") necessary for Customer to access the Service Offering in accordance with the Agreement. Thereafter, Customer will create and manage Account Access Information 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 local, state, national, and foreign laws, treaties, and regulations ("**Applicable Laws**") in connection with Customer's use of the Service Offering, including but not limited to those related to data privacy, international communications, and the transmission of technical or personal data.

4. 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 obligation under 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 Customer Attributes (as defined below).

A. ***Maintain Supported Releases***. *Customer shall maintain their on-premises environment on a currently supported, having not*

reached End of Primary Support (EOPS), version of software. This includes, but is not limited to, on-premises server software, agents, Application Programming Interfaces (API's), and Authenticator applications. RSA reserves the right to require the customer to update or upgrade to a supported release in order for RSA to provide Support Services. Actively supported versions will be listed on the Product Life Cycle pages (https://community.rsa.com/s/product-life-cycle).

B. If the customer has not entered into an Extended Support agreement with RSA, RSA may charge a fee, above and beyond the Annual Maintenance/Service Contract, per case/service request/issue, in order to deliver Support on an EOPS version. Any request for Support Services made on an EOPS release provides consent to be charged for Support Services on a per case basis. EOPS support shall be factored on a per case/service request/issue, after the Customer has renewed a valid Maintenance Support service contract and any charges shall be in addition to the service contract, not in lieu of.

5. CUSTOMER ATTRIBUTES.

RSA requires access to only the following end user attributes from the Customer (collectively, "**Customer Attributes**") in order to provide the Service Offering to Customer: First Name, Last Name, Email Address, Username, Primary Unique Identifier (entryDN), Secondary Unique Identifier (GUID), Account Status, and Account Expiration. No other personally identifiable information is required in order for the Customer to access or use the Service Offering, including but not limited to, any personally identifiable 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) (collectively, "**Sensitive PII**"). During the Term, Customer grants to RSA a limited, non-exclusive license to use the Customer Attributes solely for all reasonable and necessary purposes contemplated by this Service Description and for RSA to provide the Service Offering. Customer, not RSA, shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use of all Customer Attributes. RSA shall use reasonable and appropriate administrative, technical and physical safeguards to protect the security, integrity and confidentiality of the Customer Attributes. However, for clarity, Customer acknowledges and agrees that 1) the Service Offering is not intended or designed to securely host and store any Sensitive PII, and 2) Customer shall not modify or use the Service Offering to store any such Sensitive PII or provide RSA with access to any Sensitive PII or information other than the Customer Attributes.

6. RSA OBLIGATIONS.

A. General.

RSA will, through its 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. Physical infrastructure and hardware at the Customer's location are the Customer's sole responsibility to 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. Application Upgrades.

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

C. Malware Protection.

RSA will install and run industry standard malware protection on all systems underlying the Service Offering. Anti-malware definition files shall be updated regularly in accordance with industry standards. For the avoidance of doubt, Customer remains responsible for protecting its own systems by installing, updating, and maintaining industry standard malware protection.

D. Logging.

RSA will monitor and log all authentication and administrative system access to the Service Offering and will maintain at least thirty (30) day backups of such logs. Such logs are RSA Confidential Information but will be disclosed as necessary to comply with Applicable Law and to Customer upon written request.

E. Service Levels.

i. Service Levels for Cloud Service Offerings are specified in Exhibit 1.

ii. Service Levels for Hybrid, On-Premises and Cloud, Service Offerings are specified in Exhibit 1 and Exhibit 2.

7. 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/.

8. Support Options

A. Support services fees will be directly related to the per user license volume.

B. Software Service Request Resolution Process

(i) Process. RSA handles all Customer support Service Requests on a **first-in-first-out** basis. RSA shall prioritize all Errors according to their impact to Customer using the severity definitions described in Section II(A) of

Exhibit 2. RSA may upgrade or downgrade the severity of an Error depending on developments during the resolution process. For example, if available, a temporary resolution may be provided to mitigate the material impact of a given Error resulting in the reduction of the severity of a Service Request.

(ii) Escalation. If Customer and RSA are unable to mutually agree upon a resolution plan for S1 and S2 Errors, then the parties shall escalate the Service Request in accordance with RSA's escalation process. Once the escalation process has been initiated, RSA shall provide Customer with Service Request progress updates via phone or email on a mutually agreed upon schedule. Such progress updates shall include information about the Error description, daily progress, root cause (if known) and overall plan to resolve the Error.

SUPPORT OPTIONS	BASIC SUPPORT	ENHANCED SUPPORT	PREMIUM SUPPORT
Support Availability	9x5 Online + Phone (Customer local time)	24x7 Online + Phone (Customer local time)	24x7 Online + Phone PRIORITY ACCESS
Designated Level 2 Resources	None	None	Included
Access Methods	Web Email	Web Email Phone	Web Email Dedicated Phone Lines
Direct Phone Access to TSEs	N/A	N/A	Included
Language	English Only	English Only	We guarantee support in English, and to our best case in French, Arabic and German languages
Root Cause Analysis	N/A	N/A	Included for S1 upon request
*Hours of support for Support Availability are subject to change by RSA upon prior written notice.			

C. Software Support Service Level Objectives (SLOs). RSA will take all commercially reasonable efforts to provide support services on the Generally Available (GA) releases and the immediate prior release, provided the customer maintains current versions under a valid and active Support Contract with RSA. RSA will use reasonable commercial efforts to provide Customer with technical advice and assistance in connection with their use of the Software according to severity level. The table below sets forth RSA's targets for support responses to Software Errors based on Severity Level:

SUPPORT LEVEL	SEVERITY LEVEL	INITIAL TARGET RESPONSE	TARGET WORK EFFORT	TARGET COMMUNICATION FREQUENCY
BASIC (9x5)	S1	2 hours (9x5)	Continuous 9x5 during customer business hours until relief identified	Once per day (business day only)
	S2	4 hours (9x5)	Daily, during customer business hours only	Every 2 to 3 days (business day only)
	S3	8 hours (9x5)	Weekly, during customer business hours only	Once a week
	S4	12 hours (9x5)	Every other week during customer business hours	Once a month
ENHANCED (24x7)	S1	1 hour (24x7)	Continuous 24x7 until Relief identified	Every 3-4 hours, 7 days/week
	S2	3 hours (24x7)	Daily, during Customer business hours*	Once per day, business hours*
	S3	4 hours (9x5)	Weekly during business hours	Once a week
	S4	10 hours (9x5)	Every other week during business hours	Twice a month
PREMIUM (24x7)	S1	30 Minutes (24x7)	Continuous 24x7 until Relief identified	Every 3-4 hours, 7 days/week
	S2	1 hours (24x7)	Daily, during Customer business hours*	Once per day, business hours*
	S3	3 hours (9x5)	Weekly, during customer business hours	Twice a week
	S4	4 hours (9x5)	Weekly, during customer business hours only	Once a month
* Available weekends and evenings per Customer request				

9. DS100 Subscription.

i. *DS100 Overview*. The DS100 is a cloud-managed, multi-functional hardware authenticator that supports one-time password (OTP) and passwordless FIDO2 authentication. With dynamic seeding and self-registration, Customer can secure users as they transition from OTP to FIDO2 without having to change or touch their authentication device. The DS100 authenticator supports OTP generation when unplugged from a device to support high security environments without USB connectivity. Though it is physically deployed, the DS100 is conveniently managed in the cloud along with your software authenticators. This, combined with dynamic seeding simplifies distribution and allows for user self-registration. The DS100 also features user updatable firmware.

ii. *DS100 Subscription Term & Price*. The DS100 subscription term and price shall be specified in the Customer's accepted Order for DS100s, and subject to the Terms of Service for RSA Cloud Offerings currently located at https://www.rsa.com/standard-form-agreements/.

iii. *DS100 License*. RSA grants to Customer a non-exclusive, non-transferable, worldwide, royalty-free, term license to use

the DS100s during the Subscription Term in accordance Customer's accepted Order.

iv. *Supplemental Hardware*. The DS100 authenticator may be provided as Supplemental Hardware if specified in the Customer's accepted Order for the Service Offering.

v. *Initial Order.* The initial order quantity of DS100s shall be specified in the Customer's accepted Order and shall not exceed the User quantity for the Service Offering ("DS100 Users").

vi. *User Adjustments.* Customers may increase the quantity of DS100 Users at any time through an additional Order. Customers may decrease their DS100 Users only at the end of the current Subscription Term.

vii. *Annual Allocation*. Upon full payment for the subscription year, a DS100 Subscription entitles the Customer to receive a 25% annual allocation of DS100s for DS100 Users. Customer may replace up to 25% of its DS100s with the annual allocation to assist in administration, defect and warranty replacement, and re-assignment, provided that, Customer ceases to use the replaced DS100s and return all warranty replaced DS100s to RSA. The first-year allotment is not available until after 90 days from the initial Order. Thereafter, the annual allocation is defined as every 12 months from Order date. Annual allocation not utilized in the current 12 months shall not carry over to subsequent years or months. Annual allocations may only be ordered through the MyRSA Customer portal and ordered in one lump sum order. Customers will be able to view the inventory of their annual allotment on their Customer portal.

10. Supplemental Software.

i. *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.

ii. *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.

iii. *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.

iv. *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.

v. *Help Desk Live Verify.* Help Desk Live Verify (HDLV) is a core capability within RSA ID Plus that enables secure, passwordless, bi-directional identity verification between help desk agents and end-users, eliminating the need for shared secrets like PINs or personal information. This capability is especially critical now, as IT help desk impersonation attacks are on the rise, causing substantial financial and reputational harm. HDLV helps organizations combat these threats by ensuring mutual trust, preventing credential phishing, and detecting anomalies in real time. HDLV integrates seamlessly with RSA's Risk AI and Mobile Lock.

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 used solely for authentication activities. The Production Instance shall have 99.95% or higher Availability on a monthly basis (the "**Production Availability Standard**"), calculated as set forth below. "**Availability**" means, subject to the exclusions below, solely the availability of the cloud authentication components of the Service Offering and does not apply to any components of the Service Offering that are not delivered by RSA over the internet as part of the Service Offering (e.g., Incidental Software) or other RSA products, software, services, solutions, maintenance, or support services. A high availability solution can be enabled via hybrid deployment of on-premises and cloud environments.

A. PRODUCTION INSTANCE INTERRUPTIONS.

1. **Measurement.** Production Downtime, as defined below, is measured from the RSA-confirmed commencement time 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 extent that 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) Issues with or lack of network connectivity between the IT systems of Customer to the Service Offering;
   (iv) Routinely Scheduled Maintenance, Service Updates or Emergency Maintenance. "Emergency Maintenance" 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 in advance.
   - **Emergency Maintenance** - Notifications will be provided at least 24 hours in advance for any emergency maintenance.

   (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, acts of 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 emergency or unscheduled maintenance which shall not exceed 240 minutes per month;
   N = actual authorized Availability in minutes for the elapsed month which is calculated as follows:
   N = [(M – Y)x99.95%]
   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 is due. 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://community.rsa.com/s/article/Monitor-Uptime-Status-for-the-Cloud-Authentication-Service-5273feb4.

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. 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/or testing processes. A Non-Production Instance is only provided to Customer upon Customer's written request to RSA. Customer acknowledges that Service Offering in the Non-Production Instance are 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

SUPPORT SERVICE LEVELS

I. **ON-PREMISES MAINTENANCE SERVICES**

A. Maintenance Services.

(i) Except as otherwise provided in Section D below (Personalized Support Options), all Maintenance Services are provided remotely from RSA's premises as follows:

(a) Web Support. RSA shall provide Customer with access, through a separate registration process, to (i) for Customers who have licensed RSA product where such resources are available, such RSA product's community offering Blogs, Discussion Forums, and download of patches and bug fixes, and (ii) for all other Customers, RSA's online technical support knowledge database, offering Customer the ability on a 24x7 basis (24 hours a day, seven days a week) to raise issues, monitor Services Requests, and download patches and bug fixes. RSA's on-line Web Support resource is currently hosted at the following web address: https://community.rsa.com/s/news/how-to-contact-rsa-support-MCXZ5QDM4ZQZATLL3Y6NMQVUNYWE.

(b) Telephone Support. RSA shall provide telephone support to Customer. RSA's Telephone Support numbers are currently located at the following address: https://community.rsa.com/s/news/how-to-contact-rsa-support-MCXZ5QDM4ZQZATLL3Y6NMQVUNYWE.

(ii) In the performance of the Maintenance Services, RSA will:

(a) Use good-faith, commercially reasonable efforts to aid in the diagnosis of, and correct, Errors in the Software and/or Hardware; and

(b) Provide advice on how to use the Products by way of telephone, e-mail, and web-based technical assistance.

B. Software and Hardware Operating System Upgrades. Customers who are current on payment of Maintenance Service fees, shall also receive the following software and hardware upgrades:

(i) **Software Upgrades**. All Software Releases (including all Error corrections made available pursuant to this Agreement) that RSA in its sole discretion: (a) deems to be logical improvements to the Software; (b) make generally available to all licensees of the Software; and (c) does not separately price or market.

(ii) **Hardware Operating System Upgrade**. RSA shall also provide all core Hardware operation system upgrades. This does not include additional software or operating system variants that are required for optional capabilities. The application of a new operating system to the Hardware may require that Customer re-images the Hardware so that the updates apply properly. Application or use of any operating system, or other software or equipment with the Hardware, other than that provided by RSA, shall void Customer's Hardware warranty and RSA's maintenance obligations.

C. Personalized Support Options. Customers may purchase the Personalized Support Options described herein at an additional fee and as ordered in a Quote, Schedule, or Customer Purchase Order, and such personalized support options may be subject to additional terms located in a Service Brief, SOW or similar document.

In addition to the TAM and DSE support services specified below, all Personalized Support Options will include the following services:

(a) Review, reporting, and management of Service Requests;
(b) Monitoring and notification to Customer of Service Request trends;
(c) Technical escalation management;
(d) Bi-annual on-site account reviews;
(e) Conference calls, scheduled as necessary, to discuss support-related matters; and
(f) If the TAM or DSE is unavailable, Customer may access RSA's 24x7x365 Telephone Support

(i) Technical Account Manager (TAM) Support Services.

(a) Technical Account Manager. RSA shall provide a Technical Account Manager ("TAM") who shall act as the Customer's designated point of contact within RSA for technical account management and escalation of Service Requests. The TAM shall be responsible for overseeing the Maintenance Services delivered and will work closely with Customer to ensure that appropriate resources are engaged to resolve Service Requests in a timely manner.

(b) Limitations:

(1) TAM support services shall be provided in English language only.

(2) Each TAM will be assigned to one Product and one geographical region only, to be selected by Customer (i.e. North America, Europe Middle East Africa, and Asia Pacific Japan). Customer must purchase additional TAM support for additional Products and/or geographical regions.

(ii) Designated Support Engineer (DSE) Support Services.

(a) Designated Support Engineer. RSA shall provide a Designated Support Engineer (**"DSE"**) who will act as Customer's single and direct point of contact on all technical issues associated with an assigned Product. The DSE will become familiar with Customer's technical environment, staff and unique support issues and

will work directly with the Customer Contacts to resolve issues, manage technical escalations, and deliver business reviews. The DSE shall be reasonably available by telephone during Standard Support Hours.

(b) Limitations:

(1) DSE Support Services shall be provided in the English language only.

(2) Each DSE will be assigned to one Product and one regional time zone only, to be selected by Customer (i.e. North America (EST or PST), Europe Middle East Africa, and Asia Pacific Japan). Customer must purchase additional DSE support for additional Products and/or regional time zones.

(3) Customer shall be required to identify a maximum of four (4) Customer Contacts, who are familiar with Customer's software environment, to coordinate all technical support calls and/or interaction with the identified DSE as set forth above.

II. SOFTWARE ERROR SEVERITY CLASSIFICATIONS AND SERVICE REQUEST RESOLUTION PROCESS.

A. Software Error Severity Classifications. All Software Errors shall be classified by RSA as follows:

Severity Level	Definition	Examples
1 ("S1")	Critical: Severe problem preventing Customer or workgroup from performing critical business functions	▪ Production System data corruption (data loss, data unavailable) ▪ Production System crash or hang ▪ Production Systems significantly impacted, such as severe performance degradation ▪ Production System and/or data is at high risk of potential loss or interruption ▪ Production System workaround is required immediately ▪ Time critical Production cutover impacted
2 ("S2")	High: Customer or workgroup able to perform job function, but performance of job function degraded or severely limited	▪ Production System adversely impacted ▪ Non-Production System data corruption (data loss, data unavailable) ▪ Non-Production System crash or hang ▪ Non-Production System and/or data is at high risk of potential loss or interruption ▪ Non-Production System workaround is required immediately ▪ Development system(s) is inoperative
3 ("S3")	Medium: Customer or workgroup performance of job function is largely unaffected	▪ Production or development system has encountered a non-critical problem or defect and/or questions have arisen on product use.
4 ("S4")	Request: Minimal system impact; includes feature requests and other non-critical questions	▪ No Customer business impact ▪ Requests for enhancements by Customer

III. HARDWARE SUPPORT

If an Error is identified in the Hardware and the Hardware is under warranty, RSA shall use commercially reasonable efforts to provide one of the following remedies at RSA's sole and exclusive discretion: (a) an electronic remedy; (b) spare part replacement; or (c) Advance Replacement of Hardware.

A. **Advance Replacement of Hardware.** An "Advance Replacement" occurs when RSA authorizes shipment of a replacement Hardware component to Customer prior to the defective Hardware component being returned to RSA for repair. Solely on the approval of an RSA customer care representative and subject to the RSA Return Material Authorization ("RMA") Process, RSA shall use commercially reasonable efforts to provide an Advance Replacement if an Error is identified in the Hardware. Any Hardware shipped under RSA's RMA process shall have the same licensed capacity as the original Product regardless of whether such replacement is a newer model of the defective Hardware. RSA posts additional information regarding its Advance Replacement policy on its Support Website.

B. **Return Material Authorization ("RMA") Process**. If RSA determines that it is necessary for the Customer to return Hardware to RSA for repair or replacement, Customer must provide RSA with the Hardware component model, serial number, and failure information to initiate the RMA Process. Customer must return Hardware within fifteen (15) calendar days for all other Hardware or Customer will be charged for the Advanced Replacement.

IV. CUSTOMER OBLIGATIONS.

A. **Documenting Errors.** Customer shall use good-faith, reasonable efforts to isolate and document Errors to enable RSA to fulfill its obligations herein. Once a Service Request has been initiated, Customer will be asked to provide necessary Error data which may include but not be limited to, applicable identification number for Software or Hardware, description of Error, any error messages, and any requested support files.

B. **Maintaining Product Integrity.** Customer will follow RSA best practices guidelines, which include maintaining an onsite disaster recovery for each Hardware appliance to enable RSA to restore the appliance in accordance with Customer's configuration. Customer agrees to not install any third party non-certified software or modify any existing software or firmware on the Hardware without notification to, and prior authorization by, RSA technical support in order to ensure that

RSA's ability to maintain accurate records of Customer's existing environment.

V. **ADDITIONAL EXCLUSIONS.**

A. **Use.** Maintenance Services specifically **excludes** support for any Errors caused by (i) operator error or use of the Software and/or Hardware in a manner not in accordance with the Product Documentation; (ii) use of the Software and/or Hardware with software and/or hardware other than that for which the Software and/or Hardware was originally licensed; (iii) Errors caused by any fault in the Customer's environment, hardware, or in any software used in conjunction with the Software or Hardware but not provided by or approved by RSA; (iv) any integration, modification, or repair of the Software and/or Hardware made by any person other than RSA; (v) installation of any appliance, firmware, or operating system on the Hardware other than that provided by RSA; (vi) unusual physical, electrical or electromagnetic stress, fluctuations in electrical power beyond Product specifications, or failure of air conditioning or humidity control; and (vii) accident, misuse, or neglect or causes not attributable to normal wear and tear. In addition, support excludes any Errors for which a correction is available in a subsequent Software Release than that currently operated by Customer and such subsequent Software release has been made available to Customer by RSA.

B. **Supported Versions.** Maintenance Services also specifically **excludes** support for any version of the Software released by RSA which has reached its "end of primary support" (EOPS) date, as determined by RSA. Each Software Release will reach its EOPS date after a period of not less than twenty four (24) months following the date of that Software Release's "General Availability" (or "GA" release date, as this term is generally understood in the software industry), unless another EOPS date is set forth at https://community.securid.com/s/news/product-version-life-cycle-for-securid-MC47AXTAGWJFFFXCWPRTM6DA7VXU.This time period may be extended by RSA at its sole discretion. In order to continue to receive ongoing Maintenance Services hereunder for any Software Release which is beyond its EOPS date, Customers must upgrade to a currently supported Software Release. For certain Software Products, Customers may enter into an Extended Support agreement for a period of one or two years to obtain Maintenance Services for Software which has already reached its EOPS date. For additional information on Software EOPS dates and the availability of Extended Support agreements for such Software, please go to https://community.securid.com/s/news/product-version-life-cycle-for-securid-MC47AXTAGWJFFFXCWPRTM6DA7VXU.

VI. **DEFINITIONS.**

The following definitions apply to the terms as used in this Exhibit 2:

A. **"Customer Contacts"** means identified Customer personnel who are familiar with Customer's software environment and will coordinate all technical support calls to RSA.

B. **"Documentation"** means the then-current, generally available, written user manuals and online help and guides for any Software and/or Hardware provided by RSA.

C. **"Error"** shall mean any reported malfunction, error or other defect in the Product that can be reproduced by RSA and constitutes a non-conformity from the Product Documentation. Each Error will be assigned a severity level as further detailed in Section II(A) of this Exhibit 2.

D. **"Hardware"** means the hardware product that the Software is incorporated in or bundled with and sold as a unit.

E. **"Product"** means Hardware and/or on-premises Software. Products do not include evaluation Products.

F. **"Production System"** shall mean a computer system, including any Hardware where applicable, upon which the Software is installed and resident and which is used by Customer for purposes other than development, quality, assurance, disaster recovery or testing.

G. **"Relief"** shall mean an intervention by RSA that restores Product operations impacted by an Error. Examples may include without limitation: (i) a solution or workaround has been provided to resolve the Product issue; (ii) Customer's Production System is operational and Customer is able to perform business critical operations that relate to the Product; and/or (iii) the identified Error does not originate from the Product.

H. **"Service Request"** shall mean a ticket that has been opened, documented, and is being managed by RSA in response to a Customer's report of an Error.

I. **"Software"** shall mean the on-premises software licensed by Customer under the End User License Agreement located at https://www.rsa.com/standard-form-agreements/, consisting of a series of instructions or statements in machine-readable, object code form only, including without limitation firmware incorporated in any Hardware.

J. **"Software Release"** means any subsequent version of Software that RSA makes generally available to its customers who are current on their Maintenance Services fees but does not mean new Software.

EXHIBIT 3

INFORMATION SECURITY AND BUSINESS CONTINUITY PLANNING FOR ID PLUS CLOUD

I. ADHERENCE TO STANDARDS OF PROTECTION.

RSA will apply commercially reasonable efforts to carry out the procedures set forth in this Exhibit 3 to protect the Production Instance. In fulfilling its obligations under this Exhibit 3, 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 terms set forth below and shall provide safeguards no less protective in all material respects than those in this Exhibit 3.

A. Definitions.

1. **"Authorized Persons"** means RSA's employees, contractors, or other agents who need to access Customer Attributes to enable RSA to perform its obligations under the Agreement, and who are bound by confidentiality and other obligations sufficient to protect Customer Attributes 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 indicate an intrusion is occurring or is likely to take place soon.
5. **"Security Incident"** means any loss of, or unauthorized or unlawful access to, acquisition of, use of, or disclosure of, Customer Attributes 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 Security Incident, RSA shall, in the most expedient time possible under the circumstances, notify Customer of the Security Incident and shall, subject to Applicable Laws or a governmental request, provide Customer with details to the extent available about the Security Incident, including how it occurred and how RSA will address the Security Incident. In the event of a Security Incident, RSA and Customer shall cooperate in good faith to resolve any privacy or data security issues involving Customer Attributes, and to make any legally required notifications to individuals affected by the Security Incident. In the event of an actual Security Incident involving RSA's systems or network, 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 facts and 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 Customer Attributes. 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 when possible but in all cases as soon as possible under the circumstances. RSA shall cooperate in good faith with Customer 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 Customer Attributes are 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 SOC 2, 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 Customer Attributes as follows:

1. **Information Classification.** If Customer discloses Customer Attributes to Service Provider or if Service Provider accesses Customer Attributes as permitted by the Agreement, Customer Attributes shall be classified as Confidential Information and handled in accordance with the terms hereof.
2. **Encryption of Information.** 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 Customer

Attributes. RSA shall use industry standard authentication practices to authenticate parties and secure messages and/or communications involving Customer Attributes.

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 Customer Attributes are 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. **Data Access; Transmission.** RSA shall make RSA-controlled applications and systems used to process or store Customer Attributes accessible only by those whose job responsibilities require such access. If transferred across the Internet, wireless network (e.g., cellular, 802.11x, or similar technology), or other public or shared networks, Customer Attributes shall be protected using appropriate cryptography.
5. **Event Logging.** For systems directly providing the Service Offering to Customer, RSA shall maintain logs of 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. The logs shall be retained for at least 30 days and protected against unauthorized changes (including, amending or deleting a log).
6. **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.
7. **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 Customer Attributes are not accessible from 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.

E. Computer & Network Security. RSA shall use commercially reasonable efforts to carry out the following procedures to protect Customer Attributes:

1. **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 fulfill obligations within this Agreement.
2. **Internal Network Segment Security.** Data entering the Service Offering's network from external sources shall pass through Firewalls to enforce secure connections between internal and external systems.
3. **External Network Segment Security.** 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's IDP shall be designed to detect and report unauthorized activity prior to entering the Firewalls. RSA shall disable unnecessary network access points.
4. **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.
5. **User Authentication.** RSA shall implement Processes designed to authenticate the identity of its system users through the following means:
    a) User IDs. Each user of a system containing Customer Attributes shall be assigned a unique identification code ("**User ID**").
    b) Passwords. Each user of a system containing Customer Attributes shall use a unique password whose length, complexity, and age should be governed in accordance with industry best practices.
    c) Two-Factor Authentication for Remote Access. Remote access to systems containing Customer Attributes shall require the use of two-factor authentication.
    d) 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 Customer Attributes shall be deactivated promptly upon changes in job responsibilities that render such access unnecessary and during termination of employment.
6. **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 with a 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. **Customer Attributes in Test Environments.** RSA shall ensure that Customer Attributes 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 are:
   a) Two-Factor Authentication. Two-factor authentication shall be required for any access to the Service Offering; and
   b) Limited Internet Access. Authorized Persons shall have access to external email and/or the Internet from within the Service Offering environment only 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 Offering under 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 Attributes.

II. CONTINUITY AND DIASTER RECOVERY PLANNING.

RSA shall ensure that the necessary Service Offering disaster recovery and continuity of operations contingency policies and procedures are in place that facilitate the implementation of contingency planning policies and controls necessary to meet 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 Customer Attributes 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 four (4) 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 Customer Attributes at the remote contingency site in accordance with a two (2) 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://www.rsa.com/secure/. 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 under this 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.