Service Description
for
RSA Agent ID

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

The use of RSA Agent ID 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 RSA Agent ID 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 **RSA Agent ID** 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 RSA Agent ID except to the extent all or any portion of RSA Agent ID is subject to a separate written agreement set forth in a quotation issued by RSA.

By proceeding with the use of **RSA Agent ID** 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 RSA Agent ID for any purpose.

This Service Description governs the provision by RSA of the RSA offering known as "**RSA Agent ID**" to which Customer has purchased a valid subscription. 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 applicable Order controls solely with respect to the transaction-specific commercial terms; this Service Description controls with respect to RSA Agent ID functionality, deployment requirements, service levels, and Customer responsibilities; and the Terms of Service controls with respect to all other matters.
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 RSA Agent ID as set forth in the ordering document (the "**Term**"), RSA will provide Customer with access to and use of RSA Agent ID (the "**Service Offering**") in accordance with the subscription level selected in the Order and this Agreement as further described therein. Customer access to and use of the Service Offering will be subject to all those restrictions stated in the Agreement.

2. SERVICE OFFERING.

Service Offering is a subscription-based agentic identity security platform designed to discover and secure artificial intelligence agents, related non-human identities, Model Context Protocol (MCP) servers, and the tools and resources they can access. The modules, deployment options, usage quantities, hosting region, and support level purchased by Customer are stated in the applicable Order. Only modules, features, and deployment options that are generally available, identified in the then-current Documentation, and expressly included in the Order form part of the Service Offering. The generally available modules and deployment options are summarized below.

RSA AGENT ID MODULES AND DEPLOYMENT OPTIONS		
Characteristic	**Agent ID Discover**	**Agent ID Secure**
Primary function	Correlates supported sources to identify sanctioned and shadow agents, related non-human identities, and MCP servers; presents discovered resources and available ownership and posture information for Customer review. Customer administrators, not RSA Agent ID Discover, determine and perform remediation actions, including registration, blocking, ownership assignment, and lifecycle changes, except to the extent an automated action is expressly documented as generally available and enabled by Customer.	Applies Customer-configured policy to supported agent calls routed through an AI/MCP Gateway, including allow, deny, and human approval outcomes where supported; records attributable evidence as described in the then-current Documentation.
Delivery	RSA hosted SaaS service, including the administrative experience and RSA-hosted discovery and correlation functions described in the then-current Documentation.	RSA-hosted SaaS service plus one or more AI/MCP Gateways. Gateway hosting may be RSA-hosted, Customer-hosted, or hybrid, as expressly stated in the Order and then-current Documentation.
Gateway deployment	Not applicable.	RSA-hosted, Customer-hosted, or hybrid, as stated in the Order and Documentation.
Data and control	Tenant data is maintained in the supported region selected for the tenant, subject to the Agreement and Documentation.	For Customer-hosted Gateways, policy decisions and per-call records are generated in the Gateway; per call records are transmitted to and displayed in the RSA-hosted administrative console as described in the then-current Documentation. RSA manages RSA-hosted components.
Integrations	Supported identity, cloud, endpoint, collector, and Gateway sources identified in Documentation. A collector or other Customer-Hosted Software may require Customer deployment to endpoints or other Customer-controlled systems using Customer's device-management or software-distribution tools. Customer is responsible for authorization, deployment, configuration, endpoint notices, and compliance with applicable law and internal policy.	Supported identity providers, tools, MCP servers, APIs, evidence outputs, and SIEM integrations identified in Documentation.

Customer's accepted Order identifies the RSA Agent ID modules and deployment options purchased by Customer. RSA Agent ID Discover and RSA Agent ID Secure may be ordered separately or together when generally available. Any reference in Documentation, marketing materials, demonstrations, or communications to RSA Agent ID Govern, a fully air-gapped or fully self-managed deployment, future connectors, future regions, or other roadmap capabilities is informational only and does not create a delivery obligation or form part of the Service Offering unless the capability is generally available and expressly listed in Customer's Order.

Software that RSA makes available for installation in Customer's environment, including a Customer-hosted AI/MCP Gateway, connector, collector, or other customer-hosted component ("Customer-Hosted Software"), is governed by the End User License Agreement located at https://www.rsa.com/standard-form-agreements/ unless the Order states otherwise. Third-party products and services used with the Service Offering remain subject to their providers' terms. No hardware is included unless expressly identified in the Order.

3. ACCOUNT ACCESS.

RSA will deliver to Customer an initial administrator user identifier and enrollment or activation instructions necessary for Customer to access the Service Offering in accordance with the Agreement. RSA does not provide an initial password; the administrator must establish authentication credentials through the applicable activation or password-reset process. Customer thereafter creates and manages access for Customer authorized users and is responsible for account security and activity under Customer controlled accounts. Customer 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 keep Customer-Hosted Software, connectors, API clients, identity-provider integrations, and other Customer-controlled components on versions then supported by RSA and shall install required security updates and upgrades within a commercially reasonable period. RSA may require Customer to update or upgrade to a supported release before RSA provides Support Services. Supported versions are identified on the applicable Product Life Cycle pages at 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.

To provide the Service Offering, RSA may process information submitted by Customer or collected from Customer-configured sources and integrations (collectively, "Customer Attributes"), including: administrator and user identifiers; agent, non-human identity, MCP server, tool, API, application, endpoint, cloud-resource, and credential metadata; assigned owner, purpose, risk tier, lifecycle state, and entitlement information; policy and configuration data; and action, approval, decision, audit, and security-event records. For Gateway-mediated requests, Customer Attributes may also include request parameters, response metadata, and other content transmitted through the Gateway to the extent configured by Customer. The categories, location, and custody of Customer Attributes depend on the modules, connectors, Gateway deployment, hosting region, and Customer configuration stated in the Order and Documentation. During the Term, Customer grants RSA a limited, non-exclusive license to process Customer Attributes solely as reasonably necessary to provide, secure, support, and improve the Service Offering as permitted by the Agreement. Customer is responsible for the accuracy, legality, and appropriateness of Customer Attributes and for obtaining all rights, notices, consents, and authorizations required for their processing. Customer shall not intentionally submit special-category, highly sensitive, or regulated data unless the applicable Documentation expressly supports that data and Customer has configured the Service Offering accordingly. RSA shall use reasonable and appropriate administrative, technical, and physical safeguards to protect Customer Attributes in RSA's possession or control.

6. RSA OBLIGATIONS.

A. General.

For RSA-hosted components, RSA will, directly or through its cloud infrastructure providers, supply and maintain the physical facilities, power, server hardware, network infrastructure, bandwidth, physical security, environmental controls, and fire detection and suppression reasonably necessary to provide those components. Customer is solely responsible for infrastructure and controls at Customer locations and for Customer-hosted components, including Kubernetes or other runtime environments, network connectivity, capacity, hardening, availability, backup, disaster recovery, physical security, and access controls, except to the extent the Order expressly assigns a responsibility to RSA.

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.

Authentication and administrative access to RSA-hosted components will be logged as described in the then-current Documentation. Customer is responsible for retention, backup, monitoring, and lawful use of records maintained in Customer-controlled systems. Logs maintained by RSA are RSA Confidential Information but may be disclosed as necessary to comply with Applicable Law and, where reasonably available, to Customer upon written request. For Customer-hosted Gateways, per-call records are generated at the Gateway and transmitted to the RSA-hosted administrative counsel for display, subject to Customer configuration and the then-current Documentation.

Service Levels.

i. Service levels for RSA-hosted production components, if any, are specified in Exhibit 1 and the applicable Order.

ii. Service levels do not apply to Customer-hosted Gateways or other Customer-controlled components, Customer or third-party infrastructure, unsupported integrations, preview or evaluation features, or any module or capability not expressly

included in the Order.

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. The support level and fees applicable to RSA Agent ID are specified in the applicable Order. Support response targets are determined by the purchased support level and the severity of the applicable Service Request. D

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

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

A. Error Severity Classifications. All reproducible Errors in the Service Offering or Customer-Hosted Software will 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

C. Software Support Service Level Objectives (SLOs). RSA will use commercially reasonable efforts to provide support services for generally available, supported releases of the Service Offering and Customer-Hosted Software while Customer maintains an active subscription and any required Support Contract. RSA will provide technical advice and assistance according to the severity level and purchased support level. The table below sets forth target responses for Software Errors.

SUPPORT LEVEL	SEVERITY LEVEL	INITIAL TARGET RESPONSE	TARGET WORK EFFORT	TARGET COMMUNICATION FREQUENCY
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. RSA AGENT ID MODULES AND DEPLOYMENT OPTIONS.

i. Agent ID Discover. Discover is delivered as an RSA-hosted SaaS service, including the administrative experience and RSA-hosted discovery and correlation functions described in the then-current Documentation. Discover correlates supported identity, cloud, endpoint, collector, and Gateway signals to identify sanctioned and shadow agents, related non-human identities, and MCP servers and presents discovered resources in a searchable inventory. Customer administrators determine and perform remediation, registration, blocking, ownership assignment, and lifecycle actions unless a specific automated capability is generally available, documented, and enabled by Customer.

ii. Agent ID Secure. Secure applies Customer-configured policy to supported agent tool calls routed through an RSA Agent ID AI/MCP Gateway. Depending on generally available functionality and Customer configuration, the Gateway may allow a call, deny a call, or require approval by an authenticated and accountable human. Secure may evaluate supported calls and parameters, restrict delegated authority, and record attributable evidence as described in the then-current Documentation. Customer is responsible for policy design, approver authority, routing, and the consequences of each policy decision.

iii. Gateway Deployment. Secure Gateways may be RSA-hosted, Customer-hosted, or deployed in a hybrid combination, as specified in the Order and then-current Documentation. An RSA-hosted Gateway operates in RSA's cloud environment. A Customer-hosted Gateway operates in Customer's environment but, unless the Order expressly states otherwise, connects to the RSA-hosted administrative tenant for configuration, intelligence, updates, and related services.

iv. Customer-Hosted Software. Customer is responsible for deploying, operating, monitoring, scaling, backing up, and securing Customer-Hosted Software and its runtime environment; maintaining required connectivity to the RSA-hosted administrative tenant; protecting local cryptographic material; configuring logging and evidence forwarding; and ensuring that agents and resources route through the applicable Gateway. RSA is not responsible for unavailability or degradation caused by Customer-controlled infrastructure or configuration.

v. Supported Integrations. The Service Offering may interoperate with supported identity providers, cloud and endpoint sources, Gateways, governance systems, workflow tools, and SIEM platforms identified in the then-current Documentation. Integrations, connectors, APIs, and provider capabilities may change. Customer is responsible for third-party accounts, licenses, permissions, configurations, and provider charges.

vi. Subscription Metric. Unless the Order states otherwise, RSA Agent ID is licensed by Managed Identity. A "Managed Identity" means either: (i) a human user who has one or more agents acting on the user's behalf or who is enabled to create or operate agents within the Service Offering; or (ii) a fully autonomous agent operating independently and not counted under a human user. Each Managed Identity is counted once per RSA Agent ID tenant, regardless of the number of associated agents, subject to the measurement rules in the Order and Documentation.

vii. Ownership and Accountability. Customer shall assign an accountable human owner to each agent where supported, maintain current ownership and lifecycle information, and configure policies appropriate to each agent's purpose and

risk. The Service Offering assists Customer in applying controls but does not replace Customer's governance, risk-management, security, legal, or compliance program.

10. ADDITIONAL PRODUCT TERMS.

i. Human Approval. Customer determines which actions are designated high-risk, the approval policy and assurance level, the persons authorized to approve, and the consequences of approval or denial. RSA does not independently determine whether a transaction or action is lawful, accurate, appropriate, or authorized for Customer's business.

ii. Evidence and Framework Mapping. RSA Agent ID may make underlying logs, policy records, approval records, and other information available as described in the then-current Documentation. Unless a framework-mapping capability is generally available and expressly included in the Order, Customer is responsible for assembling, interpreting, and mapping that information to any legal, regulatory, contractual, or industry framework. Any future mapping functionality is a roadmap capability only and does not constitute legal advice, certification, an audit opinion, or a representation that Customer is compliant with any law, regulation, standard, or framework.

iii. Identity Provider Independence. RSA Agent ID interoperates with the third-party identity providers and with RSA identity products identified and supported in the then-current Documentation. RSA ID Plus, RSA Governance & Lifecycle, and all other RSA offerings are separate products unless expressly included in the Order. Customer is responsible for third-party accounts, licenses, permissions, configurations, and charges.

iv. Data Residency and Custody. RSA-hosted Customer Attributes are processed and stored in supported locations as described in the Order, DPA, and then-current Documentation. Data locations, key custody, record generation, retention, support access, telemetry, and connectivity vary by module and vary by deployment model. No statement in this Service Description limits cross-border processing or support access otherwise permitted under the DPA. For Customer-hosted components, Customer is responsible for validating the location, custody, security, retention, and lawful handling of data in Customer-controlled environments. For Customer-hosted Gateways, per-call records are generated at the Gateway and transmitted to the RSA-hosted administrative console for display; their processing and storage locations are governed by the applicable Order Form, DPA, hosting region, and then-current Documentation.

v. Roadmap Disclaimer. RSA may describe planned modules, features, integrations, regions, deployment models, or release dates. Roadmap information is subject to change, may not be delivered, and shall not be relied upon in making a purchase decision. Future capabilities are excluded from the Service Offering unless and until generally available and expressly included in Customer's Order.

EXHIBIT 1

CLOUD SERVICE LEVELS

I. SERVICE LEVELS FOR PRODUCTION INSTANCE.

This Section I of Exhibit 1 applies only if the applicable Order states a Production Availability Standard for specifically identified RSA-hosted, generally available production components. "Production Instance" excludes Customer-hosted Gateways, Customer-controlled components, third-party services, connectors, integrations, and preview, evaluation, beta, or non-production functions. or preview features are excluded. Availability is measured for the covered RSA-hosted components as a whole unless the Order expressly states component-specific standards. No availability commitment applies by implication. For RSA Agent ID, the Production Availability Standard is 99.95% per calendar month for the covered RSA-hosted production components as a whole. A partial outage or degradation constitutes Product Downtime only to the extent it materially prevents Customer from accessing or using the covered production functionality of the Service Offering as a whole.

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) Scheduled maintenance, service updates or emergency maintenance. Scheduled maintenance and service updates are excluded only to the extent performed within published maintenance windows or after notice consistent with the then-current Documentation. Emergency maintenance is excluded when reasonably necessary to protect the Service Offering, RSA, Customer, or others, whether or not advance notice is practicable. RSA will provide notice when commercially reasonable. No monthly maintenance cap applies unless expressly stated in the Order.
   - **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** - RSA will provide advance notice when commercially reasonable and, when advance notice is not practicable, notice as soon as reasonably possible.

   (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 excluded scheduled maintenance, service updates, and emergency maintenance during the elapsed month;
   N = actual authorized Availability in minutes for the elapsed month which is calculated as follows:
   A = the applicable Production Availability Standard stated in the Order; N = [(M – Y) x A].
   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 Level Credit as set forth below.

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 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 availability information through the RSA status page or support portal identified in the then-current Documentation.

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 a non-production instance of the Service Offering made available by RSA ("Non-Production Instance"). A Non-Production Instance supports development, testing, staging, preview, or evaluation activities and is provided only if stated in the Order or made available by RSA. Non-Production Instances are at-risk services, are not subject to an availability standard, and are not eligible for Service Level Credits.

EXHIBIT 2

SUPPORT SERVICE LEVELS

II. CUSTOMER-HOSTED COMPONENT MAINTENANCE SERVICES

A. Maintenance Services.

(i) Except as otherwise stated in the Order or Section D below (Personalized Support Options), maintenance and support for Customer-Hosted Software 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 diagnose and correct reproducible Errors in the Service Offering or Customer-Hosted Software; and

(b) Provide advice on use of the Service Offering and Customer-Hosted Software by telephone, email, and web-based technical assistance.

B. Software Updates and Upgrades. Customers current on required subscription and support fees may receive the following updates and upgrades:

(i) **Software Releases.** Updates, patches, Error corrections, and subsequent versions of Customer-Hosted Software that RSA, in its discretion: (a) deems logical improvements; (b) makes generally available to similarly situated customers; and (c) does not separately price or market.

(ii) **Customer-Hosted Component Updates.** Customer shall apply required security updates, compatibility updates, and supported-version upgrades to Customer-Hosted Software in accordance with Documentation. Customer is responsible for testing and deploying updates in Customer's environment. Use of unapproved modifications, components, or configurations may void applicable support obligations to the extent the modification causes or contributes to the issue.

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.

III. CUSTOMER-HOSTED GATEWAY SUPPORT

If an Error is identified in supported Customer-Hosted Software, RSA will use commercially reasonable efforts to provide one or more of the following remedies at RSA's discretion: configuration guidance, a workaround, a software update, a patch, or a subsequent supported Software Release.

A. **Customer Environment.** RSA does not operate Customer-hosted infrastructure and is not responsible for its capacity, availability, backup, recovery, networking, orchestration, or security. RSA may require Customer to reproduce an issue, provide diagnostic information, or test a correction in a non-production environment**.**

B. **Diagnostic Data.** Customer shall provide logs, configuration details, version information, and other diagnostic data reasonably requested by RSA. Customer shall remove or minimize personal, confidential, or regulated data not necessary to diagnose the issue and shall transmit diagnostic data using RSA-approved secure methods**.**

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 Documentation and best practices for Customer-Hosted Software, maintain supported runtime and dependency versions, preserve appropriate backup and disaster-recovery procedures, and not modify the Software or install unapproved components that materially interfere with RSA's ability to support the Service Offering**.**

V. ADDITIONAL EXCLUSIONS.

A. **Use.** Maintenance Services exclude support for Errors caused by: (i) operator error or use contrary to Documentation; (ii) unsupported software, infrastructure, models, tools, identity providers, connectors, or versions; (iii) Customer or third-party systems, networks, configurations, integrations, or data; (iv) modification or repair by anyone other than RSA or an authorized provider; (v) failure to install required updates; (vi) unusual physical, electrical, network, or environmental conditions; or (vii) accident, misuse, neglect, or causes not attributable to the Service Offering. Support also excludes an Error for which a correction is available in a supported Software Release made available to Customer.

B. **Supported Versions.** Maintenance Services exclude versions of Customer-Hosted Software that have reached end of primary support (EOPS), as determined by RSA. Customer must upgrade to a supported Software Release to continue receiving Maintenance Services unless RSA and Customer enter into a separate Extended Support agreement. Current lifecycle information is available at https://community.rsa.com/s/product-life-cycle.

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"** means a reported, reproducible malfunction or defect in the Service Offering or Customer-Hosted Software that constitutes a material non-conformity from the Documentation. RSA assigns each Error a severity level under Section II(A) of this Exhibit 2**.**

D. **"Gateway"** means an RSA Agent ID AI/MCP Gateway, whether RSA-hosted or Customer-hosted, that mediates supported agent calls and applies configured policy**.**

E. **"Product"** means the RSA Agent ID Service Offering and any Customer-Hosted Software included in Customer's Order. Products do not include evaluation or preview services unless expressly stated**.**

F. **"Production System"** means a production computing environment in which the Service Offering or Customer-Hosted Software is used for business operations, excluding development, quality-assurance, disaster-recovery testing, or other non-production purposes**.**

G. **"Relief"** means an intervention by RSA that restores material Product operations affected by an Error, including a correction, workaround, supported configuration change, or determination that the issue 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"** means Customer-Hosted Software licensed to Customer under the applicable End User License Agreement located at https://www.rsa.com/standard-form-agreements/ and made available in object-code form, including any associated configuration files or container images.

J. **"Software Release"** means a subsequent supported version of Software that RSA makes generally available to customers current on required subscription and support fees, but does not include a separately priced product or module.

EXHIBIT 3

INFORMATION SECURITY AND BUSINESS CONTINUITY PLANNING FOR RSA AGENT ID CLOUD COMPONENTS

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 involving Customer Attributes, 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, to the extent available, 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 appropriate to the data and transmission context,

including AES-256 or an equivalent strength 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. **Logical Segregation.** RSA-hosted systems used to provide the Service Offering may operate in a multitenant environment. RSA shall implement logical access controls and tenant-segregation measures designed to prevent one customer from accessing another customer's Customer Attributes. RSA shall not use production systems for development or testing in a manner that exposes Customer Attributes contrary to the 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 cloud providers used to host

RSA-hosted components of the Service Offering apply industry-standard physical security controls for their data centers, including barrier and access controls designed to protect against 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 DISASTER RECOVERY PLANNING.

For RSA-hosted production components, RSA shall maintain disaster-recovery and continuity-of-operations policies and procedures designed to support RSA's obligations under this Agreement. Customer is responsible for disaster recovery and continuity for Customer-hosted components. For RSA-hosted production components, 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. maintain a target of eight (8) hour recovery time objective ("RTO"), or such other RTO

as specified in the applicable Order, following declaration of a disaster-recovery event; the RTO is an operational objective and not a service level unless the Order Form expressly states otherwise; and

6. maintain a target recovery point objective for Customer Attributes maintained in

RSA-hosted production components of twenty-four (24) recovery point objective ("RPO"), or other RPO as specified in the applicable Order; the RPO is an operational objective and not a service level unless the Order expressly states otherwise.

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.