Service Description – Archer Engage for Vendors & Archer Engage for Business Users

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

The use of the Archer Engage for Vendors Service Offering and Archer Engage for Business Users Service Offering described herein is subject to and expressly conditioned upon acceptance of this Service Description.

This Service Description is subject to: (i) Terms of Service between RSA and Customer; or if the parties have no such agreement in place (ii) the Terms of Service currently located at https://www.rsa.com/en-us/company/standard-form-agreements ; and (iii) the applicable ordering document covering Customer's purchase of the Service Offering(s) from RSA or an RSA authorized reseller, the terms of which are incorporated herein by reference (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 subscribing to the Service Offering(s) for its internal use and not for outright resale ("Customer")) and RSA (which means (i) RSA Security LLC, if Customer is located in the United States, Mexico or South America; (ii) the local RSA sales subsidiary if Customer is located outside United States, Mexico or South America and in a country in which RSA has a local sales subsidiary; and (iii) the local Dell or EMC entity authorized by RSA 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 subsidiary; or (iv) 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 in a country in which neither RSA Security LLC nor Dell or EMC has a local sales subsidiary). Unless RSA agrees otherwise in writing, this Service Description governs the Customer's use of the Service Offering(s) except to the extent all or any portion of the Service Offering(s) is subject to a separate written agreement set forth in a quotation issued by RSA.

By proceeding with the installation or use of this Service Offering(s), 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 in 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 Agreement on behalf of the Customer, or do not accept the terms of this Agreement on behalf of the Customer, immediately cease any further attempt to use this Service Offering(s) for any purpose.

This Service Description governs the performance by RSA of certain services, as described in the Terms of Service (the "Agreement") and further described herein, in relation to the Service Offering(s) purchased by Customer generally known as "Archer Engage for Vendors" (the "Service Offering(s)") under the Agreement. Notwithstanding anything to the contrary in the Agreement, in the event of a conflict between the terms of the Agreement 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.

The Service Offering(s) is performed by RSA in an environment where Customer Content is not co-mingled with that of any other RSA customer. Service levels and operational procedures are standardized for all customers.

1. SCOPE OF SERVICES.

A. During the Term, RSA will provide the services through the World Wide Web described herein to Customer in accordance with the service levels set forth in Exhibit 1A or 1B hereof in order to allow Customer to access and use the Service Offering(s) and as further described in Exhibit 1A or 1B attached hereto. Customer's access and use of the Service Offering(s) will be subject to all those restrictions stated in the Agreement.

2. SERVICE OFFERING PACKAGES.

For Customer's purchasing the Archer Engage for Vendors Service Offering:

Archer's Third Party Risk Management use case is a prerequisite for Archer Engage for Vendors. A Customer's accepted order for the Service Offering may state additional relevant details. Archer Engage for Vendors is a US based Service Offering.

For Customer's purchasing the Archer Engage for Business Users Service Offering:

The base Archer GRC Platform is a prerequisite for Archer Engage for Busines Users. A Customer's accepted order for the Service Offering may state additional relevant details. Archer Engage for Business Users is a US based Service Offering.

A. If Customer is an on-premises RSA Archer GRC Platform Software customer, Customer acknowledges and agrees that Incidental Software must be downloaded, installed, managed, configured, and maintained by Customer to use its on-premises installation of the RSA Archer GRC Platform Software to enable Customer to use the Service Offering(s). "Incidental Software" shall mean software incidental to Customer's use of the Service Offering(s), which must be installed in Customer's on-premises environment to enable Customer to use the Service Offering(s). Customer may use that software only (a) in connection with Customer's use of the Service Offering(s), (b) for the Subscription Term, and (c) in accordance with the Agreement. If that software is subject to an accompanying license agreement, Customer must comply with the terms of that license. If that software does not have an accompanying license agreement, then Service Provider's standard end user license agreement made generally available by Service Provider on its website applies.

B. Activation. Activation of the Service Offering(s) will occur after Customer's order for the Service Offering(s) is accepted by Service Provider. If Customer is an on-premises RSA Archer GRC Platform Software customer, activation of the Service Offering(s) requires that customer obtain a license key for which the Service Offering(s) is licensed and implement said license key within Customer's on-premises RSA Archer GRC Platform Software installation appropriately. Customer shall abide by all applicable local, state, national and foreign laws, treaties and regulations in connection with Customer's use of the Service Offering(s), including those related to data privacy, international communications and the transmission of technical or personal data.

3. CUSTOMER RESPONSIBILITIES.

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 Content.

4. CUSTOMER CONTENT.

During the Term, Customer grants to RSA a limited, non-exclusive license to use the Customer Content solely for all reasonable and necessary purposes contemplated by this Service Description and for RSA to provide the Service Offering(s). Customer, not RSA, shall have sole responsibility for the accuracy, quality, integrity, legality, type, category, reliability, appropriateness and intellectual property ownership or right to use of all Customer Content. RSA shall not be responsible or liable for any deletion, destruction, damage, or loss of any Customer Content. RSA will have no visibility at upload into the types of information stored on the Service Offering(s) by Customer.

5. RSA OBLIGATIONS.

A. General.

RSA will 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(s).

B. Service Upgrades.

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

C. Backup Management.

During the Term, RSA shall perform regular backups of the Service Offering(s) to assist RSA in recovery of the Service Offering(s) in the event of a Force Majeure event affecting the Service Offering(s). Where Customer utilizes Incidental Software in connection with the Service Offering(s), Customer is responsible for backups of the Incidental Software that is under Customer's control.

D. Malware Protection.

RSA will install and run industry standard malware protection on all systems underlying the Service Offering(s) that are under RSA control. 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. Where Customer utilizes Incidental Software in connection with the Service Offering(s), Customer is responsible for malware protection on all systems underlying the Incidental Software that is under Customer's control.

E. Capacity.

RSA will provide appropriate capacity to support the Service Offering(s) stated on Customer's accepted order. Where Customer utilizes Incidental Software in connection with the Service Offering(s), Customer is responsible for providing appropriate capacity to support the Incidental Software that is under Customer's control.

F. Logging.

RSA will monitor and log use of the Service Offering(s) to produce a forensic trail supporting RSA security obligations as defined in Exhibit 2. Such logs are RSA confidential information, but will be disclosed as necessary to comply with applicable law. Where Customer utilizes Incidental Software in connection with the Service Offering(s), Customer is responsible for monitoring and logging the use of the Incidental Software that is under Customer's control.

EXHIBIT 1-A

ARCHER ENGAGE FOR BUSINESS USERS - SERVICE LEVELS

This Exhibit 1 relates to the availability of the Archer Engage for Business Users Service Offering only and does not apply to any other RSA Service Offering, product, software, maintenance/support or service.

I. SERVICE LEVELS.

1. DEFINITIONS.

In addition to those defined terms stated in the Service Description and the Agreement, the following terms and definitions shall apply to the Service Offering for the purpose of this Exhibit 1, Section I:

Term	Definition
Static Maintenance Window	The period of time every Sunday from 12:00am CST/CDT to 4:00am CST/CDT and every Wednesday from 9pm to 11:59pm CST/CDT during which maintenance may be conducted on the Service Offering. The Service Offering may be unavailable during these periods.
Scheduled Maintenance Window	Maintenance of the Service Offering that cannot be conducted during the Static Maintenance Window, where RSA has provided notice to Customer as far in advance as reasonably practical (but in no event less than two business days for non-emergency maintenance and in no event less than 24 hours for emergency maintenance) before the commencement of such maintenance, which specifies the anticipated impact of such maintenance on availability, including duration. RSA will use commercially reasonable efforts to minimize the impact of any Scheduled Maintenance Window to its customers by scheduling any such Scheduled Maintenance Windows during low utilization periods whenever reasonably practical.

Where Customer utilizes Incidental Software in connection with the Service Offering, Customer is responsible for all maintenance (including maintenance windows) of the Incidental Software that is under Customer's control.

2. SERVICE INTERRUPTIONS.

A. **Measurement.** Production Downtime of the Service Offering (as defined below) is measured from the RSA-confirmed commencement time of a Production Downtime event to the time the Service Offering is operational.

B. **Exclusions.** Unavailability of the Service Offering shall not be considered Production Downtime to the extent that it is caused by one or more of the following factors:

(i) Customer's failure to perform its obligations under the Agreement;

(ii) The written request or consent by Customer's representative to interrupt the Service Offering;

(iii) Problems with Customer-controlled systems underlying Incidental Software used in connection with the Service Offering;

(iv) Problems with Customer-controlled systems underlying RSA Archer GRC Platform Software that Customer runs on Customer premises;

(v) Problems with Customer-controlled networks, firewalls, security devices, and other such systems required for communication between Customer-controlled systems and the Service Offering;

(vi) Force Majeure Events which shall mean strikes, riots, insurrection, terrorism, fires, natural disasters, acts of God, war, governmental action, or any other cause which is beyond the reasonable control of RSA. For the avoidance of doubt RSA makes no representations or warranties whatsoever with respect to the availability of network connectivity between the IT systems of Customer to the Service Offering; and

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

3. SERVICE LEVEL STANDARD AND MEASUREMENT.

A. General. The Service Offering shall have 99.5% or higher availability on a monthly basis ("**Service Availability**"). Service Availability for each elapsed calendar month is calculated as follows:

M = total number of minutes in the elapsed calendar month;

Y = actual total minutes of : (a) Scheduled Maintenance Windows and/or (b) Static Maintenance Windows within the elapsed calendar month:

N = actual authorized Service Availability in minutes for the elapsed month which is calculated as follows:

$N = [(M – Y) \times 99.5\%]$

X = the number of minutes the Service Offering 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 Service Offering is not available ("Service Downtime").

If D>X Customer will qualify for a service credit as follows.

B. 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 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. In no event shall service credits exceed five percent (5%) of the total Fees received for the Service Offering. The Customer must request a credit from RSA in the event that a credit is due. The remedies specified in this Section 2 shall be the Customer's sole and exclusive remedies for the failure of RSA to meet its obligations of Service Availability.

C. Credit Request and Payment Procedures. To receive a Service Level Credit, Customer (for logging/tracking purposes) must make a request by sending an e-mail message to archersupport@rsa.com. Each request in connection with this Section I.3(E) must include the dates and times of the Production Downtime and must be received by RSA within five (5) business days after receiving the report described under Section I.4 below. If the Production Downtime is confirmed by RSA, Service Level Credits will be applied within two billing cycles after RSA's receipt of Customer's credit request. Credits are not refundable and can be used only towards future billing charges.

4. SERVICE LEVEL REPORTING.

To receive a report assessing RSA's performance against the Service Availability commitment during the previous month, Customer (for logging/tracking purposes) must make a request by sending an e-mail message to archersupport@rsa.com no later than the 20th day of the next month. RSA shall measure and report on minutes of Service Availability. Where Customer utilizes Incidental Software in connection with the Service Offering, Customer is responsible for all reporting related to the Incidental Software that is under Customer's control.

5. GENERAL OBLIGATIONS.

RSA will use reasonable commercial 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 Service Offering ; (ii) monitor the Service Offering for problems; (iii) identify root causes; (iv) correct problems; and (v) minimize recurrences of Service Downtime for which it is responsible. Notwithstanding anything to the contrary , should a Force Majeure Event result in Service Downtime, RSA will use best efforts to restore availability of the Service Offering. Customer is responsible for the foregoing with respect to Incidental Software under Customer's control that is used in connection with the Service Offering.

EXHIBIT 1-B

ARCHER ENGAGE FOR VENDORS - SERVICE LEVELS

This Exhibit 1 relates to the availability of the Archer Engage for Vendors Service Offering only and does not apply to any other RSA Service Offering, product, software, maintenance/support or service.

I. SERVICE LEVELS.

1. DEFINITIONS.

In addition to those defined terms stated in the Service Description and the Agreement, the following terms and definitions shall apply to the Service Offering for the purpose of this Exhibit 1, Section I:

Term	Definition
Static Maintenance Window	The period of time every Sunday from 12:00am CST/CDT to 4:00am CST/CDT and every Wednesday from 9pm to 11:59pm CST/CDT during which maintenance may be conducted on the Service Offering. The Service Offering may be unavailable during these periods.
Scheduled Maintenance Window	Maintenance of the Service Offering that cannot be conducted during the Static Maintenance Window, where RSA has provided notice to Customer as far in advance as reasonably practical (but in no event less than two business days for non-emergency maintenance and in no event less than 24 hours for emergency maintenance) before the commencement of such maintenance, which specifies the anticipated impact of such maintenance on availability, including duration. RSA will use commercially reasonable efforts to minimize the impact of any Scheduled Maintenance Window to its customers by scheduling any such Scheduled Maintenance Windows during low utilization periods whenever reasonably practical.

Where Customer utilizes Incidental Software in connection with the Service Offering, Customer is responsible for all maintenance (including maintenance windows) of the Incidental Software that is under Customer's control.

2. SERVICE INTERRUPTIONS.

A. Measurement. Production Downtime of the Service Offering (as defined below) is measured from the RSA-confirmed commencement time of a Production Downtime event to the time the Service Offering is operational.

B. Exclusions. Unavailability of the Service Offering shall not be considered Production Downtime to the extent that it is caused by one or more of the following factors:

(viii) Customer's failure to perform its obligations under the Agreement;

(ix) The written request or consent by Customer's representative to interrupt the Service Offering;

(x) Problems with Customer-controlled systems underlying Incidental Software used in connection with the Service Offering;

(xi) Problems with Customer-controlled systems underlying RSA Archer GRC Platform Software that Customer runs on Customer premises;

(xii) Problems with Customer-controlled networks, firewalls, security devices, and other such systems required for communication between Customer-controlled systems and the Service Offering;

(xiii) Force Majeure Events which shall mean strikes, riots, insurrection, terrorism, fires, natural disasters, acts of God, war, governmental action, or any other cause which is beyond the reasonable control of RSA. For the avoidance of doubt RSA makes no representations or warranties whatsoever with respect to the availability of network connectivity between the IT systems of Customer to the Service Offering; and

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

3. SERVICE LEVEL STANDARD AND MEASUREMENT.

A. General. The Service Offering shall have 99.5% or higher availability on a monthly basis ("**Service Availability**"). Service Availability for each elapsed calendar month is calculated as follows:

M = total number of minutes in the elapsed calendar month;

Y = actual total minutes of : (a) Scheduled Maintenance Windows and/or (b) Static Maintenance Windows within the elapsed calendar month:

N = actual authorized Service Availability in minutes for the elapsed month which is calculated as follows:

$N = [(M – Y) \times 99.5\%]$

X = the number of minutes the Service Offering 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 Service Offering is not available ("Service Downtime").

During the Term, if RSA fails to meet the Service Availability standard in any three consecutive months (commencing from the month where the Service Availability standard first failed), then Customer shall have the right to terminate the Service Offering.

4. SERVICE LEVEL REPORTING.

To receive a report assessing RSA's performance against the Service Availability commitment during the previous month, Customer (for logging/tracking purposes) must make a request by sending an e-mail message to archersupport@rsa.com no later than the 20th day of the next month. RSA shall measure and report on minutes of Service Availability. Where Customer utilizes Incidental Software in connection with the Service Offering, Customer is responsible for all reporting related to the Incidental Software that is under Customer's control.

5. GENERAL OBLIGATIONS.

RSA will use reasonable commercial 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 Service Offering ; (ii) monitor the Service Offering for problems; (iii) identify root causes; (iv) correct problems; and (v) minimize recurrences of Service Downtime for which it is responsible. Notwithstanding anything to the contrary , should a Force Majeure Event result in Service Downtime, RSA will use best efforts to restore availability of the Service Offering. Customer is responsible for the foregoing with respect to Incidental Software under Customer's control that is used in connection with the Service Offering.

EXHIBIT 2

INFORMATION SECURITY AND BUSINESS CONTINUITY PLANNING FOR SERVICE OFFERING(S)

1. ADHERENCE TO STANDARDS OF PROTECTION.

RSA will apply commercially reasonable efforts to carry out the following procedures to protect Customer Content. In fulfilling its obligations under this Exhibit, RSA may, from time to time, utilize 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 than those of the original terms of this Exhibit in all material respects.

For the avoidance of doubt, all terms of this Exhibit 2 apply to the Service Offering(s), not to Incidental Software controlled by Customer; Customer acknowledges and agrees that it is responsible for all appropriate information security and business continuity concerns related to Customer's use of Incidental Software.

A. Definitions.

(i) "Firewall" is an integrated collection of security measures used to prevent unauthorized electronic access to a networked computer system.

(ii) "Encryption" is a process of using an algorithm to transform data into coded information in order to protect confidentiality.

(iii) "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.

(iv) "Security Incident" means any loss of, or unauthorized or unlawful access to, acquisition of, use of, or disclosure of, Customer Content within the possession (*e.g.,* the physical or IT environment) of RSA or any Authorized Person.

(v) "Authorized Persons" means RSA's employees, contractors, or other agents who need to access Customer Content to enable RSA to perform its obligations under the Agreement, and who are bound by confidentiality and other obligations sufficient to protect Customer Content in accordance with the terms and conditions of the Agreement.

B. Breach Notification and Remediation.

In the event RSA becomes aware of a Security Incident of the Service Offering(s), RSA shall, in the most expedient time possible under the circumstances, notify Customer of the Security Incident and shall, subject to applicable laws, regulations, 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 Content, 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:

(i) Breach Notification. Within seventy-two (72) hours after 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.

(ii) Breach Remediation. Promptly implement reasonable measures necessary to address the security of RSA's systems and the security of Customer Content. If such measures include temporarily restricting access to any information, network or systems comprising the Service Offering(s) 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:

(i) Attestation. At least annually and at its own expense, RSA shall ensure that an audit of data center facilities where Customer Content is stored, processed, or transmitted by RSA is conducted according to appropriate industry security standards by an independent third party auditor and that such audit will result in the generation of an industry standard audit report (for example, SSAE-18 SOC 2, Type II, ISO 27001, or similar) ("Audit Report"). Upon Customer request and no more than once annually, RSA shall: (i) make good faith answers to an industry standard security questionnaire; and (ii) ensure that a copy of the most recent Audit Report pertaining to the Service Offering(s) is available to customer. The availability of such Audit Report shall be made under a separate non-disclosure agreement mutually agreed upon by the parties.

(ii) 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 infrastructure and systems used to provide the Service Offering(s) and upon reasonable Customer request, RSA will provide a copy of the most recent executive summary pertaining to said testing.

D. Data Security.

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

(i) Information Classification. If Customer discloses Customer's Content to Service Provider or if Service Provider accesses Customer's content as permitted by the Agreement, Customer Content shall be classified as Confidential and handled in accordance with the terms hereof.

(ii) 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 Content.

(iii) 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 Content is protected against unauthorized access or destruction. RSA shall ensure that if public key infrastructure (PKI) is used, it shall be protected by 'hardening' the underlying operating system(s) and restricting access to certification authorities.

(iv) Data Access; Transmission. RSA shall make RSA-controlled applications and systems used to process or store Customer Content 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 Content shall be protected using appropriate cryptography.

(v) Event Logging. For systems directly providing the Service Offering(s) to Customer, RSA shall maintain logs of key events that may affect the confidentiality, integrity, and/or availability of the Service Offering(s) 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 90 days and protected against unauthorized changes (including, amending or deleting a log).

(vi) 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.

(vii) Disposition of Customer Content. In the event of termination of the Service Offering(s), RSA shall use industry standard techniques (such as those detailed by NIST 800-88) designed to prevent Customer Content from being exposed to unauthorized individuals as part of the decommissioning process.

E. Computer & Network Security.

RSA shall use commercially reasonable efforts to carry out the following procedures to protect Customer Content:

(i) Server Security. Computer systems comprising the Service Offering(s) shall be dedicated solely to the provision of the Service Offering(s) and not used by RSA for development and/or testing unless required to fulfill obligations within this Agreement.

(ii) Internal Network Segment Security. Data entering the Service Offering(s)'s network from external sources shall pass through Firewalls to enforce secure connections between internal and external systems.

(iii) External Network Segment Security. The Service Offering(s)'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.

(iv) Network and Systems Monitoring. RSA shall actively monitor its networks and systems used to provide the Service Offering(s) to detect deviation from access control policies and actual or attempted intrusions or other unauthorized acts.

(v) User Authentication. RSA shall implement Processes designed to authenticate the identity of its system users through the following means:

i. User IDs. Each user of a system containing Customer Content shall be assigned a unique identification code ("User ID").

ii. Passwords. Each user of a system containing Customer Content shall use a unique password whose length, complexity, and age should be governed in accordance with industry best practices.

iii. Two-Factor Authentication for Remote Access. Remote access to systems containing Customer Content shall require the use of two-factor authentication.

iv. Deactivation. RSA User IDs shall be automatically deactivated after a technologically enforced number of unsuccessful log-in attempts. Interactive sessions shall be restricted or timed out after a technologically enforced period of inactivity. User IDs for RSA Personnel with access to Customer Content shall be deactivated promptly upon changes in job responsibilities that render such access unnecessary and during termination of employment.

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

F. System Development.

(i) Development Methodology and Installation Process.

i. Documented Development Methodology. RSA shall ensure that development activities for RSA-developed software used in the provision of the Service Offering(s) are carried out in accordance with a documented system development methodology.

ii. Documented Deployment Process. RSA shall ensure that new systems and changes to existing systems used in the provision of the Service Offering(s) are deployed in accordance with a documented process.

(ii) Testing Process. RSA shall ensure that all reasonable elements of a system (i.e. application software packages, system software, hardware and services, etc.) shall be tested at all relevant stages of the systems development lifecycle before applicable system changes are promoted to the production environment.

(iii) Customer Content in Test Environments. RSA shall ensure that Customer Content is not used within RSA test environments without Customer's prior written approval.

(iv) 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.

(i) Point of Contact. RSA shall designate an account manager with whom Customer may coordinate as an escalation point beyond typical Service Offering(s) customer support avenues available to Customer.

(ii) Data Center Facilities. The Service Offering(s) shall be housed in secure areas and protected by perimeter security 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 the data center facilities are:

i. Two-Factor Authentication. Two-factor authentication shall be required for entry on access points that are designed to restrict entry and limit access to certain highly sensitive areas.

ii. Limited Internet Access. RSA Personnel shall have access to external email and/or the Internet only to the extent required by job function in support of the Service Offering(s).CCTV Systems. Closed circuit television (CCTV) systems and CCTV recording systems shall be used to monitor and record access to controlled areas.

iii. ID Badges. Identification badges showing the bearer's name, photographic likeness and organization to which he or she belongs shall be issued and required at data center facilities at all times.

iv. Visitor Procedures. Procedures for validating visitor identity and authorization to enter the premises shall be implemented and followed, including but not limited to an identification check, issuance of a clearly-marked Visitor identification badge, host identity, purpose of visit, and recorded entry and departure times.

(i) 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(s) 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.

(ii) RSA Personnel.

i. 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(s) under this Agreement, to the extent permitted by applicable law.

ii. Training. RSA Personnel involved in the provision of the Service Offering(s) shall receive appropriate ongoing security awareness training. Such security awareness training shall be provided within one (1) month of RSA Personnel being engaged in the provision of the Service Offering(s) or prior to RSA Personnel being given access to Customer Content.

iii. Subcontractors. RSA shall require subcontractors engaged in the provision of the Service Offering(s) (other than auxiliary services that facilitate the Service Offering(s) (e.g. guard service, media destruction, etc.)) to have in place and maintain a commercially reasonable business continuity program that complies with industry best practices.

2. BUSINESS CONTINUITY PLANNING.

RSA shall ensure that the Service Offering business continuity plan ("BCP") capabilities include, at a minimum, a secure contingency site containing the hardware, software, communications equipment, and current copies of data and files necessary to perform RSA's obligations under this Agreement.

A. BCP Requirements. The BCP shall:

(i) address the relocation of affected RSA Personnel to contingency locations and the reallocation of work;

(ii) require a remote contingency site with adequate security and capacity to provide the Service Offering in accordance with the obligations of this Agreement;

(iii) require Processes designed to ensure that Customer Content and other data necessary for the performance of the Service Offering are automatically copied to a remote contingency site;

(iv) include a description of the recovery process to be implemented following the occurrence of a disaster;

(v) detail key resources and actions necessary to ensure that business continuity is maintained;

(vi) include a forty-eight (48) hour recovery time objective ("RTO") in which the Service Offering shall be recovered following the occurrence of a disaster; and

(vii) allow for the recovery of Customer Content at the remote contingency site in accordance with a twenty-four (24) hour recovery point objective ("RPO").

B. BCP Testing. At least annually and at its own expense, RSA will conduct a test of the BCP Plan. 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.

C. BCP Activation.

(i) 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. Such notification shall, as soon as such details are known, contain:

i. a description of the Force Majeure Event in question;
ii. the impact the Force Majeure Event is likely to have on the Service Offering and RSA's obligations under this Agreement;
iii. the operating strategy and the timetable for the utilization of the contingency site;
iv. the timeframe in which RSA expects to return to business as usual; and
v. crisis management escalations affecting Customer Content.

(ii) Contact Points. RSA Archer Customer Support and/or Customer's RSA account manager shall coordinate with Customer's representative for the purpose of exchanging information and detailed, up-to-date status and on-going actions on and from the occurrence of a disaster. Customer shall make sure that its representative is at all times known to RSA Archer Customer Support.

D. Subcontractors. RSA shall require subcontractors engaged in the provision of the Service Offering (other than auxiliary services that facilitate the Service Offering (e.g. guard service, media destruction, etc.)) to have in place and maintain a commercially reasonable business continuity program that complies with industry best practices.