Service Description
for
Stratus

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

The use of Stratus described herein is subject to and expressly conditioned upon acceptance of the: (i) Terms of Service between RedSeal and Customer or, if the parties have no such agreement in place, the Terms of Service for RedSeal Cloud Offerings currently located at https://www.redseal.net/standard-form-agreements/ (the "Terms of Service"); (ii) the Data Processing Addendum located at https://www.redseal.net/standard-form-agreements/ the "DPA), and (iii) the applicable ordering document covering Customer's purchase of a subscription or subscriptions to Stratus from RedSeal or a RedSeal 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 Stratus for its internal use and not for outright resale ("Customer")) and RedSeal, Inc.

By proceeding with the use of Stratus or authorizing any other person to do so, you are representing to RedSeal 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 Stratus for any purpose.

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

Service levels and operational procedures are standardized for all customers.

1. SCOPE OF SERVICES.

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

2. SERVICE OFFERING.

RedSeal Stratus is a Software as a Service (SaaS) based Cloud Security Posture Management (CSPM) solution. RedSeal Stratus provides multi-cloud inventory of resources, checks if your cloud resources are compliant, and if they are exposed to the Internet. The subscription offerings are as follows:

i. Stratus Professional
ii. Stratus Enterprise

The Service Offering is designed to protect cloud resources. Customer's accepted Order for the Service Offering will state which package has been selected by Customer.

The Service Offering is governed by the End User License Agreement located at https://www.redseal.net/standard-form-agreements/.

3. ACCOUNT ACCESS.

RedSeal will deliver to Customer an application administrator user ID, password, and other account information ("**Account Access Information**") necessary for Customer to access the Service Offering in accordance with the Agreement. Thereafter,

Customer will create and manage Account Access Information for each authorized user of the Service Offering. Customer is responsible for all activity occurring under such Account Access Information and shall abide by all applicable local, state, national, and foreign laws, treaties, and regulations ("**Applicable Laws**") in connection with Customer's use of the Service Offering, including but not limited to those related to data privacy, international communications, and the transmission of technical or personal data.

4. CUSTOMER RESPONSIBILITIES.

Customer will provide RedSeal with the cooperation, access, and detailed information reasonably necessary for RedSeal 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 RedSeal to act as project manager and as a liaison between RedSeal and Customer. RedSeal 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).

5. CUSTOMER ATTRIBUTES.

RedSeal requires access to only the following end user attributes from the Customer (collectively, "**Customer Attributes**") in order to provide the Service Offering to Customer: First Name, Last Name, Email Address, Username, Account Status, and Account Expiration. No other personally identifiable information is required in order for the Customer to access or use the Service Offering, including but not limited to, any personally identifiable information that is "sensitive" by nature or deemed "sensitive" by any Applicable Laws (such as social security numbers, credit card data, drivers' license numbers, national ID numbers, bank account numbers, and health/medical information) (collectively, "**Sensitive PII**"). During the Term, Customer grants to RedSeal a limited, non-exclusive license to use the Customer Attributes solely for all reasonable and necessary purposes contemplated by this Service Description and for RedSeal to provide the Service Offering. Customer, not RedSeal, shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use of all Customer Attributes. RedSeal shall use reasonable and appropriate administrative, technical and physical safeguards to protect the security, integrity and confidentiality of the Customer Attributes. However, for clarity, Customer acknowledges and agrees that 1) the Service Offering is not intended or designed to securely host and store any Sensitive PII, and 2) Customer shall not modify or use the Service Offering to store any such Sensitive PII or provide RedSeal with access to any Sensitive PII or information other than the Customer Attributes.

6. RedSeal OBLIGATIONS.

A. General.

RedSeal will, through its cloud infrastructure provider, supply and maintain adequate heating/cooling; electrical power; server hardware; network infrastructure and bandwidth; physical security and access controls; and professional fire detection/suppression capability necessary to provide the Service Offering. Physical infrastructure and hardware at the Customer's location are the Customer's sole responsibility to supply and maintain adequate heating/cooling; electrical power; server hardware; network infrastructure and bandwidth; physical security and access controls; and professional fire detection/suppression capability necessary to provide the Service Offering.

B. Application Upgrades.

During the Term, RedSeal 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.

RedSeal 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.

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

E. Service Levels.

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

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 RedSeal Cloud Offerings currently located at https://www.redseal.net/standard-form-agreements/.

EXHIBIT 1

CLOUD SERVICE LEVELS

I. SERVICE LEVELS FOR PRODUCTION INSTANCE.

This Section I of Exhibit 1 applies to Customer's Production Instance of the Service Offering. For purposes of this Exhibit 1, "**Production Instance**" means solely Customer's production instance of the Service Offering's cloud computing environment used solely for CSPM activities. The Production Instance shall have 99.9% or higher Availability on a monthly basis (the "**Production Availability Standard**"), calculated as set forth below. "**Availability**" means, subject to the exclusions below, solely the availability of the cloud CSPM components of the Service Offering and does not apply to any components of the Service Offering that are not delivered by RedSeal over the internet as part of the Service Offering (e.g., Incidental Software) or other RedSeal products, software, services, solutions, maintenance, or support services.

A. PRODUCTION INSTANCE INTERRUPTIONS.

1. **Measurement.** Production Downtime, as defined below, is measured from the RedSeal-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) Outage with RedSeal's service providers that are beyond the control of RedSeal;
   (v) Routinely Scheduled Maintenance, Service Updates or Emergency Maintenance. "Emergency Maintenance" means unscheduled or emergency maintenance. Total maintenance not to exceed 900 minutes per month;
   - **Routine Maintenance** - Service update maintenance window, as published, for non-featured enhancements such as bugfixes, security updates and platform maintenance. These updates are routine, and no advanced notice is provided.
   - **Service updates** - Notifications will be provided at least 24 hours in advance.
   - **Emergency Maintenance** - Notifications will be provided at least 24 hours in advance for any emergency maintenance.

   (vi) The written request or consent by Customer's representative to interrupt the Production Instance; and
   (vii) 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 RedSeal.

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

B. PRODUCTION INSTANCE SERVICE LEVEL STANDARD AND MEASUREMENT.

1. **General.** Availability for each elapsed calendar month is calculated as follows:
   M = total number of minutes in the elapsed calendar month;
   Y = actual total minutes of emergency or unscheduled maintenance which shall not exceed 240 minutes per month;
   N = actual authorized Availability in minutes for the elapsed month which is calculated as follows:
   $N = [(M - Y) \times 99.9\%]$
   X = the number of minutes the Production Instance is authorized to not be available in the elapsed month and which is calculated as follows:
   $X = M - N$
   D = the number of minutes in the elapsed month that the Production Instance is not available ("**Production Downtime**").
   If $D > X$ Customer will qualify for a service credit as follows.

If RedSeal 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 RedSeal shall issue to the Customer a service credit (a "**Service Level Credit**") in an amount equal to the percentage by which RedSeal 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 RedSeal 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 RedSeal to meet the Production Availability Standard.

C. GENERAL OBLIGATIONS.

RedSeal 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 RedSeal; (ii) monitor the Production Instance and supporting infrastructure controlled or maintained by RedSeal 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, RedSeal will focus its efforts on restoring availability of the Service Offering first to the Production Instance, and then to the Non-Production Instance.

II. NON-PRODUCTION INSTANCE.

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

III. CUSTOMER OBLIGATIONS.

A. **Documenting Errors.** Customer shall use good-faith, reasonable efforts to isolate and document Errors to enable RedSeal 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. Customer's Representative will initiate all requests for Support. The Representative must be trained, qualified and authorized to communicate all necessary information, perform diagnostic testing under the direction of the RedSeal service representative and be available during the performance of any Support if required. https://www.redseal.net/services/customer-support/

IV. ADDITIONAL EXCLUSIONS.

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

EXHIBIT 2

INFORMATION SECURITY AND BUSINESS CONTINUITY PLANNING FOR STRATUS CLOUD

I. ADHERENCE TO STANDARDS OF PROTECTION.

RedSeal will apply commercially reasonable efforts to carry out the procedures set forth in this Exhibit 1 to protect the Production Instance. In fulfilling its obligations under this Exhibit 1, RedSeal may, from time to time, use methods or procedures ("**Processes**") similar to and substantially conforming to certain terms herein. RedSeal 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 1.

A. Definitions.

1. **"Authorized Persons"** means RedSeal's employees, contractors, or other agents who need to access Customer Attributes to enable RedSeal 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 RedSeal or any Authorized Person.

B. Breach Notification and Remediation.

In the event RedSeal becomes aware of a Security Incident, RedSeal 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 RedSeal will address the Security Incident. In the event of a Security Incident, RedSeal 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 RedSeal's systems or network, RedSeal shall:

1. **Breach Notification.** Within seventy-two (72) hours after becoming aware of the Security Incident, notify Customer of the approximate date and time of the Security Incident and a summary of known, relevant facts and actions taken to rectify the Processes and address the Security Incident's effects.
2. **Breach Remediation.** Promptly implement reasonable measures necessary to address the security of RedSeal'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, RedSeal 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. RedSeal shall cooperate in good faith with Customer to allow Customer to verify RedSeal's compliance with its obligations under this clause.

C. Independent Control Attestation and Testing.

RedSeal shall employ independent third-party oversight as follows:

1. **Attestation.** At least annually and at its own expense, RedSeal shall ensure that an audit of the hosted environment where Customer Attributes are stored, processed, or transmitted by RedSeal 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 RedSeal in writing no more than once annually.
2. **Penetration Testing.** At least annually and at its own expense, RedSeal shall engage a third party testing service provider for network penetration testing of the RedSeal 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 RedSeal in writing no more than once annually.

D. Data Security. RedSeal shall use commercially reasonable efforts to carry out the following procedures to manage Customer Attributes as follows:

1. **Information Classification.** If Customer discloses Customer Attributes to Service Provider or if Service Provider accesses Customer Attributes as permitted by the Agreement, Customer Attributes shall be classified as Confidential Information and handled in accordance with the terms hereof.
2. **Encryption of Information.** Industry-standard encryption techniques (for example, public encryption algorithms such as, RC5, IDEA, RedSeal and AES) shall be used at cipher strengths no less than 128-bit or equivalent for

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

3. **Cryptographic Key Management.** RedSeal 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. RedSeal 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.** RedSeal shall make RedSeal-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, RedSeal 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 RedSeal systems.
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 RedSeal. 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, RedSeal 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 RedSeal's choosing, and a certificate of destruction shall be supplied to RedSeal by such third party promptly upon its destruction.

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

1. **Server Security.** Computer systems comprising the Service Offering shall be dedicated solely to the provision of the Service Offering and not used by RedSeal for development and/or testing unless required to fulfill obligations within this Agreement.
2. **Internal Network Segment Security.** Data entering the Service Offering's network from external sources shall pass through Firewalls to enforce secure connections between internal and external systems.
3. **External Network Segment Security.** The Service Offering's connections to the Internet shall (a) have appropriate security measures and controls applied, and (b) include an IDP that monitors data within the external network segment and information coming to Firewalls. RedSeal's IDP shall be designed to detect and report unauthorized activity prior to entering the Firewalls. RedSeal shall disable unnecessary network access points.
4. **Network and Systems Monitoring.** RedSeal 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.** RedSeal 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. RedSeal 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 RedSeal 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.** RedSeal shall provide account access to RedSeal Personnel on a least-privilege, need to know basis.

F. System Development.

1. **Development Methodology and Installation Process.**
    a) Documented Development Methodology. RedSeal shall ensure that development activities for RedSeal-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. RedSeal 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.** RedSeal 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.** RedSeal shall ensure that Customer Attributes are not used within RedSeal test environments without Customer's prior written approval.
4. **Secure Coding Practices.** RedSeal 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.** RedSeal 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.** RedSeal shall ensure that the cloud provider(s) RedSeal engages to host the Service Offering use industry best standards for physical security of their data centers such as barrier access controls (e.g., the use of guards and entry badges) that provide a physical environment secure from unauthorized access, damage, and interference.

   Additional requirements specific to Authorized Persons' access to the Service Offering are:
   a) Two-Factor Authentication. Two-factor authentication shall be required for any access to the Service Offering; and
   b) Limited Internet Access. Authorized Persons shall have access to external email and/or the Internet from within the Service Offering environment only to the extent required by job function in support of the Service Offering.
3. **Change and Patch Management.** RedSeal 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 RedSeal, its customers, and other such factors as RedSeal deems relevant.
4. **RedSeal Personnel.**
   a) Background Screening. RedSeal shall perform background checks in accordance with RedSeal screening policies on all RedSeal employees and consultants who are or will be supporting the Service Offering under this Agreement, to the extent permitted by Applicable Law.
   b) Training. RedSeal personnel involved in the provision of the Service Offering shall receive appropriate ongoing security awareness training. Such security awareness training shall be provided to RedSeal personnel being engaged in the provision of the Service Offering or prior to RedSeal personnel being given access to Customer Attributes.

II. CONTINUITY AND DIASTER RECOVERY PLANNING.

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

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

A. Testing. At least annually and at its own expense, RedSeal will perform disaster recovery, continuity of operations assessments. Upon reasonable request, RedSeal 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 RedSeal reasonably believes will impact the Service Offering or its ability to perform its obligations under this Agreement, RedSeal shall, to the extent possible, promptly notify Customer of such Force Majeure Event. 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 RedSeal's obligations;
3. the operating strategy and the timetable for the utilization of the contingency site; and
4. the timeframe in which RedSeal expects to return to business as usual.