Service Description - NetWitness® SIEM Cloud

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

The use of the NetWitness® SIEM Cloud Service Offering described herein is subject to and expressly conditioned upon acceptance of the: (i) Terms of Service between NetWitness and Customer or, if the parties have no such agreement in place, the Terms of Service for the NetWitness® SIEM Cloud Service Offerings currently located at https://www.rsa.com/en-us/company/standard-form-agreements (the "Terms of Service"); (ii) the Data Processing Addendum for NetWitness® SIEM Cloud Service Offerings located at https://www.rsa.com/en-us/company/standard-form-agreements (the "DPA), and (iii) the applicable ordering document covering Customer's purchase of a subscription or subscriptions to the NetWitness® SIEM Cloud Service from NetWitness or a NetWitness 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 subscribing to the Service Offering for its internal use and not for outright resale ("Customer")) and NetWitness (which means (i) RSA Security LLC, if Customer is located in the United States, Mexico or South America; (ii) the local NetWitness sales affiliate if Customer is located outside the United States, Mexico or South America and in a country in which NetWitness has a local sales affiliate; and or (iii) RSA Security & Risk Ireland Limited or other authorized NetWitness entity as identified on the NetWitness Quote or other NetWitness ordering document if Customer is located outside the United States, Mexico, or South America and in a country in which NetWitness does not have a local sales affiliate). Unless NetWitness agrees otherwise in writing, this Service Description and the Agreement governs Customer's use of the Service Offering except to the extent all or any portion of the Service Offering is subject to a separate written agreement set forth in a quotation issued by NetWitness.

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

This Service Description governs the provision by NetWitness of the Service Offering known as "NetWitness SIEM Cloud" 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.

A. General. During the term of Customer's subscription to the Service Offering (as set forth in the ordering document) (the "**Term**"), NetWitness will provide Customer with access to and use of the NetWitness SIEM Cloud product (the "**Service Offering**") via the internet in accordance with the service levels set forth in Exhibit 1 hereof and as further described in Exhibit 1 attached hereto. Customer's access and use of the Service Offering will be subject to all those restrictions stated in the Agreement.

2. SERVICE OFFERING.

The Service Offering is offered in a single offering with additional optional add-on offerings as set forth in the NetWitness Cloud SIEM Platform documentation located at https://docs.netwitness.rsa.com/siem/.

Incidental Software provided with the Service Offering is governed by the End User License Agreement located at https://www.rsa.com/en-us/company/standard-form-agreements. Incidental Software will be listed on the applicable ordering document and may include, but is not limited to, the RSA Identity Router and RSA Authentication Manager software.

NetWitness will provide Customers with Administrative Services as described in the NetWitness Cloud SIEM Platform documentation located at https://docs.netwitness.rsa.com/siem/, which may be updated from time to time by NetWitness.

3. ACCOUNT ACCESS.

NetWitness will deliver to Customer an application administrator user ID, password, and other account information ("**Account Access Information**" or "**Login Credentials**") 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 in connection with Customer's use of the Service Offering, including those related to data privacy, international communications, and the transmission of technical or personal data.

4. CUSTOMER RESPONSIBILITIES.

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

5. CUSTOMER ATTRIBUTES.

NetWitness 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, IP address, 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 or regulations (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 NetWitness a limited, non-exclusive license to use the Customer Attributes solely for all reasonable and necessary purposes contemplated by this Service Description and for NetWitness to provide the Service Offering. Customer, not NetWitness, shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use of all Customer Attributes. NetWitness 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 the Service Offering is not intended or designed to securely host and store any Sensitive PII.

6. NETWITNESS OBLIGATIONS.

A. General.

NetWitness 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.

B. Application Upgrades.

During the Term, NetWitness 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. Capacity.

NetWitness will provide appropriate capacity to support the Service Offering stated on Customer's accepted order and pursuant to Exhibit 1 attached hereto unless otherwise provided in the NetWitness Cloud SIEM Platform documentation located at https://docs.netwitness.rsa.com/siem/.

D. Logging.

NetWitness will monitor and log all system access to the Service Offering to produce a forensic trail that includes, but is not limited to, web server logs, application logs, system logs, and network event logs. Such logs are NetWitness confidential information but will be disclosed as necessary to comply with applicable law.

EXHIBIT 1

NetWitness SIEM Cloud Service Offering – Service Level Standards

This Exhibit 1 "Service Level Standards" supplements the Agreement and is incorporated therein. Capitalized terms not defined in this Exhibit 1 shall have the meaning ascribed to them in the Agreement. If any conflict arises between the Agreement and this Exhibit, the terms of this Exhibit shall control.

"**Availability**" as described below means the ability of NetWitness and End Users to access the User Interface of the Service Offering, perform a query, and return a result.

General. The Production Instance shall have 99.9% or higher availability on a monthly basis. "**Availability**" as described below means the ability of Customer to access the user interface of the Service Offering, perform a query, and return a result. Availability for each elapsed calendar month is calculated as follows:

Standard	Service Level Specifications
AVAILABILITY OF THE SERVICE OFFERING	99.9% Availability, excluding Scheduled Downtime (as defined below) and any Force Majeure Event, on a monthly basis (the "**Availability Performance Standard**"). Availability will be calculated on a calendar month basis.

* Availability for each elapsed calendar month is calculated as:

"M" = total number of minutes in the elapsed calendar month;
"Y" = actual total minutes of Scheduled Downtime in elapsed month:
"N" = actual authorized Availability of the Service Offering in minutes for the elapsed month which is calculated as follows:

$$N = [(M – Y) \times 99.9\%]$$

"X" = is the number of minutes the system is authorized to not be Available in the elapsed month and which is calculated as follows:

$$X = M - N$$

"D" = the total number of minutes where the Service Offering was not Available.

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

In the event that the Availability Performance Standard is not achieved such that the actual system uptime (as calculated pursuant to this section above) falls below the Availability Performance Standard during any month, then NetWitness shall issue Customer a service credit according to the following table:

Availability (as defined in this Exhibit 1)	Monthly Fee Credit

<99.9% but ≥ 99.0%	5% of all fees paid or payable by Customer for such month
<99.0% but ≥ 95%	15% of all fees paid or payable by Customer for such month
<95%	25% of all fees paid or payable by Customer for such month

If NetWitness fails to meet the Availability Performance Standard of ninety-nine-point nine percent (99.9%) for any three (3) months within a twelve (12) month rolling period (commencing from the month where the Availability Performance Standard is first failed), then Customers will have the right to request a credit pursuant to Section 3.C. below.

The Customer must request a credit from NetWitness in the event that a credit is due. The remedies specified in this Section shall be the Customer's sole and exclusive remedies for the failure of NetWitness to meet its obligations of Service Availability.

1. 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.

2. PRODUCTION INSTANCE INTERRUPTIONS.

A. **Measurement.** Production Downtime is measured from the NetWitness-confirmed commencement time of a Production Downtime event to the time the Production Instance is operational.

B. **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 failure to perform its obligations under the Agreement;

(ii) The written request or consent by Customer's representative to interrupt the Production Instance; and

(iii) Neither party shall be responsible for any delays or costs caused by acts of God (such as fires, earthquakes, floods, hurricanes, tropical storms, tornadoes, explosions and other severe acts of nature or weather), war, revolutions, acts of terrorism, epidemics, pandemics, contagions, acts of governmental authorities such as expropriation, condemnation, quarantining, executive orders and changes in laws and regulations, strikes, labor disputes or for any other cause beyond the parties' reasonable control (a "**Force Majeure Event**"). For the avoidance of doubt NetWitness makes no representations or warranties whatsoever with respect to the availability of network connectivity between the IT systems of Customer to the Service Offering.

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

3. PRODUCTION INSTANCE SERVICE LEVEL STANDARD AND MEASUREMENT.

Scheduled Downtime. As used herein, Scheduled Downtime shall mean any of the following: (i) Planned Downtime, and (ii) Emergency Downtime, as both terms are defined herein. NetWitness shall not have failed to meet the Availability Performance Standard where such failure results solely from Planned Downtime or Emergency Downtime.

A. **"Planned Downtime"** means (i) any planned outage for which Customer has received notification in advance of such occurrence of at least ten (10) days for upgrades to the Service Offering and ten (10) business days for other planned outages. NetWitness shall be limited to one instance of Scheduled Downtime per month not to exceed eight (8) hours in duration. In order to minimize as much as possible, the impact on Customer, NetWitness shall make best efforts to schedule Scheduled Downtime only between 00:00 and 08:00 EST on Sunday mornings (for US-based Customers) and between 00:00 and 08:00 BST on Sunday mornings (for any EU-based Customers) and between 00:00 and 08:00 local time on Sunday mornings (for any Asia-based Customers).

B. **"Emergency Downtime"** means any unplanned outage for which NetWitness is unable to provide notice as Scheduled Downtime, but where NetWitness has notified Customer at least twelve (12) hours in advance of such occurrence. There shall be no more than one (1) instance of Emergency Downtime in any calendar month and no more than three (3) instances of Emergency Downtime in any rolling twelve (12) month period with a duration not to exceed two (2) hours in each instance.

C. **Credit Request and Payment Procedures.** To receive a Service Level Credit, Customer must contact its account manager and/or NetWitness Customer Support at: https://community.rsa.com/t5/support-information/how-to-contact-netwitness-support/ta-p/638608 within five (5) business days after the Availability Performance Standard failed for the third (3rd) time within a twelve (12) month rolling period. Credits are not refundable and can be used only toward future billing charges. If the Production Service Interruption is confirmed by NetWitness, Service Level Credits will be applied within two (2) billing cycles after NetWitness' receipt of Customer's credit request.

4. GENERAL OBLIGATIONS.

NetWitness 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 Production Instance and supporting infrastructure controlled or maintained by NetWitness; (ii) monitor the Production Instance and supporting infrastructure controlled or maintained by NetWitness for problems; (iii) identify root causes; (iv) correct problems; and (v) minimize recurrences of missed Production Service Levels for which it is responsible. Should a Force Majeure Event result in unavailability of the Service Offering, NetWitness will focus its efforts on restoring availability of the Service Offering to the Production Instance.

5. **Capacity.** NetWitness will provide computer, storage and data egress capacity as provided in the NetWitness Cloud SIEM Platform documentation located at https://docs.netwitness.rsa.com/siem/.

6. Add-On Services.

A. Extended Retention Add-On. NetWitness will make add-on storage options available at different performance levels for different durations as described in more detail in the Service Detail.

B. Other Add-On Services. Other Add-On Services, including Professional Services, may be required by Customer and NetWitness may consider adding these as add-on services in the future. NetWitness agrees to make commercially reasonable attempts to support requests for necessary product add-ons by a written amendment to this Agreement to add the relevant information regarding the services and applicable pricing.

EXHIBIT 2

Support and Maintenance

This Exhibit 2 supplements the Agreement between the parties and specifies the obligations of NetWitness and Customer with respect to support and maintenance of the Service Offering. Capitalized terms not defined herein shall have the meaning ascribed to them in the Agreement. If any conflict arises between the Agreement and this Exhibit, the terms of this Exhibit shall control.

1. **General Support**. NetWitness shall provide Customer 24-hour 7-day 365 days per year global access to its Support Center. NetWitness will respond to Customer's notice of an escalated Error by opening a trouble ticket and assigning an appropriate technical resource, experienced with the Service Offering, in the timeframe and according to the severity level of the Error as set forth below. NetWitness will establish the initial severity level for all cases.

2. **Reporting**. NetWitness shall notify Customer promptly if it discovers an error in the Service Offering and install a bug fix, patch, or workaround when it becomes available. NetWitness will provide ongoing updates/status visibility to Customer regarding open support tickets via the support portal at https://community.rsa.com/cases. NetWitness will provide Customer with access and use of a portal for Customer to be able to monitor uptime/availability, customer use and performance metrics, and status of administrative services for the Service Offering.

3. **Error Severity Definitions**. Severity levels are defined as follows:

Level	Definition	Examples
Severity 1	**Severe Error**. Customer or workgroup cannot perform normal job functions. Customer go live will be missed if not resolved. Sale at severe risk, with no contingency plan.	System down. Data production loss. Data unavailable. Workaround unavailable. System or software will not install. Critical resource unavailable needing immediate assistance. Hot Account: very sensitive Customer needing special attention.
Severity 2	**Major functionality impact**. Degraded level of service. Workaround solution required. System cannot go live, but Customer deadline not yet at risk.	Major system function is unavailable or degraded. Repeated failures. Error will create intolerable delays if not addressed. New install with major Errors, not yet impacting go live date. Resource scheduling conflicts.
Severity 3	**Issue has or will affect Customer productivity**. Workaround exists, but error must be fixed. System can go live, but with some level of degradation that is acceptable to Customer in short term.	Failure in software component that is non-critical. Failure of redundant component. Implementation phone support required in area of unfamiliarity.
Severity 4	**No Customer business impact**.	"How to" questions

		Documentation issues Enhancement request Scheduled dial home Dial home that only requires health check.

4. **Backups**. NetWitness will ensure that a backup of VMs and OS disks is performed on a weekly basis for each Customer instance, and the data contained therein. These backups will be retained for a period of two weeks. These backups do not include ingested data.

5. **Support SLOs**. NetWitness will use reasonable commercial efforts to provide customers with technical advice and assistance in connection with their use of the Software according to severity level. NetWitness' targets for support responses to Errors based on Severity Level are located at https://community.rsa.com/t5/support-information/rsa-support-case-submission/ta-p/568011#toc-hId--437603743.

EXHIBIT 3

INFORMATION SECURITY AND BUSINESS CONTINUITY PLANNING FOR NETWITNESS SIEM CLOUD SERVICE OFFERING

1. ADHERENCE TO STANDARDS OF PROTECTION.

NetWitness will apply commercially reasonable efforts to carry out the following procedures to protect Customer Content. In fulfilling its obligations under this Exhibit, NetWitness may, from time to time, use methods or procedures ("Processes") similar to and substantially conforming to certain terms herein. NetWitness 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.

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 NetWitness or any Authorized Person.

(v) "Authorized Persons" means NetWitness' employees, contractors, or other agents who need to access Customer Content to enable NetWitness 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 NetWitness becomes aware of a Security Incident, NetWitness 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 NetWitness will address the Security Incident. In the event of a Security Incident, NetWitness 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 NetWitness' systems or network, NetWitness shall:

(i) Breach Notification. NetWitness shall notify Customer without undue delay after becoming aware of an actual Security Breach.
(ii) Breach Remediation. NetWitness will promptly implement reasonable measures necessary to address the security of NetWitness' systems and the security of Customer Content. If such measures include temporarily restricting access to any information, network or systems comprising the Service Offering in

order to mitigate against further breaches, NetWitness 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.

C. Security Development Lifecycle and Security Certification Audits.

(i) Security Development Lifecycle. NetWitness shall maintain an information security program encompassing software development and operations. NetWitness' software development lifecycle (SDLC) policy shall include commercially reasonable and industry-standard controls. For every release (typically quarterly), these controls include: threat modeling of the system; security considerations during the design phase of development; code review, approval, and change management controls for approving code which will include reviewing design security considerations (access controls, input validations, as well as other consideration against OWASP Secure Coding practices) and a review of applicable static code analysis; During the test phase of the SDLC, vulnerability scanning and automated penetration testing including API / Input fuzzing of the software will be performed and reviewed.

(ii) Security Certification and Audits. At all times during the Term of this Agreement and thereafter while there are Customers of the Service Offering, NetWitness shall maintain an Information Security Management Program (ISMP) that includes administrative, technical, and physical safeguards designed to protect assets and data related to the Service Offering from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the Service Offering: (i) risk management, (ii) security policy, (iii) organization of information security, (iv) asset management, (v) human resources security, (vi) physical and environmental security, and (vii) access control. Upon Customer's request, NetWitness shall certify that an ISMP is being maintained as required herein and shall provide Customer with an overview of such program.

(iii) NetWitness agrees that it will engage an independent third-party to conduct an audit of its ISMP and Services, including the Service Offering on an annual basis. NetWitness will provide a copy of its ISMS Statement of Applicability which shall include a SOC2 Compliance Report or industry-standard successor report demonstrating information security practices within the previous twelve (12) month period. Customer will have the right, upon written request, to review an executive summary of the findings of the security audit of NetWitness conducted by such independent third party and NetWitness shall provide Customer with any additional information that Customer requests, including but not limited to results of the independent audit of the administrative, technical, and physical safeguards set forth above. Further, if the results of such audit(s) identify material gaps or deficiencies or identify material suggested changes in performance of the Service Offering or in the ISMP, NetWitness shall mutually agree with Customer upon an appropriate and effective plan to address such identified gaps, deficiencies, and suggested changes, and then Customer will implement such plan and remediate any such issues in accordance with the plan.

(iv) At all times during the Term of this Agreement and thereafter while there are End Users of the Service Offering, NetWitness shall ensure a Security Vulnerability management program is maintained and, upon Customer request, promptly furnish evidence to Customer that an industry-recognized independent third party performs a penetration at least annually of any NetWitness software used in the Service Offering and will provide the Customer an executive summary of the most recent penetration testing, with validation that Critical and Highs have been resolved or are actively being reviewed.

D. Data Security.

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

(iii) Cryptographic Key Management. NetWitness 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. NetWitness 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. NetWitness shall require 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 methods described under "Encryption of Information".

(v) Event Logging. For systems directly providing the Service Offering to Customer, NetWitness will ensure 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 NetWitness systems. The logs shall be retained for at least 180 days and protected against unauthorized changes (including amending or deleting a log).

(vi) 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, NetWitness shall ensure Customer Content is 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 Netwitness' choosing, and a certificate of destruction shall be supplied to NetWitness by such third party promptly upon its destruction.

E. Computer & Network Security.

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

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

(ii) 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.

(iii) 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. NetWitness' IDP shall be designed to detect and report unauthorized activity prior to entering the Firewalls. NetWitness shall disable unnecessary network access points.

(iv) Network and Systems Monitoring. NetWitness 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.

(v) User Authentication. NetWitness 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. NetWitness 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 NetWitness 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.

(vi) Account Access. NetWitness shall provide account access to NetWitness Personnel on a least-privilege, need to know basis.

(vii) Endpoint Protection. NetWitness shall ensure adequate measures and tools are deployed to secure and protect equipment from malware, anti-virus, etc.

F. System Development.

(i) Development Methodology and Installation Process.

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

ii. Documented Deployment Process. NetWitness 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.

(ii) Testing Process. NetWitness 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 Instance.

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

(iv) Secure Coding Practices. NetWitness 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. NetWitness shall designate an account manager with whom Customer may coordinate as

an escalation point beyond typical Service Offering customer support avenues available to Customer.

H. Change and Patch Management. NetWitness 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 NetWitness, its customers, and other such factors as NetWitness deems relevant.

I. NetWitness Personnel.

(i) Background Screening. NetWitness shall perform background checks in accordance with NetWitness screening policies on all NetWitness employees and consultants who are or will be supporting the Service Offering under this Agreement, to the extent permitted by applicable law.

(ii) Training. NetWitness personnel involved in the provision of the Service Offering shall receive appropriate ongoing security awareness training. Such security awareness training shall be provided to NetWitness personnel being engaged in the provision of the Service Offering or prior to NetWitness personnel being given access to Customer Content.

2. BUSINESS CONTINUITY PLANNING.

NetWitnessshall 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 NetWitness' obligations under this Agreement.

A. Subcontractors. NetWitness 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.