Security Services (Ireland and United Kingdom) Service Terms

1. SECURITY SERVICES

Sungard Availability Services (Sungard AS) does not guarantee device failure time to fix. Sungard AS will maintain spare device inventory or engage and manage maintenance vendors in accordance with the terms of the underlying maintenance agreement. Sungard AS is not responsible for vendor failure to deliver parts or repairs within maintenance agreement timelines.

2. FIREWALL, IDS AND IPS LOG RETENTION

2.1. Service-Level Agreements

Agreement: Sungard AS will provide Customer online access to security logs in connection with the service purchased, Firewall, Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS) Services, for 90 days after the date of the log creation.

Remedy: If Sungard AS fails to meet the Firewall, IDS and IPS Log Retention service-level agreement (SLA), Customer is entitled to a credit equal to 10% of the Order's Monthly Fee for each month in which the failure occurred.

Service Conditions: Customer administrative access to the Sungard AS devices used to provide Security Services is not permitted. Customer may request a copy of device configuration data.

3. DDOS MITIGATION SERVICE

3.1. General

The DDoS Mitigation Service provides screening of traffic to help eliminate malicious traffic through signature analysis and dynamic profiling.

Sungard AS (or its contractor in performing this Service) will only provide DDoS Mitigation Service in conjunction with Sungard AS' Managed Internet Access.

The DDoS Mitigation Service monitors for potential distributed denial of service (DDoS) attacks by alerting, diagnosing and filtering Internet traffic for the purpose of cleaning and eliminating malicious traffic immediately prior to Sungard AS' Internet-facing routers through a process of signature analysis and dynamic profiling for up to 200 Gbps of traffic. After the 200 Gbps of traffic threshold has been reached, Sungard AS may be unable to mitigate against additional threats and bears no liability in this event.

If a Customer is deemed to be at a very high risk of high-volume attacks, the parties shall review the contracted arrangement and, if they are unable to agree, Sungard AS may suspend the Service.

3.2. Service-Level Agreements

Target: The Target is 99.95% for the mitigation to be started within 15 minutes of a high-level alert.

Remedy: Where Sungard AS fails to meet the Target set out above, the following Service Credits will apply:

Frequency	Service Credit
Incident 1	15% of Monthly Subscription Charge
Incident 2	30% of Monthly Subscription Charge
Incident 3	45% of Monthly Subscription Charge
Incident 4	60% of Monthly Subscription Charge

Some attacks are too large for the 200 Gbps Mitigation Service and, therefore, will not be deemed a breach of the SLA as they are outside of the service offering.

4. MANAGED FIREWALL AND VPN SERVICE

4.1. General

Sungard AS will provide the following for the number of firewalls identified in the Order:

(a) Firewall configuration and firewall policy changes in accordance with the completed customer design requirements (CDR) form.
(b) Resolution of detected firewall problems.
(c) Retention of firewall logs for 90 days.
(d) Creation of backup and restore firewall rules.
(e) Internet Control Message Protocol/Simple Network Management Protocol (ICMP/SNMP) monitoring.
(f) Monitoring services for device throughput and VPN outage.
(g) Customer-notification and coordination of critical patch alerts.
(h) Equipment Management Services.
(i) Installation of Sungard-AS-provided solution.
(j) LAN equipment services for a Sungard-AS-provided production switch.
(k) Customer-notification and coordination of critical patch alerts.

Customer is responsible for the software management and configuration of Customer-managed VPN endpoint(s).

Sungard AS does not monitor VPN persistence.

If Customer subscribes to dual firewalls per device (i.e., router, server, etc), Sungard AS shall provide dual firewall devices configured to provide redundancy should one of the firewalls fail to operate.

4.2. Service-Level Agreements

Agreement: Network hardware components provided by Sungard AS as part of Managed Firewall Services shall be operational and available to Customer on a monthly basis as set forth below:

Redundantly configured components	99.95%
Non-redundantly configured components	99.5%

Sungard AS shall measure the network at 5-minute intervals and, on a monthly basis, compute the number of failed measurement responses as a percentage of the total number of measurements.

Remedy: If Sungard AS fails to meet the Network Hardware SLA, Customer is entitled to a credit equal to 10% of the Order's Monthly Fee for each month in which the failure occurred.

5. THREAT MANAGER SERVICE

5.1. General

The Threat Manager Service is included within the following Sungard AS Services when they are procured on an Order by Customer:

(a) Threat Manager plus ActiveWatch
(b) Threat and Log Manager
(c) Cloud Defender

5.2. Features

Based on non-Secure Sockets Layer (SSL) traffic to Customer-identified nodes, the Threat Manager Service monitors, analyzes and logs security events in real time using hardened security appliances. The Threat Manager Service is composed of:

(a) A hardened sensor appliance
(b) Logical and dynamic system analysis
(c) Sensor tuning and optimization
(d) Ongoing threat and vulnerability signature updates
(e) Intrusion detection services
(f) Asset identification and criticality ranking
(g) Vulnerability assessments and reporting
(h) Web portal
(i) Customer-selected notification of detected threats via e-mail or page
(j) Service-software patches, upgrades and updates

Security analysts supporting the service will never directly access Customer hosts or systems. Threat Manager activities are limited to monitoring and analyzing network events, as configured by Customer. Non-invasive techniques may be used to analyze events that occurred within Customer's environment, e.g., reverse Domain Name System (DNS) lookups that may query nameservers within Customer's environment.

Threat Manager appliances can be installed within a designated Sungard AS facility or at a Customer facility. In the event the Services are provided for appliances installed in a Customer facility, Sungard AS will ship the appliances to the Customer-specified facility and Customer will:

(a) Provide, monitor and manage all installation, power, network, and physical and logical infrastructure and security requirements necessary to support the appliances.
(b) Upon termination of Service, uninstall, pack and return the security appliances in the same condition as received (normal wear and tear excepted) to Sungard AS pursuant to Sungard AS' reasonable instructions.

5.3. Service-Level Agreements

Target: Threat Manager Service will be available 99.9% of the time, measured monthly.

Remedy: If Sungard AS fails to meet the Availability SLA, Customer is entitled to a credit equal to 10% of the proportion of the Order's Monthly Fee attributable to Threat Manager Service for each month in which the failure occurred.

6. ACTIVEWATCH FOR THREAT MANAGER SERVICE

6.1. General

ActiveWatch for Threat Manager Service is included within the following Order items when they are subscribed by the Customer:

(a) Threat Manager plus ActiveWatch
(b) Threat and Log Manager
(c) Cloud Defender

Active Watch for Threat Manager Service provides access to security analysts who analyze data that is generated through the Threat Manager Service. Customer will be alerted when valid hostile traffic is identified and will be advised on potential remediation steps. Security analysts monitor the network on a 24/7/365 basis.

6.2. Service-Level Agreements

Target: Escalation to a security analyst will take place within 30 minutes of an attack or vulnerability being detected by the ActiveWatch for Threat Manager Service.

Remedy: If Sungard AS fails to meet the Availability SLA, the Customer is entitled to a credit equal to 10% of the proportion of the Order's Monthly Fee attributable to the ActiveWatch for Threat Manager Service for each month in which the failure occurred.

7. LOG MANAGER SERVICE

7.1. General

Log Manager can be purchased as an additional Service within the following Order items when they are subscribed by the Customer on an Order:

(a) Threat and Log Manager
(b) Cloud Defender

Log Manager Service: The Log Manager Service collects, stores, reports and correlates log data from Customer-identified sources within the Customer network. Log Manager is deployed with an appliance within Customer's environment, which is remotely managed by Sungard AS. Customer may log into a self-service web portal to perform log searches and run pre-defined reports. Log data is stored for a period of one year before being purged; long term storage can be purchased separately.

Log Manager LogReview Service: The LogReview Service provides analyst review of the previous day's log data which has been collected and stored by the Log Manager Service to identify and notify Customer of potential security incidents and to document such incidents as well as the actions taken.

Log Manager appliances can be installed within a designated Sungard AS facility or at a Customer facility. If the Services are provided for appliances installed in a Customer facility, Sungard AS will ship the appliances to the Customer-specified facility and Customer will:

(a) Provide, monitor and manage all installation, power, network, and physical and logical infrastructure and security requirements necessary to support the appliances.
(b) Upon termination of Service, uninstall, pack and return the security appliances in the same condition as received (normal wear and tear excepted) to Sungard AS pursuant to Sungard AS' reasonable instructions.

7.2. Service-Level Agreements

Target: The Log Manager Service will be available 99.9% of the time, measured monthly.

Remedy: If Sungard AS fails to meet the Availability SLA, Customer is entitled to a credit equal to 10% of the proportion of the Order's Monthly Fee attributable to the Log Manager Service for each month in which the failure occurred.

8. ACTIVE WATCH FOR LOG MANAGER SERVICE

8.1. General

The ActiveWatch for Log Manager Service is included within the following Order items:

(a) Cloud Defender

Active Watch for Log Manager can be purchased as an add-on Service for Threat and Log Manager.

Active Watch provides access to security analysts who analyze log data that is generated through the Log Manager Service. Customer will be alerted when valid hostile traffic is identified and will be advised on potential remediation steps. Security analysts monitor the network on a 24/7/365 basis.

8.2. Service-Level Agreement

Target: Escalation to a security analyst will take place within 30 minutes of an attack or vulnerability being detected by the ActiveWatch for Log Manager Service.

Remedy: If Sungard AS fails to meet the Availability SLA, Customer is entitled to a credit equal to 10% of the proportion of the Order's Monthly Fee attributable to the ActiveWatch for Log Manager Service for each month in which the failure occurred.

9. WEB APPLICATION FIREWALL SERVICES

9.1. General

The Web Application Firewall (WAF) Service is included within the following Order item:

(a) Cloud Defender

The Web Application Firewall Service uses security policies to determine whether web requests are legitimate or malicious. When malicious alerts and violations are identified, alerts will be sent to Customer and Sungard AS.

Customer websites will be deployed initially in "Detect" mode. In Detect mode, violations to configured policy rules will only be logged. This will be the default operating mode during the tuning phase for Customer websites. Sungard AS will monitor the out-of-band web application firewall (WAF) to tune for false positives and configure for allowed content types, denylisted and allowlisted IP addresses and SSL configuration.

Sungard AS provides WAF functionality delivering updates that are downloaded to the WAF appliance. This facilitates:

(a) HTTP monitoring to determine whether the monitored site(s) are available and responding to regular requests.
(b) HTTPS monitoring to determine whether the monitored site(s) are available and responding to regular requests.
(c) Inspection of and responses to all incoming web traffic based on the applicable Customer-defined security policy.
(d) SSL client authentication, authorization and certificate forwarding to the back-end support.
(e) Threat and vulnerability signature updates.
(f) HTTPS termination and optional re-encryption of requests before being sent to the web system.
(g) Customer-selected notification of detected threats.
(h) Hosting of logs and policy configuration in Sungard AS' third-party service provider's data center.
(i) Access to third-party web portal for Service-related reports.
(j) Monitoring of Service availability.
(k) Hardware provision, if identified on the Order.

Customer shall:

(a) Provide a list of websites and corresponding virtual hosts/domains that will be monitored.
(b) Provide up-to-date signed certificates and keys for Sungard AS to tune and configure the WAF for protection of SSL traffic.
(c) Report all operational and environment changes that may impact the performance of the Service, including, but not limited to, changes to network topology, network hardware, firewall rules and configuration and HTTP/HTTPS site code.

(d) Open specified ports on Customer's network to ensure that Sungard AS' third-party service provider has the connectivity required to deliver the Service.
(e) Provide necessary hardware meeting Sungard-AS-supported specifications, unless provided by Sungard AS as identified on the Order.
(f) Unless provided by Sungard AS under a separate Service, ensure that all physical connections and network configurations enable Sungard AS to monitor, maintain and administer the Web Application Firewall Service.

9.2. Service-Level Agreements

Target: The Web Application Firewall Service will be available 99.9% of the time, measured monthly.

Remedy: If Sungard AS fails to meet the Availability SLA, Customer is entitled to a credit equal to 10% of the proportion of the Order's Monthly Fee attributable to the Web Application Firewall Service for each month in which the failure occurred.

10. WEB SECURITY MANAGER PREMIER SERVICE

10.1. General

Web Security Manager Premier Service is purchased as a stand-alone Service (i.e., it is not included within another Service).

Web Security Manager Premier Service includes the same features as the Web Application Firewall Service as well as providing a Protect mode in which violations to configured policy rules will be blocked and logged. This will be the default operating mode following the tuning phase for Customer websites.

10.2. Service-Level Agreements

Target: The Web Security Manager Premier Service will be available 99.9% of the time, measured monthly.

Remedy: If Sungard AS fails to meet the Availability SLA, Customer is entitled to a credit equal to 10% of the proportion of the Order's Monthly Fee attributable to the Web Security Manager Premier Service for each month in which the failure occurred.

11. CLOUD DEFENDER SERVICE

11.1. General

The Cloud Defender Service combines the following Services together into one solution:

(a) Threat Manager plus ActiveWatch
(b) Log Manager
(c) ActiveWatch for Log Manager
(d) Web Application Firewall

Cloud Defender is only available on virtual appliances.

12. TWO-FACTOR AUTHENTICATION (EMEA)

12.1. General

Sungard AS will provide to the Customer managed two-factor authentication and credential validation service ("Two-Factor Authentication Service") as specified in the Order. In connection with the Two-Factor Authentication Service, Sungard AS will provide:

(a) An Identity Management Centre (IMC) base pack and organizational license to facilitate Customer set up and access to the web portal.
(b) Support via the Sungard AS Service Desk.

The Two-Factor Authentication Service is only available in conjunction with Sungard AS Hosting or Managed Services.

Customer will:

(a) Where necessary to establish the Two-Factor Authentication Service, allow online access to all authentication nodes.
(b) Allow access at all reasonable time to any Customer Equipment associated with the Two-Factor Authentication Service located within a Delivery Location.
(c) Ensure that all its end users abide by the End User Rules (which will be provided during registration) and that its end users comply with all reasonable instructions given in relation to the Two-Factor Authentication Service or its operation or delivery.
(d) Ensure that the end user of the Two-Factor Authentication Service shall keep all credentials and authentication node keys safe, secure and confidential and that such credentials and authentication node keys are not used by any unauthorized person or in an unauthorized way.
(e) Send a notification through the End User Help Desk, IMC or the Sungard AS Service Desk if any credentials or authentication node keys are or may have been compromised, or if any other potential threat to the security of the Service has been noted.
(f) Comply with any security procedures reasonably required by Sungard AS and where any records of or relating to credentials or authentication node keys are no longer needed. Then destroy them in a secure way so as to make sure that they cannot subsequently be reconstituted, read or used.
(g) Send a notification via the IMC to:
    - Terminate, amend, restrict the right of an end user to use the Two-Factor Authentication Service
    - Reassign an end-user device
    - Change a credential or authentication node
    - Add or terminate an authentication node
(h) Appoint two or more end users to act as Customer Administrators who will be responsible for:
    - Defining the security policy to be enforced on the end users
    - Ordering and cancelling services for end users
    - Changing the access permissions in respect of end users
    - Managing the operation of the authentication node(s)
    - Dealing with any billing or other commercial issues
    - Allocating and removing administration rights
    - Any other functions agreed with Sungard AS from time to time
(i) As software provided by Sungard AS will be subject to a third-party software license, Customer agrees and will ensure that any end user agrees to:
    - Comply with the license terms and conditions
    - Only use the software on the particular type of hardware on which the software is designed to be installed to receive the Two-Factor Authentication Service
    - Not to mistreat, damage or open any devices or try to reverse engineer, decompile, disassemble, translate, copy or otherwise alter the devices (or any of their technology or components); or make or use any copies of any devices other than as permitted by these terms
(j) Notwithstanding that the Two-Factor Authentication Service is provided by a third party, acknowledge and confirm that all its rights and obligations are set out in the Agreement and accordingly, it will indemnify Sungard AS against any claims made against the third-party supplier by end users in relation to the Service provided hereunder.

Sungard AS may:

(a) Suspend access to the Two-Factor Authentication Service or the operation of a particular authentication node if Sungard AS considers it necessary to maintain the security or integrity of the Service or to prevent misuse.
(b) Change the technical specification or the functionality of the Service or the design or functionality of the IMC; or a network, facility, IP address or third-party service by means of which the Service is provided as long as this does not have any material adverse effect on the standard of the Service.
(c) Change the URL of the IMC or the End User Help Desk. Customer and end users will be notified of any replacement URL on not less than 12-day notice, unless the change is required to try and ensure continuity of the Service or compliance with service levels in which circumstances, shorter notice shall be given.

13. INCIDENT RESOLUTION SERVICES

Incident Resolution Services shall be provided for those devices or Services specified in the Order as covered by Managed Services (whether Equipment Management, Operating System Management or Database Management Services), LAN Device Management Services, Microsegmentation Services or Managed Firewall Services.

Where Sungard AS detects a problem with an eligible device, Sungard AS will notify the Customer's nominated personnel (previously notified to Sungard AS in writing by the Customer from time to time for this purpose) of the problem.

Depending upon the categorisation of the problem associated with the eligible device then within the corresponding timescale to respond from Sungard AS' detection or having been notified by the Customer of the problem, Sungard AS will engage its then-available technical support personnel to assist (in conjunction with the Customer's personnel) in problem diagnosis. The Customer shall also as soon as reasonably possible, make available its personnel to assist in problem diagnosis.

Sungard AS does not give any guarantee or warranty and nor is it a condition of the Agreement that Sungard AS will be able to fix any detected or notified problem with any eligible device within any timescale, as resolution will depend upon the nature and circumstances of the problem, the Customer's timely assistance and response times from Equipment and Software vendors. However, where it is able to do so, Sungard AS will use its reasonable endeavours to fix the problem as soon as reasonably possible and will otherwise liaise with the Equipment and Software vendors, the Customer, and the Customer's suppliers to enable them to do so. Furthermore, until resolution of the problem, Sungard AS will internally escalate the problem in accordance with the escalation time flow procedures. In its attempts to remedy any problem, the Customer shall be liable to pay Sungard AS' charges in relation to provision of any additional Sungard AS Equipment or Software and any charges or costs levied by maintenance, Software or Equipment vendors that are called upon by Sungard AS in order to remedy the problem.

14. GENERAL SERVICE TERMS

These Services are also subject to the General Service Terms at https://www.sungardas.com/hubfs/_multimedia/document-file/sungardas-general-service-terms.pdf.