IBM Managed Security Services General Provisions

Services Description

Table of Contents

IBM Managed Security Services General Provisions

THIS IBM MANAGED SECURITY SERVICES GENERAL PROVISIONS SERVICES DESCRIPTION ("GENERAL PROVISIONS") APPLIES TO ALL IBM MANAGED SECURITY SERVICES. THESE GENERAL PROVISIONS ARE IN ADDITION TO THE SPECIFIC TERMS AND CONDITIONS PROVIDED IN THE SERVICES DESCRIPTIONS SELECTED IN THE ORDER DOCUMENT.

1. Scope of Services

IBM Managed Security Services (called "MSS" or "Services") is a portfolio of IBM offerings that are listed and described at the following location: http://www.ibm.com/services/us/iss/html/contracts_worldwide_landing.html

From this security services contract documents portal, Client selects the applicable country to access the documents.

Services are designed to allow an organisation to outsource the management of certain Internet security functions as further described in the applicable Services Descriptions. Services will be provided to the Client, based on the selected Services Descriptions specified in the applicable order document (called "Order Document"). Client means and includes the company, its authorised users or recipients of the Service.

Capitalised terms not defined in this Services Description ("SD") are defined in the agreement specified in the Order Document ("Agreement").

2. Definitions

Agent – a security technology supported by IBM MSS.

Alert Condition ("AlertCon") – a global risk metric developed by IBM, using proprietary methods. The AlertCon is based on a variety of factors, including quantity and severity of known vulnerabilities, exploits for such vulnerabilities, the availability of such exploits to the public, mass-propagating worm activity, and global threat activity. The four levels of AlertCon are described in the IBM Managed Security Services ("IBM MSS") Portal.

Education Materials – include, but are not limited to, lab manuals, instructor notes, literature, methodologies, electronic course and case study images, policies and procedures, and all other training-related property created by or on behalf of IBM. Where applicable, Education Materials may include participant manuals, exercise documents, lab documents and presentation slides provided by IBM.

3. Services

IBM's specific responsibilities are detailed in the individual Services Descriptions.

3.1 MSS Portal

The MSS Portal (called "Portal") provides access to an environment (and associated tools) designed to monitor and manage the security posture by merging technology and service data from multiple vendors and geographies into a common, Web-based interface.

The Portal may also be used to deliver Education Materials. All such Education Materials are licensed, not sold, and remain the exclusive property of IBM. IBM grants Client a license in accordance with the terms provided in the Portal. EDUCATION MATERIALS ARE PROVIDED "AS IS" AND WITHOUT WARRANTY OR INDEMNITY OF ANY KIND BY IBM, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF PROPRIETARY AND INTELLECTUAL PROPERTY RIGHTS.

IBM Responsibilities

IBM will:

a. provide access to the MSS Portal 24 hours/day, 7 days/week. The MSS Portal will provide:

(1) multiple levels of access for MSS Portal users which may be applied to an IBM Managed Security Service, an MSS Agent, or a group of Agent(s);

(2) security intelligence awareness and alerting;

(3) MSS Agent(s) configuration and policy details where applicable;

(4) security incident and/or service ticket information;

(5) ticketing and workflow initiation and updates;

(6) interaction with SOC analysts;

(7) a template-driven reporting dashboard;

(8) access to MSS Agent(s) logs and events where applicable;

(9) authorisation to download log data when applicable;

(10) access to Education Materials in accordance with the terms provided in the MSS Portal; and

(11) where applicable, the MSS Portal will include:

(a) the ability to parse and normalise unknown, text-based system activity logs; and

(b) the ability to create user-defined correlation rules;

b. maintain availability of the MSS Portal in accordance with the metrics provided in the section of this Services Description entitled "Service Level Agreements", "Portal Availability"; and

c. provide a username, password, URL and appropriate permissions to access the MSS Portal.

Client Responsibilities

Client agrees to:

a. utilise the MSS Portal to perform daily operational Services activities;

b. ensure Client's employees accessing the MSS Portal on Client's behalf comply with the Terms of Use provided therein including, but not limited to, the terms associated with Educational Materials;

c. appropriately safeguard Client's login credentials to the MSS Portal (including not disclosing such credentials to any unauthorised individuals);

d. promptly notify IBM if a compromise of Client's login credentials is suspected; and

e. indemnify and hold IBM harmless for any losses incurred by Client or other parties resulting from:

(1) Client's failure to safeguard Client's login credentials; and

(2) when Log Management and Alerting is included as part of Client's Service contract:

(a) Client's incorrect use of regular expressions when parsing and normalising event and log data;

(b) Client's incorrect use of user-defined correlation rules;

(c) to be responsible for parsing and normalising unknown log formats in the Portal;

(d) to be solely responsible for testing and verifying the performance of log parsers and user-defined correlation rules;

(e) to enable and disable log parsers and user-defined correlation rules utilising the Portal; and

(f) and acknowledge that:

(i) OA performance and the timely delivery of log data can be negatively affected by incorrectly written or inefficient log parsers;

(ii) IBM is not responsible for the log parsers or user-defined correlation rules that are configured and saved in the Portal; and

(iii) configuration assistance for parsing unknown log formats is not included in the Services.

3.2 Security Services Contacts

Client may choose from multiple levels of access to IBM Security Operations Centers (“SOCs”) and the MSS Portal to accommodate varying roles within Client's organisation: Authorised Security Contacts, Designated Services Contacts, and MSS Portal Users.

3.2.1 Authorised Security Contacts

IBM Responsibilities

IBM will:

a. allow Client to create up to three Authorised Security Contacts;

b. provide each Authorised Security Contact with:

   (1) administrative MSS Portal permissions to Client's MSS Agent(s) as applicable;

   (2) the authorisation to create Designated Services Contacts and MSS Portal Users; and

   (3) the authorisation to delegate responsibility to Designated Services Contacts;

c. interface with Authorised Security Contacts regarding support and notification issues pertaining to the MSS Features; and

d. verify the identity of Authorised Security Contacts using an authentication method that utilises a pre-shared challenge pass phrase.

Client Responsibilities

Client will:

a. provide IBM with contact information for each Authorised Security Contact. Such Authorised Security Contacts will be responsible for:

   (1) authenticating with the SOCs using a pre-shared challenge pass phrase;

   (2) maintaining notification paths and Client's contact information, and providing such information to IBM;

   (3) creating Designated Services Contacts and delegating responsibilities and permissions to such contacts, as appropriate; and

   (4) creating Portal users;

b. ensure at least one Authorised Security Contact is available 24 hours/day, 7 days/week;

c. update IBM within three calendar days when Client contact information changes; and

d. acknowledge that Client is permitted to have no more than three Authorised Security Contacts regardless of the number of IBM services or MSS Agent(s) subscriptions for which Client has contracted.

3.2.2 Designated Security Contacts

IBM Responsibilities

IBM will:

a. verify the identity of Designated Services Contacts using a authentication method that utilises a pre-shared challenge pass phrase; and

b. interface only with Designated Services Contacts regarding the subset of operational issues for which such contact is responsible.

Client Responsibilities

Client will:

a. provide IBM with contact information including roles and responsibilities for each Designated Services Contact. Such Designated Services Contacts will be responsible for authenticating with the SOCs using a pass phrase; and

b. acknowledge that a Designated Services Contact may be required to be available 24 hours/day, 7 days/week based on the subset of responsibilities for which it is responsible (e.g., FW Agent(s) outage).

3.2.3 MSS Portal Users

IBM Responsibilities

IBM will:

a. provide multiple levels of access to the MSS Portal, as follows:
   (1) administrative user capabilities which will include:
      (a) creating Portal users;
      (b) creating and editing custom Agent groups;
      (c) submitting policy change requests to the SOCs for a managed Agent or a group of Agents;
      (d) submitting Services requests to the SOCs;
      (e) “live chat” communicating with SOC analysts regarding specific incidents or tickets, generated as part of the Services;
      (f) creating internal Services-related tickets and assigning such tickets to Portal users;
      (g) querying, viewing, and updating Services-related tickets;
      (h) viewing and editing Agent details;
      (i) viewing Agent policies, where applicable;
      (j) creating and editing vulnerability watch lists;
      (k) performing live event monitoring, where applicable;
      (l) querying security event and log data;
      (m) scheduling downloads of security event and log data;
      (n) scheduling and running reports; and
      (o) where applicable, administrative user capabilities will also include:
         (i) parsing and normalising unknown, text-based system activity logs from operating systems and applications;
         (ii) enabling/disabling automated intelligence (“AI”) analysis alert policy rules; and
         (iii) creating custom user-defined correlation rules;
   (2) regular user capabilities which will include all of the capabilities of an administrative user, for the Agents to which they have been assigned, with the exception of creating Portal users;
   (3) restricted user capabilities which will include all of the capabilities of a regular user, for the Agents to which they have been assigned, with the exception of:
      (a) creating and submitting policy change requests;
      (b) updating tickets; and
      (c) editing Agent details;

b. provide Client with authorisation to apply levels of access to an MSS Agent or groups of MSS Agents;

c. authenticate MSS Portal Users using static password; and

d. authenticate MSS Portal Users using two-factor authentication tokens Client provides (RSA SecureID).

Client Responsibilities

Client agrees:

a. that Portal users will use the Portal to perform daily operational Services activities;

b. to be responsible for providing IBM-supported RSA SecureID tokens (as applicable); and

c. and acknowledges that the SOCs will only interface with Authorised Security Contacts and Designated Services Contacts.

3.3 Security Reporting

Utilising the Portal, Client will have access to Services information and reporting with customisable views of activity at the enterprise, work group and Agent levels. The Portal also provides Client with the ability to schedule customised reporting.

IBM Responsibilities

IBM will provide Client with access to reporting capabilities within the Portal which includes relative information associated with the MSS agent included as part of the Service. Information may include but is not limited to some or all of the following (where applicable):

a. number of SLAs invoked and met;

b. number, types, and summary of Services requests/tickets;

c. number of security incidents detected, priority and status;

d. list and summary of security incidents;

e. MSS Agent reports;

f. event correlation and analysis;

g. system logs;

h. firewall reports that include summary, traffic analysis, protocol usage, targeted IP and rule utilisation;

i. Payment Card Industry ("PCI") Audit Readiness Reports that tie system activity events on designated devices to specific PCI requirements; and

j. Advanced Analytics and Compliance reporting.

Client Responsibilities

Client agrees:

a. to generate MSS related reports using the MSS Portal;

b. to be responsible for scheduling reports (as desired); and

c. and acknowledges that assistance from a PCI qualified security assessor ("QSA") is not provided as part of the Services, but Client may contract separately with IBM to address this need (where applicable).

3.4 Security Intelligence

Security intelligence is provided by the IBM X-Force Threat Analysis Center. The X-Force Threat Analysis Center publishes an Internet threat-level. The Internet threat-level describes progressive alert postures of current Internet security threat conditions. In the event Internet threat-level conditions are elevated to AlertCon 3, indicating focused attacks that require immediate defensive action, IBM will provide Client with real-time access into IBM's global situation briefing. Utilising the MSS Portal, Client can create a vulnerability watch list with customised threat information. In addition, each MSS Portal User can request to receive an Internet assessment e-mail each business day. This assessment provides an analysis of the current known Internet threat conditions, real-time Internet port metrics data, and individualised alerts, advisories and security news.

NOTE: Client's access and use of the security intelligence provided via the Portal (including the daily Internet assessment e-mail) is subject to the Terms of Use provided therein. Where such Terms of Use conflict with the terms of this Agreement, the Portal Terms of Use shall prevail over this Agreement. In addition to the Terms of Use provided in the Portal, Client's use of any information on any links or non-IBM Web sites and resources are subject to the terms of use posted on such links, non-IBM Web sites, and resources.

IBM Responsibilities

IBM will:

a. provide access, via the MSS Portal, to the X-Force Hosted Threat Analysis Service;

b. display security information on the MSS Portal as it becomes available;

c. if configured by Client, provide security intelligence specific to Client's defined vulnerability watch list, via the MSS Portal;

d. if configured by Client, provide an Internet security assessment e-mail based on Client's subscription, each business day;

e. publish an Internet threat-level via the MSS Portal;

f. declare an Internet emergency if the daily Internet threat-level level reaches threat-level 3;

g. provide MSS Portal feature functionality to create and maintain a vulnerability watch list;

h. provide additional information about an alert, advisory, or other significant security issue as IBM deems necessary; and

i. provide access to regularly produced IBM X-Force Threat reports via the MSS Portal.

Client Responsibilities

Client will use the MSS Portal to:

a. subscribe to the daily Internet security assessment e-mail, at Client's option;

b. create a vulnerability watch list, if desired;

c. access the IBM X-Force Threat Reports; and

d. agree to adhere to the licensing agreement and not forward Services information to individuals who do not have a proper license.

3.5 Standard Services Deployment and Activation

During Standard Services Deployment and Activation, IBM will work with Client to deploy the service on a new Agent or begin management of an existing Agent.

Note: Deployment and Activation activities are performed one time during the performance of the services. If Client chooses to replace, upgrade, or move Client's Agent during the Services contract, IBM may require that such Agent be redeployed and reactivated (called “Redeployment”). Such Redeployments will be provided at an additional charge as specified in an applicable Order Document. For log and alert services Client may contract separately for IBM to provide physical installation and configuration services.

Note:Advanced Services Deployment and Activation activities are available upon request and for an additional fee. Such activities must be accompanied by a separate services description or statement of work. Examples of advanced deployment and activation may include activities such as:

a. dedicated resources/multiple resources;

b. policy design, migration, and/or conversion services;

c. network design or re-design; and

d. support for data center builds, data center transitions or data center-to-cloud transformation activities.

3.5.1 Data Gathering and Project Kickoff

IBM Responsibilities

IBM will:

a. upon receiving a service order, send Client a welcome e-mail that contains services questionnaire(s) to be completed by Client;

b. schedule a project kick-off call, for up to one hour for up to three of Client's assigned personnel, to:

   (1) introduce Client's Point of Contact to the assigned IBM MSS transition team;

   (2) review each party's respective responsibilities;

   (3) set schedule expectations; and

   (4) review and confirm;

      (a) project scope and Client's requirements;

      (b) acquired services; and

      (c) Client's business and network environment.

Client Responsibilities

Client agrees to:

a. complete the services questionnaire(s) and return them to IBM within 5 business days of receipt;

b. provide IBM with a network diagram for Client's devices to be managed by IBM;

c. obtain and provide applicable information, data, consents, decisions and approvals as required by IBM to perform the Services deployment, within two business days of IBM's request;

d. attend the project kickoff call;

e. acknowledge that IBM will not approve unplanned deployment and activation night and weekend work; and

f. be responsible for scheduling any night and weekend work, in advance, and as discussed during the project kick-off call. Night and weekend work is provided at an additional charge and subject to IBM resource availability and blackout dates.

3.5.2 Assessment

IBM Responsibilities

Upon completion of the Data Gathering and Project Kickoff activities, IBM will:

a. use the information provided in the service questionnaire(s) to assess Client's existing environment;

b. remotely assess the Agent to verify it meets IBM specifications;

c. determine Agent configuration based on the information provided in the service questionnaire(s);

d. for Agents not meeting IBM's specifications:

   (1) identify Agent software requiring upgrading, and/or

   (2) identify Agent firmware requiring upgrading, and/or

   (3) identify Agent hardware requiring upgrading to meet applicable vendor compatibility lists; and

e. identify application and user accounts to be removed or added, as applicable; and

f. determine if Agent data collection will be implemented using the Universal Log Agent ("ULA") or via SYSLOG (where applicable).

Client Responsibilities

Client agrees:

a. to ensure the existing Agent meets IBM's specifications;

b. to remove or add IBM-specified applications and user accounts, as required by IBM to perform Services;

c. if requested by IBM:
   (1) to upgrade IBM-specified Agent software to the most current IBM-supported version
   (2) to upgrade IBM-specified Agent firmware;
   (3) to upgrade IBM-specified Agent hardware; and
   (4) adjust the agents policy as requested by IBM.

d. to maintain current licensing, support and maintenance for the Agents;

e. and acknowledges:
   (1) protection provided by Agents deployed in passive mode will be substantially decreased; and
   (2) transition to an inline configuration at a later date will be considered Redeployment and is available at an additional fee.

3.5.3 Network Access Requirements

IBM Responsibilities

Upon completion of Assessment activities, IBM will:

a. provide Client with a document called “Network Access Requirements”, detailing specific technical information required for remote management and monitoring connectivity.

b. Note: IBM may make changes to the “Network Access Requirements” document, as it deems appropriate, throughout the performance of the Services.

c. connect to Client's network through the Internet, using IBM standard access methods as defined in the Network Access Requirements; and

d. if appropriate, utilise a site-to-site virtual private network (“VPN”) to connect to Client's network.

Client Responsibilities

Client agrees to:

a. review and comply with the IBM “Network Access Requirements” document during deployment and throughout the term of the contract;

b. be responsible for implementing any changes within the Clients network to facilitate connectivity by IBM based on the provided Network Access Requirements; and

c. be solely responsible for any charges incurred as a result of IBM utilising a site-to-site VPN to connect to Client's network.

3.5.4 Agent Configuration

IBM Responsibilities

Upon completion of Assessment activities, IBM will:

a. remotely configure the Agent, including configuring and hardening the OS, configuration of software and other setting based on information provided by Client in the service questionnaire(s);

b. implement and test IBM's Network Access Requirements; and

c. provide live phone support and location of vendor documents to assist Client in configuring the Agent with a public IP address and associated settings. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist.

Client Responsibilities

Client agrees to:

a. ensure Client's servers and operating systems meets or exceeds IBM specifications, as required by IBM;

b. update Agent software and/or hardware to most current IBM supported version;

c. configure the Agent with a public IP address and associated settings: and

d. assist IBM in remotely configuring the Agent (i.e., cabling, network access, etc).

3.5.5 Policy Configuration

IBM Responsibilities

Prior to Agent Integration activities, IBM will:

a. review the policy provided by Client in the service questionnaire(s);

b. stage and configure the policy based on information provided by Client in the service questionnaire(s). Note: Policy design activities are considered out-of-scope for Standard Deployment and Activation and may be provided upon request and for an additional fee.

c. provided guidance, suggestions, and corrections for the policy where needed to assist with proper functionality; and

d. tune the Agent policy where appropriate to reduce the number of erroneous alarms.

Client Responsibilities

Client agrees to:

a. provide IBM with the policy to be implemented via the completed service questionnaire(s); and

b. acknowledge that while IBM may tune the Agent policy to reduce the number of erroneous alarms during standard deployment and activation, actual policy tuning is performed over a period of time that begins after service activation.

3.5.6 Agent Integration

IBM Responsibilities

Upon completion of Agent Configuration and Policy Configuration activities, IBM will:

a. provide live support, via phone and/or e-mail, to assist Client in locating applicable vendor documents that detail physical installation procedures and cabling. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist;

b. activating the agent and registering the agent with the MSS infrastructure where appropriate; and

c. apply and implement the configured security policy to the Agent.

Note: Physical installation services are considered out-of-scope. Client may contract separately for IBM to provide physical installation services.

Client Responsibilities

Client agrees:

a. to work with IBM in locating vendor documents that detail physical installation procedures and cabling. Client will schedule such support in advance to ensure availability of an IBM deployment specialist;

b. to be responsible for the physical cabling and installation of the Agent(s);

c. to perform any IBM-specified adjustments to the layout of the network to enhance security;

d. and acknowledge:

   (1) that IBM recommends Agents be deployed inline and inside Client's firewall; and

(2) to be responsible for scheduling night and weekend work in advanced and as discussed during the project kick-off call. Night and weekend work is provided at an additional cost and subject to IBM resource availability and blackout dates.

3.5.7 Testing and Verification

IBM Responsibilities

IBM will:

a. verify management connectivity of the Agent or on-site aggregator to the IBM MSS infrastructure;

b. verify delivery of log data from the Agent to the IBM MSS infrastructure;

c. verify health and alert monitoring is reporting correctly to the IBM MSS infrastructure;

d. perform quality assurance testing of the Agent;

e. support Client in executing Services acceptance testing;

f. verify availability and functionality of the Agent in the Portal; and

g. remotely demonstrate the primary features of the Portal for up to ten of Client's personnel, for up to one hour. Additional Portal demonstrations can be made available for an additional fee.

Client Responsibilities

Client agrees:

a. to be responsible for development of all of Client's specific acceptance testing plans;

b. to be responsible for performing acceptance testing of Client's applications and network connectivity; and

c. and acknowledges:

(1) IBM does not participate in troubleshooting and or problem resolution activities that do not directly pertain to the deployment and/or health of the managed Agent subscribing to the Services;

(2) that additional acceptance testing performed by Client, or lack thereof, does not preclude IBM from setting the Agent to “active” in the SOCs for ongoing support and management; and

(3) Client is responsible for scheduling night and weekend work in advanced as determined during the project kick-off call. Night and weekend work is provided at an additional cost and subject to IBM resource availability and blackout dates.

3.5.8 Services Activation

IBM Responsibilities

IBM will:

a. assume management and support of the Agent;

b. set the Agent to “active” as part of MSS (where applicable); and

c. begin transitioning the Agent to the SOCs for ongoing management and Services support within 48 business hours of successful completion of Services acceptance testing..

Client Responsibilities

Client acknowledges that IBM will begin transitioning the Agent to the SOC within 48 hours of successful completion of Services acceptance testing.

3.6 On-Site Aggregator Implementation for Log Management and Alerting

During On-Site Aggregator Implementation for Log Management and alerting, IBM will work with Client to deploy a new Agent or begin management of an existing Agent

Note: Implementation activities are performed one time during the performance of the services. If Client chooses to replace, upgrade, or move Client's Agent during the Services contract, IBM may require that such Agent be redeployed and reactivated (called “Redeployment”). Such Redeployments will be provided at an additional charge as specified in an applicable Order Document. Implementation services are performed remotely, Client may contract separately for IBM to provide physical installation and configuration services.

The on-site aggregator (‘OA”) is a required device that Client provides. Such device is deployed at Client's location and managed and monitored by IBM MSS for an additional charge, as specified in the Order Document. IBM strongly encourages Out-of-Band (“OOB”) access to the OA, as described in the section of this Services Description entitled “Out-of-Band Access”

The basic functions of the OA are to:

a. compile or otherwise combine the security events and log data;

b. parse and normalise unknown, text-based system activity log formats for submission to the IBM MSS infrastructure;

c. compress and encrypt the security events and log data; and

d. transmit the security events and log data to the IBM MSS infrastructure.

Core features of the OA are to:

e. perform local spooling by queuing the events locally when a connection to the IBM MSS infrastructure is not available;

f. perform unidirectional log transmission. OA communication is performed via outbound SSL/TCP-443 connections;

g. perform message throttling, if configured. This limits the bandwidth from the OA to the IBM MSS infrastructure (in messages per second) to preserve bandwidth; and

h. provide transmit windows, if configured. The transmit windows enable/disable event transmission to the IBM MSS infrastructure during the timeframe specified by Client in the Portal.

3.6.1 Configure the OA

IBM Responsibilities

IBM will:

a. provide live support, via phone and e-mail, and will assist Client with the location of applicable vendor documents detailing the installation and configuration procedures for the OA operating system and IBM provided OA software. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist;

b. provide Client with hardware specifications for the OA platform;

c. provide Client with OA software and configuration settings;

d. provide Client with telephone and e-mail support to assist with the installation of the IBM-provided OA software on the hardware platform Client provides. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist;

e. at Client's request, and for an additional charge specified in the Order Document, provide software installation services; and

f. for existing platforms:

   (1) assess existing hardware configurations to ensure they meet IBM’s specification; and

   (2) identify required hardware upgrades to be provided and installed by Client.

Client Responsibilities

Client agrees:

a. to provide IBM with an external IP address for the OA;

b. to provide the hardware for the OA platform, based on IBM’s recommendations and requirements;

c. to maintain current licensing, and support and maintenance contracts for the hardware the OA is installed upon;

d. to install the IBM-provided OA software on Client's provided hardware, under the guidance of IBM;

e. to configure an external IP address and associated settings on the OA;

f. to provide IBM with the OA IP address, hostname, machine platform, application version, and Agent time zone; and

g. for existing platforms, to procure and install IBM-requested hardware upgrades.

3.6.2 Install the OA

IBM Responsibilities

IBM will:

a. provide live support, via phone and e-mail, and will assist Client with location of applicable vendor documents detailing physical installation procedures and cabling of the OA. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist;

b. remotely configure the OA to include registration of the OA with the IBM MSS infrastructure and begin the deployment and management takeover process of the OA; and

c. confirm the IBM MSS infrastructure is receiving communication from the OA.

Client Responsibilities

Client agrees:

a. to be responsible for physical installation and cabling of the OA; and

b. to schedule live support with an IBM deployment specialist in advance;

c. and acknowledges that night and weekend work must be scheduled in advance. Night and week-end work is provided at an additional cost and subject to IBM resource availability and blackout dates.

3.7 Universal Log Agent Implementation for Log Management and Alerting

During Universal Log Agent Implementation for Log Management and Alerting, IBM will work with client to deploy a new Agent or begin management of an existing Agent.

The ULA is a light-weight log collection application that runs on an Agent subscribing to the Services. The ULA gathers text-based logs locally from the Agent and securely forwards them to the OA. The OA then securely forwards the logs to the IBM MSS infrastructure for collection, long term storage, and display in the Portal.

The basic functions of the ULA are to:

a. collect events/logs locally from the Agent;

b. compress the events/log data;

c. encrypt the events/log data; and

d. securely transmit the events/logs to the OA.

Core features of the ULA are to:

a. perform generic text file data collection;

b. perform event log collection;

c. perform system information collection, which may include:

   (1) operating system (“OS”) version;

   (2) memory;

   (3) CPU;

   (4) local user accounts;

(5) network interface details;

(6) running processes; and

(7) open network sockets;

d. perform unidirectional log transmission. ULA communication is performed via outbound SSL/TCP-443 connections;

e. perform message throttling, if configured. This limits the bandwidth from the ULA to the OA, in messages per second, to preserve bandwidth; and

f. provide transmit windows, if configured. The transmit windows enable/disable event transmission to the IBM MSS infrastructure during the timeframe specified by Client in the Portal.

3.7.1 Prepare Client's Agent

IBM Responsibilities

IBM will provide Client with a list of Agents that require ULA installation.

Client Responsibilities

Client agrees:

a. to enable Client's organisations desired system, security and application-level auditing of the operating systems, or applications that will be monitored; and

b. to verify connectivity between the Agent and the OA.

3.7.2 Install the ULA

IBM Responsibilities

IBM will:

a. provide the ULA for download via the Portal; and

b. provide Client with access to the Log Management ULA Installation Guide via the Portal.

Client Responsibilities

Client agrees:

a. to download the ULA software from the Portal;

b. to install the ULA on Agent(s) subscribing to the Services; and

c. and acknowledge, to be solely responsible for all ULA installation tasks.

3.7.3 Configure the ULA

IBM Responsibilities

IBM will provide Client with instructions on how to login to the Portal and configure the Agent.

Client Responsibilities

Client agrees:

a. to login to the Portal and confirm the Agent is available and is receiving logs within three business days of ULA installation and configuration;

b. to configure the ULA with appropriate configuration settings (including: service level, site, platform, operating system and time zone;

c. to update the ULA configuration settings (including service level, site, platform, operating system and time zone), within three days of any future device modification;

d. to modify the ULA policy (if desired); and

e. and acknowledge, to be solely responsible for all ULA configuration tasks.

3.8 Non-ULA Log Collection Implementation for Log Management and Alerting

The purpose of this activity is to facilitate log collection via SYSLOG streams when it is not technically feasible or appropriate to install the ULA on an Agent.

IBM Responsibilities

IBM will:

a. provide Client with a list of Agents that require SYSLOG collection; and

b. provide the IP address of the OA to which the SYSLOG stream must be forwarded.

Client Responsibilities

Client agrees:

a. to configure the Agent to point SYSLOG streams to the OA under the guidance of IBM;

b. to login to the Portal and confirm the Agent is available and is receiving logs within three business days; and

c. and acknowledge, to be solely responsible for all SYSLOG installation tasks.

3.9 Log Management and Alerting Activation

IBM Responsibilities

IBM will:

a. activate Log Management and Alerting, by:

(1) assume support of the Agent; and

(2) transition the Agent to the SOCs for ongoing support for Log & Alert services.

Client Responsibilities

Client agrees:

a. to be responsible for development of all of Client's specific acceptance testing plans;

b. to be responsible for performing acceptance testing of Client's applications and network connectivity;

c. to verify that the logs of each Agent are available in the Portal;

d. to update the ULA configuration settings (including service level, site, platform, operating system and time zone), within three days of any future device modification; and

e. and acknowledge that additional acceptance testing performed by Client, or lack thereof, does not preclude IBM from setting the Agent to “active” in the SOCs for ongoing support and management.

3.10 Redeployment and Reactivation

IBM Responsibilities

During Redeployment and Reactivation, IBM will work with Client to replace, upgrade, or move an MSS Agent.

Note: Redeployment and Reactivation activities are performed on a one time basis. If Client chooses to replace, upgrade, or move its MSS Agent during the Services contract, IBM may require that such MSS Agent be redeployed. Such Redeployment and Reactivation will be provided at an additional charge via a Contract Change Request. Redeployment and Reactivation charges apply only to hardware replacements, upgrades, or moves initiated by Client. Such charges do not apply to MSS Agent failures resulting in Agent Return Material Authorisation (”RMA”) activities.

IBM will provide Redeployment and Reactivation activities as per the “Standard Services Deployment and Activation” sections of this document and for the charge specified in the Order Document.

Client Responsibilities

Client will assume and acknowledge Redeployment and Reactivation activities as per the “Standard Services Deployment and Activation sections of this document.

Note: For Log and Alert services Client may contract separately for IBM to provide physical installation and configuration services.

3.11 Security Event and Log Collection

Security Event and Log Collection will be provided as part of MSS, except where the Managed Security Information and Event Management is involved. IBM utilises the X-Force Protection System for collecting, organising, and storing logs. Logs will be viewable in the Portal for the retention period specified in the Order Document. At the end of the retention period specified in the Order Document, the data will be permanently deleted.

3.11.1 Log Storage

IBM Responsibilities

IBM will:

a. uniquely identify, collect and store logs generated by the Agent(s) as such data reaches the IBM MSS infrastructure;

b. where supported, utilise custom or standard parsers to normalise logs for display and storage;

c. provide storage and display of logs via the Portal for the retention period specified in the Order Document;

d. irrevocably delete logs using a first in, first out (“FIFO”) method:

   (1) based on the retention period specified in the Order Document; or

   (2) when the log data age has exceeded seven years;

   - Notwithstanding any retention periods defined by Client, IBM will not retain log data for more than seven years. If Client exceeds Client's seven year retention period at any time during the contract period, IBM will purge the logs using the FIFO method; and

e. if it deems it appropriate, recommend a site-to-site VPN be utilised to encrypt traffic that is not natively encrypted by the Agent(s).

Client Responsibilities

Client agrees:

a. to use the Portal to review log data;

b. to use the Portal to maintain available log storage space awareness;

c. and acknowledges that:

   (1) IBM will store the logs for the retention period specified in the Order Document;

   (2) if the Services are terminated for any reason whatsoever, IBM will be relieved of its obligation to store Client's log data;

   (3) all log data will be transmitted to the IBM MSS infrastructure via the agreed upon transport method;

   (4) should Client choose not to utilise an IBM-recommended site-to-site VPN for Agent(s) that does not provide encryption algorithms natively, log data transmitted via the Internet will not be encrypted;

   (5) IBM only stores logs that successfully reach the IBM MSS infrastructure;

(6) IBM does not guarantee the legal submission of any logs into any domestic or international legal system. Admissibility of evidence is based on the technologies involved and Client's ability to prove proper data handling and chain of custody for each set of data presented;

(7) Client's defined retention periods may not exceed seven years, since IBM will not store log data for more than seven years; IBM will delete logs using the FIFO method when the age of the log exceeds seven years, regardless of Client's specified retention periods; and

(8) IBM may use the logs collected by the Service for the purposes of: a) identifying trends, and b) real or potential threats. IBM may compile or otherwise combine this information with that of other customers so long as such data is compiled or combined in a manner that will not in any way reveal the data as being attributable to Client.

3.12 Automated Analysis

Automated Analysis will be provided as part of MSS, except where the Managed Security Information and Event Management is involved. Agents are capable of generating a high volume of alarms in response to the security conditions they are configured to detect. The actual security risk corresponding to a particular condition detected is not always clear, and it is not practical to block all data that may be harmful as the default.

IBM has developed and maintains proprietary analysis engines as part of the X-Force Protection System. Logs are submitted to the analysis engines for correlation and alerting, as they are collected.

The analysis engines perform the following basic functions:

- correlates both real-time and historical logs;
- utilises statistical and rules-based analysis techniques;
- leverages raw, normalised and consolidated data; and
- operates on application and operating system logs.

X-Force Protection System alerts are made available to Client via the MSS Portal. IBM will send Client an hourly X-Force Protection System alert notification e-mail, summarising the alerts, if Client selects this option in the Portal.

Automated analysis and the subsequent alerts generated by the X-Force Protection System are available only on IBM-specified platforms.

IBM Responsibilities

IBM will:

a. submit collected log data to the X-Force Protection System analysis engines for correlation and alerting;

b. when Log Management and Alerting is included as part of Client's Service contract, utilise user-defined correlation rules that are enabled for analysis and alerting;

c. display applicable alerts generated by the X-Force Protection System analysis engines in the MSS Portal, as such alerts become available; and

d. if configured by Client, deliver X-Force Protection System alert notification within the timeframes established in the section of this Services Description entitled “Service Level Agreements”, “Security incident alert notification”.

Client Responsibilities

Client agrees:

a. to be responsible for enabling/disabling applicable AI analysis engine rules, using the MSS Portal;

b. to be responsible for scheduling X-Force Protection System alert notification, using the MSS Portal;

c. and acknowledge:

(1) the Portal can be used to monitor and review alerts generated by the X-Force Protection System analysis engines; and

(2) that automated analysis is available only on IBM-specified platforms or the log sources Client normalise utilising the custom log parser (where applicable).

3.13 Threat Analyst Monitoring and Notification

Threat Analyst Monitoring and Notification will be provided as part of MSS, except where the Secure Web Gateway ("SWG") and FW components are involved. IBM MSS security analysts will perform monitoring and analysis alerts generated by the X-Force Protection System which result from automated analysis performed on supported log data. Whether or not an alert is considered a security incident is determined solely by IBM. Alerts will be classified, prioritised, and escalated as IBM deems appropriate. Alerts that are not eliminated as benign are classified as a security incident ("SI").

Security incidents ("SI") are classified into one of the three priorities described below:

- SI – Priority 1

  Investigations that result in a high priority classification (i.e., Priority 1) require immediate defensive action.

- SI – Priority 2

  Investigations that result in a medium priority classification (i.e., Priority 2) require action within 12 - 24 hours of notification.

- SI – Priority 3

  Investigations that result in a low priority classification (i.e., Priority 3) require action within 1 – 7 days of notification.

IBM Responsibilities

IBM will:

a. request modification to the Agent configuration, to be implemented by Client, if the current policy prevents the SOC from processing log data satisfactorily and the device is not under management by the IBM MSS SOC;

b. perform investigation and analysis of alerts;

c. when possible, eliminate false positives and benign triggers and classify them as commented security incidents ("CSI");

d. identify alerts that are not eliminated as benign triggers and classify such alerts as security incidents ("SI's"):

   (1) start the SLA timers; and

   (2) prioritise the SI as either high, medium or low;

e. using the standard notification path that Client provides, escalate SIs to an Authorised Security Contact or Designated Services Contact based on IBM security notification "best practices" within the time frame and using the medium (for example e-mail or telephone) established in the section of this Services Description entitled "Service Level Agreements", "Security Incident Notification";

f. provide remediation/countermeasure recommendations, if applicable;

g. document details of CSIs and SIs in the IBM ticketing system; and

h. list CSIs and SIs in the Portal.

Client Responsibilities

Client agrees:

a. to implement MSS requested policy changes to the Agent prior to the next monitoring period, if the device is not under management by IBM;

b. to utilise the MSS Portal for investigation of logs and events that are not considered to be immediate threats;

c. to provide IBM with current in-depth documentation of Client's environment;

d. to update IBM within three calendar days of changes within Client's environment;

e. to provide IBM with the following information, and keep such information current via the MSS Portal;
   (1) information about critical servers (for example, name, platform, operating system (“OS”), Internet protocol (“IP”) address and network segment type);
   (2) information about monitored networks;
   (3) information about devices utilising network address translation (‘NAT”) (for example, name, platform, OS, and network segment type);
   (4) proxy servers; and
   (5) authorised scanners;
f. to provide and keep current a linear contact notification path, including telephone numbers and e-mail addresses;
g. to update IBM, via the MSS Portal, within three calendar days of a change in Client's contact information;
h. to provide e-mail aliases, as necessary, to facilitate notification;
i. to ensure an Authorised Security Contact or Designated Services Contact listed in the notification path is available 24 hours /day, 7 days / week;
j. to view details of CSIs and SIs via the MSS Portal;
k. to work with IBM to optimise the monitoring service;
l. to provide feedback on CSIs and SIs via the MSS Portal; and
m. and acknowledges that:
   (1) once IBM has escalated an SI, Client is solely responsible for all SI incident responses, and remediation activities;
   (2) not all investigations of alerts will result in the declaration of an SI;
   (3) Alert Monitoring and Notification applies only to alerts resulting from automated analysis performed against applicable agents;
   (4) lack of feedback can result in a lower prioritisation of persistent or recurring activity; and
   (5) if Client does not make the requested policy modifications prior to the next monitoring period, the Security Incident Notification SLA established in the section of this Services Description entitled “Service Level Agreement” will be null and void.

3.14 Policy Management

Policy Management will be provided as part of MSS and IBM defines a single rule-based Agent policy/configuration change as any authorised request for the addition or modification of one rule on one context with five or fewer objects in a single request. A change request requiring the addition of six or more objects or the manipulation of two or more rules will be counted as two or more requests. If the request applies to changes outside of the rule-based Agent policy, each submitted request will be considered a single change. IBM will provide the following services where applicable.

Client may configure the managed Agent with a single global policy that applies to all Agents.

IBM Responsibilities

IBM will:

a. accept policy change requests up to the designated number of changes selected by Client per month from Authorised Security Contacts or Designated Services Contacts, via the MSS Portal;
b. acknowledge policy change requests via the MSS Portal within the timeframes established in the section of this Services Description entitled “Service Level Agreements”, “Policy change request acknowledgement”;
c. review submitted policy change requests to verify Client has provided all required information in such requests;
d. if necessary, notify the submitter that additional information is needed. During this time, service level agreement (“SLA”) timers will be placed on hold;

e. prepare and review the policy change configuration as requested by Client;

f. implement policy change requests within the time specified in the Order Document as the Time to Implement which is selected by Client when initiating Client's change request through the MSS Portal. Time to Implement options are established in the section of this Services Description entitled "Policy change request implementation";

g. document details of the policy change request in the IBM MSS ticketing system;

h. display policy change request tickets in the Portal;

i. rollover any unused policy change requests from the current month to the next month; rollover policy change requests will be available for use until the last day of the following month, at which point, if unused, these rollover policy change requests will expire;

j. at Client's request, and for an additional charge (and subject to availability of IBM resource), provide up to the number of policy changes as specified in the Order Document;

k. perform daily configuration backup of the managed Agent;

l. maintain 14 configuration backups;

m. display the current configuration of the Agent in the MSS Portal (where applicable); and

n. on a quarterly basis upon Client's written request:

(1) audit Client's policy settings to verify accuracy; and

(2) work with Client to review Agents under management and provide recommended changes to the network protection strategy.

Client Responsibilities

Client agrees:

a. to ensure all policy change requests are submitted by an Authorised Security Contact or a Designated Services Contact, using the Portal, in accordance with the established procedures identified above;

b. to be responsible for providing sufficient information for each requested policy change to allow IBM to successfully perform such change;

c. to be responsible for notifying IBM if Client wishes IBM to perform a quarterly policy review;

d. to be solely responsible for Client's own security strategy, including security incident response procedures; and

e. and acknowledges:

(1) all policy changes will be completed by IBM and not by Client;

(2) implementation of policy changes that IBM has deemed as having an adverse impact on the Agents' ability to protect the network environment will result in the suspension of applicable SLAs;

(3) following closure of a calendar month, unused changes will be used upon request by Client for an extended period of 30 days. After this 30 day period, these changes will no longer be available. Unused policy changes that have rolled over to the following month will be used first before using the new month's policy changes;

(4) to clearly identify a policy change that requires an emergency implementation when submitting such a request in the Portal; and

(5) to contact the SOC via telephone, following submission of an emergency policy change request using the MSS Portal, to escalate such policy change request to an emergency status.

3.15 Out-of-Band Access

Out-of-Band ("OOB") access is a highly recommended feature that assists the SOCs if connectivity to an Agent is lost when an Agent is managed by IBM and installed at a client location. If such connectivity

problems occur, the SOC analyst can dial into the modem to verify the Agent is functioning properly and assist in determining the source of the outage before escalation to Client.

IBM strongly encourages OOB access to an OA or an Agent installed at a client location is managed by IBM, as described below.

IBM Responsibilities

At Client's request, and for no additional charge, IBM will:

a. provide live support, via phone and/or e-mail, to assist Client in locating applicable vendor documents which detail physical installation procedures and cabling;

b. configure the OOB device to access the managed Agents; or

c. work in good faith with Client to utilise an IBM-approved existing OOB solution.

Client Responsibilities

Client agrees:

a. to use the Portal to review log data;
   (1) to purchase an IBM-supported OOB device;
   (2) to physically install and connect the OOB device to the Agent;
   (3) to provide a dedicated analog telephone line for access;
   (4) to physically connect the OOB device to the dedicated telephone line and maintain the connection;
   (5) to be responsible for all charges associated with the OOB device and telephone line; and
   (6) to be responsible for all charges associated with the ongoing management of the OOB solution;

b. for existing OOB solutions:
   (1) to ensure the solution does not allow IBM to access non-managed devices;
   (2) to ensure the solution does not require installation of specialised software;
   (3) to provide IBM with detailed instructions for accessing managed Agents; and
   (4) to be responsible for all aspects of managing the OOB solution;

c. and acknowledge that existing OOB solutions must be approved by IBM;

d. to maintain current support and maintenance contracts for the OOB (as required);

e. to be responsible for performing all remote configuration activities for OOB and all OOB troubleshooting, if Client elects not to implement an OOB solution or if the OOB solution is unavailable for any reason; and

f. and acknowledge that if Client chooses to deploy the Services without OOB access to an OA or an Agent installed at a client location that is managed by IBM , or if OOB access is not available to IBM for any reason, then:
   (1) IBM is relieved of all SLAs which are directly influenced by the availability of such access;
   (2) IBM may require additional time to troubleshoot and/or maintain Client's devices; and
   (3) Client will be required to provide on-site assistance with configuration, problem solving, device updates, troubleshooting and/or any other situation that would typically be performed using OOB access.

3.16 Other Client Responsibilities

3.16.1 Client Point of Contact Responsibilities

Prior to the start of the Services, Client will designate a person ("Client Point of Contact"), to whom all non-technical communications relative to the Services will be addressed and who will have the authority to act on Client's behalf for all matters described in this SD. Client Point of Contact will:

a. serve as the interface between IBM's project team and all of Client's departments participating in the Services;

b. obtain and provide applicable information, data, consents, decisions and approvals as required by IBM to perform the Services, within two business days of IBM's request; and

c. help resolve Services issues and escalate issues within Client's organisation for resolution.

3.16.2 Client General Responsibilities

IBM's performance is dependent upon Client's management and fulfillment of Client's responsibilities under this SD and the Agreement, at no charge to IBM. Client will:

a. make appropriate personnel available to assist IBM in the performance of IBM's responsibilities;

b. ensure that current maintenance, license, and other applicable agreements are in place with third parties whose work may affect IBM's ability to provide the Services. Unless specifically agreed to otherwise in writing, Client is responsible for the management and performance of the third parties and for any third party hardware, software or communications equipment used in connection with the Services;

c. acquire and maintain IBM-defined levels of maintenance for all Products and any other hardware and software products which IBM manages for the Services Recipient. The service level agreements, specified in the Services Descriptions, will not apply for any period during which the IBM-defined levels of maintenance are not available or for any period during which IBM is unable to leverage existing support and maintenance contracts on Client's behalf (i.e., the vendor will not engage with IBM on Client's behalf). The Services Recipient may purchase such maintenance through its IBM Business Partner, IBM, or from third parties;

d. agree that IBM may process the business contact information of Client's employees and contractors and information about Client as a legal entity (contact information) in connection with IBM Products and Services or in furtherance of IBM's business relationship with Client. This contact information can be stored, disclosed internally and processed by International Business Machines Corporation and its subsidiaries, Business Partners and subcontractors wherever they do business, solely for the purpose described above provided that these companies comply with applicable data privacy laws related to this processing. Where required by applicable law, Client has notified and obtained the consent of the individuals whose contact information may be stored, disclosed internally and processed and will forward their requests to access, update, correct or delete their contact information to IBM who will then comply with those requests;

e. obtain any necessary consents and take any other actions required by applicable laws, including but not limited to data privacy laws, prior to disclosing any of Client's employee information to IBM. Client also agrees that with respect to data that is transferred or hosted outside of the country or countries specified in the Order Document(s), Client is responsible for ensuring that all such data transmitted outside of the country or countries specified in the Order Document(s) adheres to the laws and regulations governing such data;

f. if making available to IBM any facilities, software, hardware or other resources in connection with IBM's performance of Services, obtain at no cost to IBM any licenses or approvals related to these resources that may be necessary for IBM to perform the Services. IBM will be relieved of its obligations that are adversely affected by Client's failure to promptly obtain such licenses or approvals. Client agrees to reimburse IBM for any reasonable costs and other amounts, including costs of litigation and settlements, that IBM may incur from Client's failure to obtain these licenses or approvals;

g. be responsible as sole Data Controller for complying with all applicable data protection or similar laws such as EU Directive 95/46/EC and laws implementing that Directive that regulate the Processing of any Personal Data and special categories of data that are provided by or through Client to IBM as such terms are defined in that Directive. Client is solely responsible for determining the purposes and means of processing Client's Personal Data by IBM under this SD and the Agreement, including that such processing according to Client's instructions will not place IBM in breach of applicable data protection laws. Prior to processing, Client will inform IBM about any special categories of data contained within Client's Personal Data and any restrictions or special requirements

in the processing of such special categories of data, including any cross border transfer restrictions. Client is responsible for ensuring that the Services as described in this SD and the Agreement meet such restrictions or special requirements. Client appoints IBM as data processor and IBM will follow Client's reasonable data processing instructions and only process Client's Personal Data in a manner which is reasonably necessary to provide the Services and only for that purpose. IBM will apply the security measures as set forth in this SD and the Agreement or as notified to IBM in writing in advance. Client is responsible for determining that these measures provide an appropriate level of protection. On termination or expiry of this SD or the Agreement, IBM will destroy or return to Client all Client's Personal Data. If Client is, or Client's Data Controller is, required by applicable data protection laws to provide information about or access to Client's Personal Data to an individual or to the relevant authority, IBM will reasonably cooperate with Client in providing such information or access; Client agrees that IBM may perform such processing as IBM reasonably considers necessary or appropriate to perform the Services, and Client appoints IBM and, as appropriate, IBM subcontractors, each as a data processor according to these terms;

h. agree that when IBM reasonably determines it is useful in its provision of the Services, IBM may transfer Client's data, including Personal Data, across a country border, to the entities and countries listed in this SD or the Agreement or previously notified to Client. Such transfer may be made to a country outside the European Economic Area (EEA) or to a country that has not been declared by the European Commission to provide an adequate level of data protection (a “Third Country”) provided that Client has had an opportunity to obtain any mandatory approvals. IBM shall reasonably cooperate with Client to meet its legal requirements, including mandatory legal approvals. On this basis Client consents to the Services being provided by these entities in these countries and is solely responsible for determining that any transfer of Client's data, including Personal Data, across a country border under this SD and the Agreement complies with the applicable data protection laws. If a transfer is to a Third Country, IBM collaboration may include the execution of one or more processing agreements that contain the EU standard contractual clauses for the transfer of personal data to data processors established in third countries in accordance with Decision 2010/87/EU or any European Commission approved replacement (a “Transfer Agreement”). IBM or IBM affiliates would be a Data Importer and Client or Client's affiliates would be a Data Exporter as defined in a Transfer Agreement. Any disputes or liability arising from any Transfer Agreement, even if executed by affiliates of parties to this SD and the Agreement, will be treated as if the dispute or liability arose between those parties under the terms of this SD and the Agreement;

i. be responsible for the identification and interpretation of any applicable laws, regulations, and statutes that affect the existing application systems, programs, or data to which IBM will have access during the Services. It is Client's responsibility to ensure that the systems, programs, and data meet the requirements of those laws, regulations and statutes;

j. be responsible for the content of any database, the selection and implementation of controls on its access and use, backup and recovery, and the security of the stored data. This security will also include any procedures necessary to safeguard the integrity and security of software and data used in the Services from access by unauthorised personnel; be responsible for the identification of interpretation of, and compliance with, any applicable laws, regulations, and statutes that affect Client's existing systems, applications, programs, or data to which IBM will have access during the Services, including applicable data privacy, export, and import laws and regulations. It is Client's responsibility to ensure the systems, applications, programs, and data meet the requirements of those laws, regulations and statutes;

k. acknowledge and agree that IBM does not provide legal services or represent or warrant that the services or products IBM provides or obtains on Client's behalf will ensure Client's compliance with any particular law, including but not limited to any law relating to safety, security or privacy; and

l. be responsible for:

   (1) obtaining those products (such as any required software or hardware) and services upon which IBM is relying to provide the Services;

   (2) the physical installation and cabling of all hardware devices;

   (3) providing and paying for Internet access service or telecommunications transport circuits; and

   (4) Client's own network security policy and security violation response procedures.

4. Service Level Agreements

IBM SLAs establish response time objectives and countermeasures for specific events resulting from the Services. The SLAs become effective when the deployment process has been completed, and support and management of the Agent have been successfully transitioned to “active” in the SOCs. The SLA remedies are available provided Client meets Client's obligations as defined in this Services Description and all associated contract documents.

4.1 SLA Availability

The SLA defaults described below comprise the measured metrics for delivery of the Services. Unless explicitly stated below, no warranties of any kind shall apply to Services delivered under this Services Description. The sole remedies for failure to meet the SLA defaults are specified in the section of this Services Description entitled “SLA Remedies”.

a. Security incident alert notification (also know as “automated alerting”) – If X-Force Protection System alert notification has been configured by Client in the Portal and an alert has been generated, IBM will send an hourly e-mail notification to the Designated Services Contact, summarising the X-Force Protection System alerts, except where Threat Analyst Monitoring and Notification is enabled. This SLA only applies to the initial sending of the X-Force Protection System alert notification; not the confirmed delivery to the end recipient(s).

b. For purpose of clarification, an e-mail notification will be sent only if an alert has been generated during the preceding hour.

c. Security incident identification (also known as “Eyes on Screen” or “Threat Analyst Monitoring and Notification”) – IBM will identify all events it deems to be Priority 1, 2, and 3 level security incidents based on Agent IDPS event data received by the SOCs (where applicable).

   (1) Priority 1 incidents: high-risk events that have the potential to cause severe damage to Client's systems or environments and require immediate defensive action. Priority 1 incident examples include system or data compromises, worm infections/propagation, and massive denial of service (“DOS”) attacks.

   (2) Priority 2 incidents: lower-risk events that have the potential to impact Client's systems or environments and require action within 12-24 hours of notification. Priority 2 incident examples include unauthorised local scanning activity and attacks targeted at specific servers or workstations.

   (3) Priority 3 incidents: low-risk or low confidence events that have the potential to impact Client's systems or environments. This category of investigation encompasses activity on a network or server that should be further investigated within 1-7 days but may not be directly actionable. Discovery scanning, information gathering scripts, and other reconnaissance probes are grouped into this category.

Note: Whether or not a security event is considered a security incident is determined solely by IBM.

d. Security incident notification, except where the FW or SWG service components are involved - IBM will initiate notification for all identified security incidents within the selected Incident Response SLA. Client's Authorised Security Contact or Designated Services Contact will be notified by telephone for Priority 1 security incidents and via e-mail for Priority 2 and 3 security incidents. During a Priority 1 security incident notification, IBM will continue attempting to contact the Authorised Security Contact or Designated Services Contact until such contact is reached or all notification contacts have been exhausted.

e. Operational activities related to security incidents and responses will be documented and time-stamped within the IBM trouble ticketing system. Such documentation and time-stamp shall be used as the sole authoritative information source for purposes of this SLA.

f. The incident response SLA that applies is based on the options specified in the Order Document.

g. Policy change request acknowledgement – when applicable, IBM will acknowledge receipt of Client's policy change request by IBM within the Policy change request acknowledgement response

time specified in the Order Document. This SLA is only available for policy change requests submitted by an Authorised Security Contact or a Designated Services Contact in accordance with the established procedures documented in the Portal.

h. Policy change request implementation – when applicable, IBM will implement Client's policy change requests within the selected Time to Implement number of hours specified in the Order Document. The Time to Implement hours will be met by IBM unless the request has been placed in a "hold" status due to insufficient information required to implement the submitted policy change request. This SLA is only available for policy change requests submitted by an Authorised Security Contact or a Designated Services Contact in accordance with the established procedures documented in the Portal, and does not apply to policy change requests that exceed the monthly entitlements – commonly referred to as "overages".

i. The policy change request implementation SLA that applies is based on the following Time to Implement options and is specified in the Order Document.

j. Proactive system monitoring – IBM will notify Client within the Response Time designated after IBM determines Client's Agent is unreachable via standard in-band connectivity. The Response Time SLA that applies is based on the Response Time options specified in the Order Document.

k. Proactive security content update – when applicable, IBM will begin application of new security content or device updates within the Agent Update Time specified in the Order Document after the following sequential events occur:

   (1) the update is published as generally available by the applicable vendor;

   (2) IBM has successfully completed an evaluation period with positive results; and

   (1) a confirmation (if required) has been received from Client to apply the update within the Agent Update time as specified in the Order Document unless we mutually agreed to apply the update time at a later time. The approved update will be applied consistent with specific change window requirements indicated by Client and may require confirmation prior to application. The Agent Update Time SLA that applies is based on the Agent Update Time options as specified in the Order Document.

b. Services availability – IBM will provide 100% service availability for the SOCs.

c. Portal availability – IBM will provide 99.9% accessibility for the Portal outside of the times specified in the section entitled "Scheduled and Emergency Portal Maintenance".

4.2 SLA Remedies

a. Security incident identification remedy – If IBM fails to meet this SLA in a given calendar month, a credit will be issued as specified below;

   (1) Priority 1 incidents: Failure to identify the security event(s) as a security incident will result in a one month credit for the initial Agent that reported the event(s).

   (2) Priority 2 incidents: Failure to identify the security event(s) as a security incident will result in a one week credit for the initial Agent that reported the event(s).

   (3) Priority 3 incidents: Failure to identify the security event(s) as a security incident will result in a one day credit for the initial Agent that reported the event(s).

b. Security incident alert notification, policy change request acknowledgement, policy change request implementation, proactive system monitoring, proactive security content update, services availability and Portal availability credits – If IBM fails to meet any of these SLAs, a credit will be issued for the applicable charges for one day of the monthly monitoring charge for the affected Agent and, if applicable, the specific managed security platform for which the respective SLA was not met.

SLA Credit Summary

Service Level Agreements	Availability Credits
Security incident identification	Credit for 1 month, 1 week, or 1 day for the initial Agent that reported the event, as indicated above

Policy change request implementation	Credit
Policy change request acknowledgement	Credit of 1 day of the monthly charge for the affected Agent
Security Incident Alert Notification	
Security incident notification	
Proactive system monitoring	
Proactive security content update	
Services availability	

4.3 SLA Exclusions and Stipulations

4.3.1 Policy Change Request Overages

Certain Services include support for a specified number of policy change requests as defined in the section of the applicable Services Descriptions entitled “Policy Management”. Policy change requests in excess of the specified amount will not be addressed as a priority and will not be bound by the SLAs provided in the section of the applicable Services Descriptions entitled “Service Level Agreements”.

If the Services Recipient exceeds its specified number of policy change requests for two or more months during the contract period, IBM may move the Services Recipient to the Select or Premium level of Services (as applicable). Client may be invoiced at the then-current rate. SLAs will be re-set for the new Services level. Failure to upgrade Client's Services may result in an interruption of such Services.

As an example, Client contracts for the Standard level of Services and are allowed two policy changes per month. For two months during the contract period, the Services Recipient requests (and IBM provides) more than two policy changes. IBM may move the Services Recipient to the Select or Premium level of Services (as applicable). Client may be invoiced at the then-current rate.

4.3.2 Testing of Monitoring and Response Capabilities

Client may test IBM monitoring and response capabilities by staging simulated or actual reconnaissance activity, system or network attacks, and/or system compromises upon advance written notice to IBM. Such activities may be initiated directly by Client or by a contracted third party. SLAs will not apply during the period of such staged activities, and remedies will not be payable if the associated SLA(s) are not met.

4.3.3 Internet Emergency Declaration

During declared Internet emergencies, IBM will provide real-time access into IBM's global situation briefing, and a summarised e-mail designed to provide information Client can use to protect Client's organisation. Situation briefings following the onset of an Internet emergency will supersede any requirement for IBM to provide specific escalations for events directly related to the declared Internet emergency. IBM will communicate all other priority level incidents, during an Internet emergency, via automated systems such as e-mail, pager and voice mail.

Standard escalation practices will resume upon conclusion of the stated Internet emergency. Termination of an emergency state is marked by a decrease in the AlertCon level to AlertCon 2, or an e-mail notification delivered to Client's Authorised Security Contact.

4.3.4 Scheduled and Emergency Maintenance

Scheduled maintenance means any maintenance:

a. that is performed during the standard monthly maintenance window on the second Saturday of every month from 8:00 a.m. – 8:00 p.m. United States Eastern Time; or

b. of which Client is notified at least five days in advance. Notice of scheduled maintenance will be provided to the Designated Services Contact.

Emergency maintenance means any non-scheduled, non-standard maintenance required by IBM.

No statement in the section of any Services Description entitled “Service Level Agreements” shall prevent IBM from conducting emergency maintenance on an “as needed” basis. During such emergency maintenance, Client's Point of Contact will receive notification within 30 minutes of initialisation of the emergency maintenance and within 30 minutes of the completion of the emergency maintenance. IBM will be relieved of its obligations under the applicable SLAs during scheduled and emergency maintenance.

4.3.5 Contact Information

Certain SLAs require IBM to provide notification to the Authorised Security Contact or a Designated Services Contact after certain events occur. In the case of such an event, Client is solely responsible for providing IBM with accurate and current contact information for Authorised Security Contact(s) and/or Designated Services Contact(s). Notifications will be provided to Client's authorised contacts at the current contact information on record through the Portal. IBM will be relieved of its obligations under these SLAs if contact information is out of date or inaccurate due to Client's action or omission.

4.3.6 Network/Server Change Notifications

Client is responsible for providing IBM advance notice regarding any network or server changes or outages to the managed services environment. In the event advance notice cannot be provided, Client is required to provide IBM with notification of changes within seven calendar days of such network or server changes. Unless otherwise specified in the Services Description, notification is completed by the submission or update of an inquiry ticket through the Portal for changes that will be implemented by Client. For changes that must be implemented by IBM, Client must submit a policy change request ticket. If Client fails to notify IBM as stated above, all SLA remedies are considered null and void.

4.3.7 Network Traffic Applicable to SLAs

Certain SLAs focus on the prevention, identification and notification of security incidents. Such SLAs assume the traffic has successfully reached the Agent, the Agent is healthy and not experiencing any hardware or software errors and the Agent has the ability to process the traffic against the installed policy and generate a logged event. IBM is not responsible for traffic that does not logically or electronically pass through an Agent, or a logged event that does not reach the SOCs, or traffic that does not generate a logged event.

4.3.8 SLA Compliance and Reporting

SLA compliance and the associated remedies are based on fully functional network environments, Internet and circuit connectivity, Agents, and properly configured servers. SLA compliance reporting will be provided through the Portal. If SLA compliance failure is deemed by IBM in its sole discretion to be caused by customer premise equipment hardware or software (including any and all Agents), all SLAs are considered null and void and remedies will not be paid.

5. Other Terms and Conditions

Some of the Services may be performed by an IBM subcontractor. If an IBM subcontractor assists with the project, IBM is solely responsible for completion of the work described herein and compliance with the terms hereof and coordinating any involvement of IBM subcontractors who may be engaged to assist IBM in accomplishing the work described herein.

5.1 Contract Changes

If IBM agrees to a request for an increase in the number of supported devices, or another change that requires a new order be placed with IBM (such as a change from Standard to Select or Premium service), the following terms apply:

d. all devices (including those for which Client initially contracted) will be governed by the then-current versions of all applicable documents (for example, the Agreement and the Services Descriptions); and

e. the contract period will be adjusted so that all devices will be coterminous.

5.2 Modification of Services

IBM reserves the right to modify the terms of the Services Descriptions at any time. Should such modification reduce the scope or level of the Services being delivered (for example, eliminating previously provided Services or lengthening the security incident response time), IBM will provide a minimum of 30 days

prior notice via the Portal or other electronic means. Client may request that IBM defer the change effective date until the end of the then-current contract period for the Services by notifying IBM in writing within the 30 calendar days immediately following IBM's notice of such modification. The modification will then become effective when the Services are renewed. If the modification is the result of circumstances outside of IBM's control (such as technology changes or vendor service changes), IBM reserves the right to reject Client's request for deferment.

5.3 Decommission or Turn-Down of Services

If the Services are terminated or the contract is not renewed, Client will have either 90 days from the date of termination or 90 days from the date of contract expiration, whichever first occurs, to request the receipt of archived data. Such request may be submitted through the Portal or via telephone if access to the Portal is no longer available. IBM will charge Client for all time and materials, and shipping charges (if applicable) utilised to restore and make the data available via download from a secured IBM server. In cases where the amount of archived data is deemed by IBM to be too excessive to make available via download, IBM will store the data on encrypted media and ship it to a location specified by Client.

If a request is not received within the 90 day period described above, IBM will permanently destroy all archived data no longer under a valid Services contract.

5.4 Data Compilation

Client consents to IBM collecting, gathering and compiling security event log data to look at trends, and real or potential threats. IBM may compile or otherwise combine this security event log data with similar data of other Services Recipients so long as such data is compiled or combined in a manner that will not in any way reveal the data as being attributable to Client.

5.5 Regulatory Services

IBM does not operate as a provider of services regulated by the Federal Communications Commission ("FCC") or state regulatory authorities ("State Regulators"), and does not intend to provide any services which are regulated by the FCC or State Regulators. If the FCC or any State Regulator imposes regulatory requirements or obligations on any services provided by IBM hereunder, IBM may: (a) modify, replace, or substitute products at Customer's expense, and/or (b) change the way in which such services are provided to Client to avoid the application of such requirements or obligations to IBM (for example, by acting as Client's agent for acquiring such services from a third party common carrier.)

5.6 Disclaimers

Products and Services are not warranted to operate uninterrupted or error free. Client understands and agrees that new technology, configuration changes, software upgrades and routine maintenance, among other items, can create new and unknown security exposures. Moreover, computer "hackers" and other third parties continue to employ increasingly sophisticated techniques and tools, resulting in ever-growing challenges to individual computer system security. It is Client's sole responsibility to maintain the security of Client's computer systems. IBM's performance of the Services does not constitute any representation or warranty by IBM about the security of Client's computer systems including, but not limited to, any representation that Client's computer systems are safe from intrusions, viruses, or any other security exposures. Products and Services are not fault tolerant and are not designed or intended for use in hazardous environments requiring fail-safe operation, including without limitation aircraft navigation, air traffic control systems, weapon systems, life support systems, nuclear facilities, or any other applications in which Product or Services failure could lead to death, personal injury, or property damage. IBM does not make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information provided as part of the Services.

5.7 Background Checks

Under the governance of IBM's global employment verification standard, IBM follows a mandated set of employment verification requirements for all new hires, including regular, fixed term, supplemental, interns and students. If Client requires any additional screening, Client must notify Client's IBM point of contact and they will work with Client to establish a mutual agreement on screening. Client will be responsible for all associated expenses including, but not limited to, resource time, travel, and fees in regards to such screening.