

**IBM Managed Security Services (Cloud Computing) –
hosted mobile device security management**

Table of Contents

1.	Scope of Services	3
2.	Definitions.....	3
3.	Services	3
3.1	Security Operations Centers	4
3.2	Portal.....	4
3.2.1	IBM Portal Responsibilities.....	4
3.2.2	Your Portal Responsibilities	4
3.3	Services Contacts	4
3.3.1	IBM Services Contacts Responsibilities	5
3.3.2	Your Services Contacts Responsibilities	6
3.4	Security Intelligence	7
3.4.1	IBM Security Intelligence Responsibilities	7
3.4.2	Your Security Intelligence Responsibilities.....	8
3.5	Mobile Security Gateway.....	8
3.5.1	IBM Mobile Security Gateway Responsibilities	8
3.5.2	Your Mobile Security Gateway Responsibilities	8
3.6	Device Security Client	8
3.6.1	IBM Device Security Client Responsibilities	8
3.6.2	Your Device Security Client Responsibilities.....	8
3.7	Self-Service Mobile Security Dashboard	8
3.7.1	IBM Self-Service Mobile Security Dashboard Responsibilities.....	9
3.7.2	Your Self-Service Mobile Security Dashboard Responsibilities.....	9
3.8	Apple iOS Device Support.....	9
3.8.1	IBM Apple iOS Device Support Responsibilities	9
3.8.2	Your Apple iOS Device Support Responsibilities	9
3.9	Deployment and Activation.....	9
3.9.1	IBM Deployment and Activation Responsibilities	9
3.9.2	Your Deployment and Activation Responsibilities	11
3.10	Monitoring and Management.....	12
3.10.1	IBM Monitoring and Management Responsibilities	12
3.10.2	Your Monitoring and Management Responsibilities	12
3.11	Services Reporting	13
3.11.1	IBM Services Reporting Responsibilities.....	13
3.11.2	Your Services Reporting Responsibilities.....	13
3.12	Collection and Archival.....	13
3.12.1	IBM Collection and Archival Responsibilities.....	13
3.12.2	Your Collection and Archival Responsibilities	13
4.	Service Level Agreements.....	13
4.1	SLA Availability	13
4.2	SLA Remedies	14
5.	Other Terms and Conditions.....	14
5.1	General	14
5.2	Systems Owned by a Third Party	14
5.3	Disclaimer	15

Services Description

IBM Managed Security Services (Cloud Computing) - Hosted Mobile Device Security Management

IN ADDITION TO THE TERMS AND CONDITIONS SPECIFIED BELOW, THIS SERVICES DESCRIPTION INCLUDES THE "IBM MANAGED SECURITY SERVICES GENERAL PROVISIONS" ("GENERAL PROVISIONS") LOCATED AT <http://www.ibm.com/services/iss/wwcontracts/us/mssgp> AND INCORPORATED HEREIN BY REFERENCE.

1. Scope of Services

IBM Managed Security Services – Hosted Mobile Device Security Management (called "MDS" or "Services") is designed for IBM to provide the Services Recipient with deployment and management of mobile security using security software for mobile devices, centralized management tools, and security services.

The Services features described herein are dependent upon the availability and supportability of products and product features being utilized. Even in the case of supported products, not all product features may be supported. Information on supported features is available from IBM upon request. This includes both IBM-provided and non-IBM-provided hardware, software, and firmware.

2. Definitions

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 (called "Portal").

Device Security Client ("Client") – A security application to be downloaded and installed on the mobile device. It performs security functions for the mobile device and communicates with the Gateway to get security policies and settings.

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.

Mobile Security Gateway ("Gateway") – A Web based tool used by IBM administrators and your IT or help desk staff to perform management tasks for the solution.

Portal – A Web based management tool used by your authorized contacts to obtain information and interact with IBM personnel.

Self-Service Mobile Security Dashboard – A Web based tool used by your Device Security Client users to perform certain tasks for the solution.

3. Services

The following table highlights the measurable Services features. The subsequent sections provide narrative descriptions of each Services feature.

Services Feature Summary

Services Feature	Metric or Qty	Service Level Agreements
Services availability	100%	Services availability SLA
IBM Portal availability	99.9%	IBM Portal availability SLA
Authorized Security Contacts	3 users	N/A
Mobile Security Gateway administrative users	3 users	N/A

Mobile Security Gateway private data users	3 users	N/A
Policy change request	Up to 4 per month	N/A
Policy change request acknowledgement	2 hours	Policy change request acknowledgement SLA
Policy change request implementation	24 hours	Policy change request implementation SLA

3.1 Security Operations Centers

IBM Managed Security Services are delivered from a network of IBM Security Operations Centers (“SOCs”). IBM will provide access to the SOCs 24 hours/day, 7 days/week.

3.2 Portal

The Portal provides you with access to an environment (and associated tools) designed to monitor and manage your 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 you 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.

3.2.1 IBM Portal Responsibilities

IBM will:

- a. provide access to the Portal 24 hours/day, 7 days/week. The Portal will provide:
 - (1) security intelligence awareness and alerting;
 - (2) service ticket information;
 - (3) ticketing and workflow initiation and updates;
 - (4) live chat and collaboration with SOC analysts;
 - (5) a template-driven reporting dashboard;
 - (6) authorization to download data; and
 - (7) access to Education Materials in accordance with the terms provided in the Portal; and
- b. maintain availability of the Portal in accordance with the metrics provided in the section of this Services Description entitled “Service Level Agreements”, “IBM Portal availability”.

3.2.2 Your Portal Responsibilities

You agree to:

- a. utilize the Portal to perform daily operational Services activities, as required;
- b. ensure your employees accessing the Portal on your behalf comply with the Terms of Use provided therein including, but not limited to, the terms associated with Educational Materials;
- c. appropriately safeguard your login credentials to the Portal (including not disclosing such credentials to any unauthorized individuals);
- d. promptly notify IBM if a compromise of your login credentials is suspected; and
- e. indemnify and hold IBM harmless for any losses incurred by you or other parties resulting from your failure to safeguard your login credentials.

3.3 Services Contacts

You may choose from multiple levels of access to the SOC and the Portal to accommodate varying roles within your organization.

Authorized Security Contacts

An Authorized Security Contact is defined as a decision-maker on all operational issues pertaining to IBM Managed Security Services.

Designated Services Contacts

A Designated Services Contact is defined as a decision-maker on a subset of operational issues pertaining to IBM Managed Security Services, an Agent, or a group of Agents. IBM will only interface with a Designated Services Contact regarding operational activities that fall within the subset for which such contact is responsible (for example, designated Agent outage contact).

Portal Users

IBM provides multiple levels of access for Portal Users. These levels of access can be applied to the IBM Managed Security Services, an Agent, or a group of Agents. Portal Users will be authenticated via static password or a public-key encryption technology you provide (for example, RSA SecureID token) based on your requirements.

Mobile Security Gateway Administrative Users (“MSG Admin User”)

A Mobile Security Gateway Administrative User is defined as a user of the Mobile Security Gateway that has the ability and permission to execute administrative commands on registered mobile devices including remote locate, lock, and wipe as well as manage device deactivations and Device Security Client user password resets.

Mobile Security Gateway Private Data Users (“MSG Private Data User”)

A Mobile Security Gateway Private Data User is defined as a user of the Mobile Security Gateway that has the ability and permission to enable user tracking and monitoring for specific mobile devices and to review results

3.3.1 IBM Services Contacts Responsibilities

Authorized Security Contacts

IBM will:

- a. allow you to create up to three Authorized Security Contacts;
- b. provide each Authorized Security Contact with:
 - (1) the authorization to create unlimited Designated Services Contacts and Portal Users;
 - (2) the authorization to delegate responsibility to Designated Services Contacts;
- c. interface with Authorized Security Contacts regarding support and notification issues pertaining to the Services; and
- d. verify the identity of Authorized Security Contacts using an authentication method that utilizes a pre-shared challenge pass phrase.

Designated Services Contacts

IBM will:

- a. verify the identity of Designated Services Contacts using an authentication method that utilizes 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.

Portal Users

IBM will:

- a. provide access to the Portal with capabilities that may include (as appropriate):
 - (1) submitting Services requests to the SOCs;
 - (2) “live chat” communicating with SOC analysts regarding specific incidents or tickets, generated as part of the Services;
 - (3) creating internal Services-related tickets and assigning such tickets to Portal Users;
 - (4) querying, viewing, and updating Services-related tickets;
 - (5) scheduling and running reports;

- b. authenticate Portal Users using static password; and
- c. authenticate Portal Users using a public-key encryption technology you provide (for example, RSA SecureID token) based on your requirements.

MSG Admin Users

IBM will:

- a. provide access to the Mobile Security Gateway with capabilities that may include (as appropriate):
 - (1) ability to execute administrative commands on registered mobile devices including:
 - (a) remote locate, lock, and wipe;
 - (b) management of device deactivations; and
 - (c) Device Security Client user password resets.

MSG Private Data Users

IBM will:

- a. provide access to the Mobile Security Gateway with capabilities including:
 - (1) enabling Device Security Client user tracking and monitoring for specific mobile devices; and
 - (2) reviewing user tracking data collected for specific users.

3.3.2 Your Services Contacts Responsibilities

Authorized Security Contacts

You agree:

- a. to provide IBM with contact information for each Authorized Security Contact. Such Authorized Security Contacts will be responsible for:
 - (1) creating Designated Services Contacts and delegating responsibilities and permissions to such contacts, as appropriate;
 - (2) creating Portal users;
 - (3) authenticating with the SOCs using a pre-shared challenge pass phrase; and
 - (4) maintaining notification paths and your contact information, and providing such information to IBM;
- b. to ensure at least one Authorized Security Contact is available 24 hours/day, 7 days/week;
- c. to update IBM within three calendar days when your Authorized Security Contact information changes; and
- d. and acknowledge that you are permitted to have no more than three Authorized Security Contacts regardless of the number of IBM services or Agent subscriptions for which you have contracted.

Designated Services Contacts

You agree:

- a. to provide IBM with contact information and role responsibility for each Designated Services Contact. Such Designated Services Contacts will be responsible for authenticating with the SOCs using a pass phrase; and
- b. and 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 (i.e., Agent outage).

Portal Users

You agree:

- a. that Portal Users will use the Portal to perform daily operational Services activities;
- b. that Portal Users will be responsible for providing IBM-supported RSA SecureID tokens (as applicable); and

- c. that Portal Users will not have direct contact with the SOCs unless they are also an Authorized Security Contacts or a Designated Services Contacts.

MSG Admin Users

You agree:

- a. to execute administrative commands on registered mobile devices from the Mobile Security Gateway including:
 - (1) remote locate, lock, and wipe;
 - (2) manage device deactivations; and
 - (3) Device Security Client user password resets.

MSG Private Data Users

Your agree:

- a. to enable Device Security Client user tracking and monitoring for specific mobile devices from the Mobile Device Security Gateway; and
- b. to review results produced from the Mobile Security Gateway.

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 AlertCon threat level. The AlertCon describes progressive alert postures of current Internet security threat conditions. In the event Internet security threat conditions are elevated to AlertCon 3, indicating focused attacks that require immediate defensive action, IBM will provide you with real-time access into IBM's global situation briefing. As a user of the Portal, you have access to the X-Force Hosted Threat Analysis Service. The X-Force Hosted Threat Analysis Service includes access to the IBM X-Force Threat Insight Quarterly ("Threat IQ").

Utilizing the Portal, you can create a vulnerability watch list with customized threat information. In addition, each 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 individualized alerts, advisories and security news.

Note: Your access and use of the Security intelligence provided via the Portal (including the Threat IQ and 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 Services Description or any associated contract documents, the Portal Terms of Use shall prevail. In addition to the Terms of Use provided in the Portal, your 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.

3.4.1 IBM Security Intelligence Responsibilities

IBM will:

- a. provide you with access to the X-Force Hosted Threat Analysis Service;
- b. provide you with a username, password, URL and appropriate permissions to access the Portal;
- c. display security information on the Portal as it becomes available;
- d. if configured by you, provide security intelligence specific to your defined vulnerability watch list, via the Portal;
- e. if requested by you, provide an Internet security assessment e-mail each business day;
- f. publish an Internet AlertCon via the Portal;
- g. declare an Internet emergency if the daily AlertCon level reaches AlertCon 3. In such event, IBM will provide you with real time access into IBM's global situation briefing;
- h. provide Portal feature functionality for you to create and maintain a vulnerability watch list;
- i. provide additional information about an alert, advisory, or other significant security issue as IBM deems necessary; and
- j. provide access to the Threat IQ via the Portal.

3.4.2 Your Security Intelligence Responsibilities

You agree to use the Portal to:

- a. subscribe to the daily Internet security assessment e-mail, if desired;
- b. create a vulnerability watch list, if desired;
- c. access the Threat IQ; and
- d. provide your agreement to adhere to the licensing agreement and not forward Services information to individuals who do not have a proper license.

3.5 Mobile Security Gateway

The Mobile Security Gateway is a Web based tool intended for use by your IT or helpdesk personnel to perform certain tasks such as locate, lock, or wipe a mobile device on behalf of one of your employees.

3.5.1 IBM Mobile Security Gateway Responsibilities

IBM will:

- a. provide access to the Mobile Security Gateway 24 hours/day, 7 days/week;
- b. provide access credentials for your designated MSG Admin Users; and
- c. provide access credentials for your designated MSG Private Data Users.

3.5.2 Your Mobile Security Gateway Responsibilities

You agree to:

- a. ensure your employees accessing the Mobile Security Gateway on your behalf comply with the Terms of Use provided therein;
- b. be responsible for using the Mobile Security Gateway functions provided in accordance with your local laws and regulations;
- c. appropriately safeguard your login credentials to the Mobile Security Gateway (including not disclosing such credentials to any unauthorized individuals);
- d. manage device deactivations and Device Security Client user password resets, as required;
- e. promptly notify IBM if a compromise of your login credentials is suspected; and
- f. indemnify and hold IBM harmless for any losses incurred by you or other parties resulting from your failure to safeguard your login credentials.

3.6 Device Security Client

The Device Security Client is software provided by IBM at no additional charge to be installed on mobile devices that you designate to be managed as part of the services.

3.6.1 IBM Device Security Client Responsibilities

IBM will:

- a. provide you with instructions which may be give to your users on how to download and install the Device Security Client to their devices; and
- b. upon request, provide instruction on how to you may obtain the Device Security Client so that you may make the software available to your users from your own download site or device management system.

3.6.2 Your Device Security Client Responsibilities

You agree to:

- a. provide your users with IBM's instructions on how to download the Device Security Client to their devices; and
- b. as required, obtain the Device Security Client software from IBM and make it available to your users from your own download site or device management system.

3.7 Self-Service Mobile Security Dashboard

The Self-Service Mobile Security Dashboard is designed to be used by your Client users to perform device security functions directly, without the involvement of IBM personnel or your IT/helpdesk personnel. The Self-Service Mobile Security Dashboard will provide functions such as on-demand remote device locate, lock, and wipe as applicable to the user's device.

3.7.1 IBM Self-Service Mobile Security Dashboard Responsibilities

IBM will:

- a. provide access for your Client users to the Self-Service Mobile Security Dashboard 24 hours/day, 7 days/week.

3.7.2 Your Self-Service Mobile Security Dashboard Responsibilities

You agree to:

- a. instruct your users on how to register their devices with Services and how access the Self-Service Mobile Security Dashboard;
- b. ensure that end users appropriately safeguard their login credentials to the Self-Service Mobile Security Dashboard (including not disclosing such credentials to any unauthorized individuals);
- c. using the Mobile Security Gateway, promptly reset the password of any user if a compromise of login credentials is suspected; and
- d. indemnify and hold IBM harmless for any losses incurred by you or other parties resulting from a user's failure to safeguard their login credentials.

3.8 Apple iOS Device Support

Services include features for Apple iOS devices that require use of Apple's configuration profiles and Apple push notification service. Use of these features may require a certificate generated by Apple to provide management of your iOS devices.

3.8.1 IBM Apple iOS Device Support Responsibilities

IBM will:

- a. provide you with guidance on how to obtain the necessary certificate from Apple; and
- b. install your Apple certificate in our systems to authorize management of your Apple iOS devices.

3.8.2 Your Apple iOS Device Support Responsibilities

You agree to:

- a. obtain a certificate for your organization from Apple following Apple's process and procedures including applying for required Apple programs and paying required fees, if any;
- b. annually (or as required by Apple) obtain an updated certificate for your organization from Apple using the Apple certificate request process; and
- c. provide your updated certificate obtained from Apple to IBM.

3.9 Deployment and Activation

During deployment and activation, IBM will work with you to deploy the technology components for your environment and transition it to steady-state management.

3.9.1 IBM Deployment and Activation Responsibilities

IBM will perform the following activities in order to activate your Service.

Activity 1 - Project Kickoff

The purpose of this activity is to conduct a project kickoff call. IBM will send you a welcome e-mail and conduct a kickoff call, for up to one hour for up to three of your personnel, to:

- a. introduce your Point of Contact to the assigned IBM deployment specialist;
- b. review each party's respective responsibilities;
- c. set schedule expectations; and
- d. begin to assess your requirements and environment.

Completion Criteria:

This activity will be complete when IBM has conducted the project kickoff call.

Deliverable Materials:

- None

Activity 2 - Assessment

The purpose of this activity is to perform an assessment of your current business and technology requirements related to mobile security, in order to develop required security policies and settings.

Task 1 - Gather Data

IBM will:

- a. provide you with a data gathering form, to collect information about:
 - (1) business policies with the use of mobile devices in your work environment;
 - (2) specific security requirements related with mobile devices;
 - (3) team member names, contact information, roles and responsibilities;
 - (4) unique country and site requirements;
 - (5) number and type of Device Security Client users; and
 - (6) key business drivers and/or dependencies that could influence Services delivery or timelines.

Note: IBM may make changes to the data gathering form, as it deems appropriate, throughout the performance of the Services.
- b. schedule meetings as necessary to clarify the questions and responses (as deemed appropriate by IBM).

Task 2 - Assess Requirements

IBM will:

- a. use the information provided in the data gathering form to assess your mobile security requirements; and
- b. work with you to establish the user groups, administrator access rights, security features, policies, and settings to meet your needs.

Completion Criteria:

This activity will be complete when IBM has received the completed data gathering form and has assessed your requirements.

Deliverable Materials:

- None

Activity 3 - Implementation

The purpose of this activity is to implement the solution including mapping the identified requirements to policies and settings on the Mobile Security Gateway.

IBM will:

- a. create your customer account;
- b. create up to 10 policy groups as necessary;
- c. create administrative accounts for your help desk staff and set up roles, access rights, and permissions as required;
- d. enable agreed upon default enterprise wide security features to be deployed;
- e. configure and implement policies, profiles, and settings required for various security features;
- f. generate a license code for activating the Device Security Client;
- g. provide you with Mobile Security Gateway connection and access information; and
- h. verify connection, availability and functionality of the Self-Service Mobile Security Dashboard, and resolve issues as necessary.

Completion Criteria:

This activity will be complete when IBM has provided access to the Mobile Security Gateway and verified your access to the Self-Service Mobile Security Dashboard.

Deliverable Materials:

- None.

Activity 4 - Training and Enablement

The purpose of this activity is to enable your help desk staff to deliver the Device Security Client to users and perform self-service activities.

IBM will:

- a. provide Education Material to you at least one day before the training;
- b. remotely conduct a training for up to 90 minutes for up to 3 help desk staff to use the Mobile Security Gateway, handle Client download/device registration issues, and perform basic service tasks defined; and
- c. provide the license code for Device Security Client activation.

Completion Criteria:

This activity will be complete when IBM has conducted the training for your help desk.

Deliverable Materials:

- Education Material

Activity 5 - Services Activation

The purpose of this activity is to activate the Services.

IBM will:

- a. assume management and support of Services; and
- b. transition Services to the SOCs for ongoing management and support.

Completion Criteria:

This activity will be complete when the Services are activated.

Deliverable Materials:

- None

3.9.2 Your Deployment and Activation Responsibilities

Activity 1 - Project Kickoff

You agree to:

- a. attend the project kickoff call; and
- b. review each party's respective responsibilities.

Activity 2 - Assessment

Task 1 - Gather Data

You agree to:

- a. complete and return the data gathering form to IBM within five days of your receipt;
- b. 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; and
- c. work in good faith with IBM to accurately assess your mobile security requirements.

Task 2 - Assess Requirements

You agree to:

- a. timely respond to IBM's request for clarification of the responses to the data gathering form; and
- b. provide any other required information in order for IBM to provide Services, as requested by IBM.

Activity 3 - Implementation

You agree to:

- a. connect to the Self-Service Mobile Security Dashboard to verify set up of account, group, feature, and device settings.

Activity 4 - Training and Enablement

You agree to:

- a. identify help desk staff to participate in the training conducted by IBM;

- b. be responsible for ensuring your help desk staff is able to perform the management and Device Security Client user support tasks specified by IBM using the Mobile Security Gateway;
- c. build additional Device Security Client user communication materials if necessary for Device Security Client installation and device registration;
- d. distribute the client installation/configuration guide, license code, and additional communication materials to Device Security Client users; and
- e. instruct participating Device Security Client users to download the Device Security Client and register their mobile devices.

3.10 Monitoring and Management

Monitoring and management constitutes the ongoing services provided as part of MDS.

3.10.1 IBM Monitoring and Management Responsibilities

IBM will:

Activity 1 - Monitoring and Alerting

The purpose of this activity is to monitor Client registration status, utilization of security features enabled and alert you to abnormal activities.

IBM will:

- a. monitor the status of device registrations;
- b. monitor the usage of security features enabled for each platform and by Device Security Client users;
- c. collect and report account registration and feature usage statistics on a periodic basis; and
- d. notify you of specific violations of policy by your Device Security Client users.

Activity 2 - Reporting and Policy Management

The purpose of this activity is to provide recommendations on policy changes or steps you can take to improve the security of your mobile devices and perform policy management.

IBM will:

- a. at least monthly, analyze usage of the Device Security Client throughout your mobile device population;
- b. make suggestions for policy or profile changes which are deemed necessary;
- c. review policy change requests initiated by you;
- d. modify policy changes as jointly agreed with you;
- e. test and verify the results of such policy changes;
- f. notify you when new policies will be in place and communicate any potential impact; and
- g. implement policy changes and attempt to verify they will not have an adverse impact to the current deployment.

Deliverable Materials:

- None

3.10.2 Your Monitoring and Management Responsibilities

Activity 1 - Monitoring and Alerting

You agree to:

- a. review device registration and feature usage statistics provided by IBM; and
- b. communicate and address specific violations of policy when provided by IBM.

Activity 2 - Reporting and Policy Management

You agree to:

- a. review reports and recommendations provided by IBM;
- b. request policy changes based on IBM recommendations or your own requirements;
- c. participation in discussion of desired policy changes;

- d. communicate to Device Security Client users regarding policy changes or issues found on their devices, if necessary; and
- e. ultimately approve all policy changes.

3.11 Services Reporting

Utilizing the Portal, you will have access to Services information.

3.11.1 IBM Services Reporting Responsibilities

IBM will provide you with access to reporting capabilities in the Portal which include:

- a. number of SLAs invoked and met;
- b. number, types, and summary of Services requests/tickets;

3.11.2 Your Services Reporting Responsibilities

You agree to:

- a. generate Services-related reports using the Portal;

3.12 Collection and Archival

In the course of operating the service, IBM will collect usage statistics and, if enabled by you, private Device Security Client user tracking and activity monitoring data.

3.12.1 IBM Collection and Archival Responsibilities

IBM will:

- a. collect data generated by your Device Security Client users;
- b. make data available to you in the Self-Service Mobile Security Dashboard and in the Portal;
- c. purge data and generated reports from IBM systems within 90 days of decommissioning individual mobile devices and when terminating Services

3.12.2 Your Collection and Archival Responsibilities

You agree:

- a. and acknowledge that:
 - (1) IBM will purge data in accordance with the timeframes stated in the "IBM Collection and Archival Responsibilities" section above;
 - (2) all data will be transmitted to the SOCs via the Internet;
 - (3) IBM can only collect and scan data that successfully reaches the IBM MSS infrastructure; and
 - (4) IBM does not guarantee the legal submission of any Services data into any domestic or international legal system. Admissibility of evidence is based on the technologies involved and your ability to prove proper data handling and chain of custody for each set of data presented.

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 the Service has been successfully transitioned to "active" in the SOCs. The SLA remedies are available provided you meet your 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. Services availability – IBM will provide 100% service availability for the SOCs.
- b. IBM Portal availability – IBM will provide 99.9% accessibility for the Portal outside of the times specified in the section of this Services Description entitled "Scheduled and Emergency Portal Maintenance". This includes the IBM Portal, Mobile Security Gateway and the Self-Service Mobile Security Dashboard.

- c. Policy change request acknowledgement – IBM will acknowledge receipt of policy change request within two hours of receipt by IBM. This SLA is only available for policy change requests submitted by an Authorized Security Contact or a Designated Services Contact in accordance with the established procedures documented in the Portal.
- d. Policy change request implementation – IBM will implement policy change requests within twenty-four hours of receipt 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 Authorized Security Contact or a Designated Services Contact in accordance with the established procedures documented in the Portal.

4.2 SLA Remedies

If IBM fails to meet any of these SLAs, a credit will be issued for one day of the monthly service.

SLAs and Remedies Summary

Service Level Agreements	Availability Remedies
Services availability	Credit for 1 day of the monthly Services charge
IBM Portal availability	
Policy change request acknowledgement	
Policy change request implementation	

5. Other Terms and Conditions

5.1 General

You acknowledge and agree:

- a. that all software provided by IBM as part of these Services is licensed, not sold. Except for the licenses specifically granted herein, all right, title, and interest in and to the software shall remain vested in IBM or its licensors;
- b. that you will inform IBM in writing, at least 30 days prior to the cancellation or termination of the Services, or promptly if the license for the software is terminated by IBM for any reason, whether you choose to:
 - (1) have IBM remove the IBM provided software either remotely or by assisting you to remove the IBM provided software; or
 - (2) retain the IBM provided software.

If you choose to have the software removed, you agree to cooperate with IBM by providing the remote access necessary for IBM to remove the software, or by assisting IBM in removing the software.

- c. in addition to the terms and conditions listed above, specific licensing terms will be presented for your review and acceptance both when you download and when you install the software.

5.2 Systems Owned by a Third Party

For systems (which for purposes of this provision includes but is not limited to applications and IP addresses) owned by a third party that will be the subject of testing hereunder, you agree:

- a. that prior to IBM initiating testing on a third party system, you will obtain a signed letter from the owner of each system authorizing IBM to provide the Services on that system, and indicating the owner's acceptance of the conditions set forth in the section entitled “Permission to Perform Testing” and to provide IBM with a copy of such authorization;
- b. to be solely responsible for communicating any risks, exposures, and vulnerabilities identified on these systems by IBM's remote testing to the system owner; and
- c. to arrange for and facilitate the exchange of information between the system owner and IBM as deemed necessary by IBM.

You agree:

- a. to inform IBM immediately whenever there is a change in ownership of any system that is the subject of the testing hereunder;
- b. not to disclose the deliverable Materials, or the fact that IBM performed the Services, outside your Enterprise without IBM's prior written consent; and
- c. to indemnify IBM in full for any losses or liability IBM incurs due to third party claims arising out of your failure to comply with the requirements of this section entitled, "Systems Owned by a Third Party" and for any third party subpoenas or claims brought against IBM or IBM's subcontractors or agents arising out of (a) testing the security risks, exposures or vulnerabilities of the systems that are the subject of testing hereunder, (b) providing the results of such testing to you, or (c) your use or disclosure of such results.

5.3 Disclaimer

You understand and agree that:

- a. it is solely within your discretion to use or not use any of the information provided pursuant to the Services hereunder. Accordingly, IBM will not be liable for any actions that you take or choose not to take based on the services performed and/or deliverables provided hereunder;
- b. IBM does not provide legal services or represent or warrant that the services or products IBM provides or obtains on your behalf will ensure your compliance with any particular law, including but not limited to any law relating to safety, security or privacy;
- c. it is your responsibility to engage competent legal counsel to advise you as to the identification and interpretation of any relevant laws that may affect your business and any actions needed for compliance with such laws; and
- d. 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 your sole responsibility to provide and maintain appropriate and adequate security for the company, your assets, systems and employees. IBM's performance of Services does not constitute any representation or warranty by IBM (a) that your or any third party's information technology, software, information, equipment, facilities, personnel, customers, visitors or any other persons are or will be, (i) secure or safe from harm, or (ii) secure or safe from unauthorized access, theft, loss, corruption, interception, disruption, viruses, or other security exposures, or bodily injury (including death) to persons or damage to or loss of, property, caused by the preceding, or (b) that IBM will provide warnings regarding such exposures.