Lookout Security and Privacy Policy Statements

1 AUTHORITY

Management recognizes and is committed to supporting this policy document. This policy has been reviewed and approved for general application to the stated scope by the Chief Operating Officer (COO).

2 PURPOSE

This document defines the Lookout Policies. Lookout will implement the policies stated in this document to ensure the proper security of information systems and Lookout information resources.

All policies have been developed to define the security and privacy requirements and mechanisms to be implemented across Lookout MES in accordance with International Organization for Standardization (ISO) 27001, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 and the FedRAMP Moderate security control baselines.

3 SCOPE

This document applies to all systems and devices within the Lookout MES system boundary, including its system users, groups, services, protocols, and functions.

4 ROLES AND RESPONSIBILITIES

The following individual(s) or group(s) is/are responsible for developing, implementing, and maintaining the Access Control Policy and its associated mechanisms:

ROLE	RESPONSIBILITY
Chief Operating Officer (COO)	Final review and approval of policies
Sr. Director of Compliance	Policy development and assurance of policy compliance.
Director of Security	Policy development and security recommendations and guidance
Sr. Director of Cloud Operations	Management and oversight of Lookout MES environment
Compliance Management Team	Input to policies and procedures. Implementation of procedures.

5 REVIEWS AND UPDATES

Policies are reviewed and updated by the Sr. Director of Compliance and the Sr. Director of Security with approval by the Chief Operations Officer, at least every three (3) years or as is required to address changes to the internal or external environments governing the Lookout Information Security Management System or Organization. Changes or revisions to Lookout policies are communicated to all privileged users associated with the MES environment. Employees within applicable departments must acknowledge and comply with changes to the policy.

6 REFERENCES

The following applicable laws, directive, policies, regulations, and standards were used as part of the development for this policy. These include (but are not limited to):

- Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.
- Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, June 2010.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46 Revision 1, Guide to Enterprise Telework and Remote Access Security, June 2009.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-48 Revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks, July 2008.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-77, Guide to IPsec VPNs, December 2005.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-100, Information Security Handbook: A Guide for Managers, October 2006.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-113, Guide to SSL VPNs, July 2008.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-114, User's Guide to Securing External Devices for Telework and Remote Access, November 2007.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-121 Revision 1, Guide to Bluetooth Security, June 2012.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise, June 2013.
- Office of Management and Budget (OMB) Memorandum for the Heads of Departments

and Agencies, June 2006.

- Office of Management and Budget (OMB) Memorandum for Agency CIO's: Security Authorization of Information Systems in Cloud Computing Environments, December 2011.
- ISO/IEC 27001.2015, ISO/IEC 27018.2019
- Global Data Protection Regulation
- Cloud Consume Privacy Act
- The Cloud Security Alliance

Policy Statements

1.0 Access Controls

1.1 POLICY REQUIREMENTS

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented Access Control Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

1.2 ACCOUNT MANAGEMENT

Lookout implements an information system account management process and includes the following characteristics:

Accounts are identified to include Production VPN Accounts, SSH Accounts, Management Console Account and MES Backoffice Application Accounts.

Account managers are assigned for information system accounts.

Establish conditions for group and role membership.

Control information system access, employing group and role membership and access authorizations for each account.

All information system accounts require approval by the Managers, Service Owners, and the Security team.

The account management process is capable of establishing, activating, modifying, disabling, or removing accounts in accordance with the Lookout User Offboarding procedures.

Monitor the use of information system accounts.

Mechanisms are implemented to notify account managers when accounts are no longer required, including when information system users are terminated transferred or when information system usage or need-to know/need-to-share changes.

Information system access is only granted based on a valid access authorization and intended system usage.

Information system accounts are reviewed quarterly.

No shared or group credentials are issued for the MES environment.

Lookout employs automated mechanisms to support the management of information system accounts, including those identified in

Temporary or emergency accounts are not allowed in the MES environment.

Inactive accounts are automatically disabled after ninety (90) days.

Notifications are automatically audited and generated and sent to the Security team based on:

Account creations

Account modifications and

Disabling and terminating actions.

Employees must log out when they expect to be away from their workstations.

Privileged user accounts are administered in accordance with group and role-based access schemas.

All privileged role assignments are monitored.

Actions are taken to disable and/or revoke access once users no longer require privileged role assignments.

Shared/group accounts are not permitted in the MES environment.

System accounts are monitored for atypical usage.

Any detection of atypical usage on system accounts is reported to the Incident Response Team (IRT) and Security team.

1.3 ACCESS ENFORCEMENT

The MES information system enforces approved authorizations for logical access to the system in accordance with applicable Lookout access control policies.

1.4 INFORMATION FLOW ENFORCEMENT

In order to regulate where information is allowed to travel, the Lookout MES information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems, based on access control policies.

The Lookout MES information system separates the information flow logically

1.5 SEPARATION OF DUTIES

Lookout ensures a clear “separation of duties” framework is documented and implemented, to include:

Separating duties of individuals, to include Continuous Delivery (CD), Engineering, Security, and Customer Support teams as necessary, to prevent malicious activity without collusion.

Documenting the separation of duties within Lookout.

Implementing and defining separation of duties through assigned information system access authorizations.

1.6 LEAST PRIVILEGE

All Lookout user access privileges follow a “least-privileges” concept, where only the minimum necessary system privileges are granted to perform job duties.

Lookout explicitly authorizes access to the Lookout MES information system and security relevant information.

All users of information system accounts or roles with access to security functions are required to utilize a unique, non-privileged account when performing non-administrative functions.

Privileged accounts on the information system are restricted to the Continuous Delivery(CD), Engineering, Security, and Customer Support teams.

Lookout has configured the MES information system to audit the execution of privileged functions.

Lookout employs mechanisms to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

1.7 UNSUCCESSFUL LOGIN ATTEMPTS

In order to maintain Lookout information system security and protect access credentials, Lookout:

Enforces a limit of no more than three (3) consecutive invalid login attempts by a user during a fifteen (15) minute time period.

Automatically locks the account/node for thirty (30) minutes until released by an administrator.

1.8 SYSTEM USE NOTIFICATIONS

The Lookout MES information system is configured to display a system use notification.

The Lookout MES information system retains the notification message or banner on the screen until explicit acknowledgement and action is taken to log on to or further access the information system.

Publicly accessible Lookout information systems:

Display the system use information before granting further access.

Display references, if applicable, to monitoring, recording, or auditing, that are consistent with privacy accommodations for such systems that generally prohibit those activities.

Include in the notice given to public users of the information system, a description of authorized usage.

1.9 CONCURRENT SESSIONS

Lookout limits the number of concurrent sessions for privileged users.

1.10 SESSION LOCK AND TERMINATION

The Lookout MES information system prevents further access to the system with a session lock.

The Lookout MES information system retains session locks until the session user reestablishes access using Lookout identification and authorization procedures

Upon the activation of a session lockout mechanism on a device with a display screen,information previously visible on the display is concealed with a publicly viewable image.

Mechanisms are employed to automatically terminate a user session after users log out.

1.11 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

No user actions can be performed on information systems without identification or authentication.

1.12 REMOTE ACCESS

Lookout documents and establishes usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

Remote access to the information system is authorized prior to allowing such connections.

Automated mechanisms are utilized to facilitate the monitoring and control of remote access methods, allowing event auditing across information system components.

The confidentiality and integrity of all remote access sessions is protected using encryption.

The Lookout MES information system is configured to route all remote access through a limited number of managed access control points (e.g. external firewall, load balancer, etc.).

Lookout only authorizes the execution of privileged commands and access to security-relevant information via remote access for compelling operational needs, documenting the rationale for such decisions in the System Security Plan.

Lookout disconnects or disables any unauthorized remote access connection to the system within a selected time in accordance with customer requirements.

1.13 WIRELESS ACCESS

Wireless access points are not permitted within the Lookout MES authorization boundary.

1.14 ACCESS CONTROL FOR MOBILE DEVICES

Usage restrictions,configuration requirements, connection requirements, and implementation guidance for mobile devices have been established.

Connection(s) of mobile devices to the MES environment are authorized with the Lookout MDM.

1.15 USE OF EXTERNAL INFORMATION SYSTEMS AND INFORMATION SHARING

Terms and conditions (where applicable) have been established allowing authorized access to Lookout information systems from external information systems.

Terms and conditions have been established allowing authorized individuals to process, store, and/or transmit Lookout-controlled information using the external information systems.

Only authorized individuals are permitted to use an external information system to access Lookout systems or to process, store, or transmit organization-controlled information only when the implementation of required security can be verified on the external system, in accordance with the Lookout's System Security Plan.

Lookout only permits the connections described above if they have an approved information system connection or processing agreement with the organizational entity hosting the external information system.

The use of portable storage devices by authorized individuals on external information systems is prohibited.

The products that make up the Lookout MES information system are not designed to be collaborative sharing services for the purpose of sharing data across organizations.

1.16 PUBLICLY ACCESSIBLE CONTENT

All access to the Lookout MES information system requires administrators/users to authenticate with defined identification and authentication processes.

2.0 Awareness and Training Policy

2.1 POLICY REQUIREMENTS

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented Security Awareness and Training Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2.2 TRAINING REQUIREMENTS

Basic security awareness training is provided to information system users (including managers, senior executives, and contractors):

- As part of initial training for new users;
- When required by system changes; and
- Annually thereafter.

Security awareness training includes recognizing and reporting potential indicators of an insider threat.

Role-based security-related training is provided:

- Before authorizing access to the system or performing assigned duties;
- When required by system changes; and
- Annually thereafter.

Individual information system security training activities including basic security awareness training are documented and monitored.

Individual training records are retained for at least one (1) year.

3.0 Audit and Accountability Policy

3.1 REVIEWS AND UPDATES

The Audit and Accountability Policy is to be reviewed and updated by the Sr. Director of Security and Sr. Director of Compliance with approval by The CFO, at least every three (3) years. Changes or revisions to this policy are communicated to all privileged users associated with the MES environment. Employees within applicable departments must acknowledge and comply with changes to the policy.

3.2 POLICY REQUIREMENTS

Management of proper auditing and accountability standards for the Lookout MES environment is crucial to ensuring the security and confidentiality of all customer data and information that traverses the Lookout MES authorization boundary. The following audit and accountability requirements, mechanisms, and provisions are to be applied for all employees, management, contractors, and other users who operate within the Lookout information system boundary:

Lookout must develop, disseminate, and review/update at least every three (3) years a formal, documented Audit and Accountability Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

3.3 AUDITABLE EVENTS

The Lookout MES information system audits the following events:

1.1. Successful and unsuccessful account logon events;

1.2. Account management events;

1.3. Object access policy change;

1.4. Privilege functions;

1.5. Process tracking; and

1.6. System events.

All Lookout web applications audit the following events:

1.7. Administrator activity;

1.8. Authentication checks;

1.9. Authorization checks;

1.10. Data deletions;

1.11. Data access;

1.12. Data changes; and

1.13. Permission changes.

In order to enhance mutual support and guide the selection of relevant auditable events, security audit functions are coordinated with all organizational entities requiring audit-related information.

All auditable events are supported with a rationale in order to be considered adequate for the after-the-fact investigations of security incidents.

Processes are in place to audit the following additional events, based on current threat information and ongoing risk assessment:

Auditable events are reviewed and updated annually or whenever there is a change in the threat environment.

3.4 AUDIT RECORDS AND REPORTS

At a minimum, audit records contain the following information:

Date of the event;

Time of the event (timestamp);

Event type;

Message (what events occurred);

Outcome or actions (success, failure, deny, drop, alert, alert/deny, alert/drop, etc.); and 1.6. User ID or account (if applicable).

Audit records are identified by type, location, or subject, include connection duration, the number of bytes received and sent, additional informational messages to diagnose or identify the event, and characteristics that describe or identify the object or resource being acted upon as part of the audit record content.

3.5 AUDIT REVIEW, ANALYSIS, AND REPORTING

All information system audit records are reviewed and analyzed at least weekly to identify any inappropriate or unusual activity, reporting any findings to the Security team. Automated mechanisms are employed to facilitate the implementation of audit review, analysis, and reporting processes for investigation or response to suspicious activity.

Situational awareness is maintained through the analysis and correlation of information across different repositories.

Support for on-demand audit review, analysis, and reporting and after-the fact investigation of security incidents is provided by ensuring information systems provide an audit reduction and report generation capability. These capabilities do not alter the original content or time ordering of audit records.

Mechanisms are in place to automatically process audit records for events based on successful and unsuccessful account logon events, account management events, object access, policy, privilege functions, process tracking, and system events as well as system resource usage information.

3.6 TIMESTAMPS

As part of the audit record content, information systems are configured to obtain time stamps from internal system clocks. Record time stamps for audit records are mapped to UTC time and meet one (1) second of granularity.

The MES information system compares internal system clocks at least hourly with the NIST time service. Information systems synchronize internal system clocks to the NIST time service when the time difference is greater than one (1) hour.

3.7 AUDIT RECORD RETENTION

All audit records are retained for at least ninety (90) days to provide support for after-the fact investigations of security incidents and to meet regulatory and Lookout information retention requirements.

The MES information system provides audit record generation capability for all the listed auditable events in AU-2. This applies to all information system components where audit capability is deployed/available where audit capability is deployed.

The MES information system allows the Incident Response Team and Security team to select which auditable events are to be audited by the specific components of the system.

The MES information system is capable of generating audit records for the list of auditable events (Ref. AU-2(a)) defined in this document.

3.8 PROTECTION OF AUDIT RECORDS

Mechanisms are in place to protect all audit information and audit tools from unauthorized access, modification, and deletion.

All audit records are backed up in near real-time onto a physically different system or system components than MES.

Access to the management of audit functionality is authorized only to select members of the Security and Engineering teams.

3.9 AUDIT STORAGE CAPACITY AND AUDIT PROCESSING FAILURES

Audit record storage capacity is adequately allocated, and auditing is configured in a manner that reduces the likelihood of such capacity being exceeded by employing a central log management system.

In the event of audit processing failures, mechanisms are in place to alert the Engineering team, Incident Response Team (IRT), and Security team.

In the event of auditing processing failures, mechanisms are in place to:

Overwrite oldest record in the event of a failure.

4.0 Security Assessment and Authorization Policy

4.1 REVIEWS AND UPDATES

The Security Assessment and Authorization Policy is to be reviewed and updated by the Sr. Director of Security and Sr. Director of Compliance with approval by The CFO, at least every three (3) years. Changes or revisions to this policy are communicated to all privileged users associated with the MES environment. Employees within applicable departments must acknowledge and comply with changes to the policy.

4.2 POLICY REQUIREMENTS

Management of the security assessment and authorization cycle for the Lookout MES environment is crucial to validating and ensuring the security and confidentiality of all customer data and information that traverses the Lookout MES authorization boundary. The following security assessment and authorization requirements, mechanisms, and provisions are to be applied for all employees, management, contractors, and other users who operate within the Lookout information system boundary:

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented Security Assessment and Authorization Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

4.3 SECURITY ASSESSMENTS

As part of ongoing security assessment and authorization requirements for federal accreditation, a Security Assessment Plan (SAP) is developed and documented. The Lookout SAP describes the scope of the assessment, including the following:

Security controls and control enhancements under assessment;

Assessment procedures used to determine security control effectiveness; and

Assessment environment, assessment team, and assessment roles and responsibilities.

Annually, a Third-Party Assessment Organization (3PAO) assesses the security controls in the information system to determine that controls have been implemented correctly and are operating as intended.

Upon assessment of the security controls, a Security Assessment Report is documented and contains the results of the assessment.

The results of the security assessment are provided, in writing, to the authorizing official or authorizing official's designated representative.

The Lookout security assessment on the information system is conducted by independent assessors or an assessment team with a 3PAO.

Announced penetration testing and vulnerability scanning is included as part of the annual security assessment.

Lookout accepts the results of the assessment performed by a FedRAMP accredited 3PAO when

the assessment meets the conditions of the Provisional-Authorization To Operate (P ATO).

As part of the ISO program, the Lookout organization engages a Third Party Assessment Organization to assess the effectiveness of the Lookout Information Security and Privacy Management System.

Upon assessment of the effectiveness of the ISO controls, the independent third party assessor will provide an updated ISO certificate for publication and dissemination to customers upon request.

4.4 INFORMATION SYSTEM CONNECTIONS

A process to authorize connections from the information system to other information systems outside of the MES authorization boundary is in place. The authorization connection process contains the use of Interconnection Security Agreements.

For each information system connection, the interface characteristics, security requirements, and the nature of the information communicated are documented.

Interconnection Security Agreements are reviewed and updated at least annually or when input is received from FedRAMP, or other Lookout MES customers.

The direct connection of the MES system to an external network without the use of boundary protections that meet Trusted Internet Connection (TIC) requirements is prohibited.

A deny-all, permit-by-exception policy is in place to facilitate MES connecting to external information systems.

An authorization process is in place for internal connections of Lookout Corporate to the information system, ensuring documentation for each connection is generated and contains interface characteristics, security requirements, and the nature of the information communicated.

4.5 PLAN OF ACTION AND MILESTONES

In order to document Lookout's planned remedial actions based on the security assessment of controls, a plan of action and milestones (POA&M) for the information system is developed and documented.

The existing plan of action and milestones (POA&M) is updated at least monthly based on the results of security assessments, analyses, and continuous monitoring activities.

4.6 SECURITY AUTHORIZATIONS

A senior-level executive or manager is assigned to the role of authorizing official for the information system, which is a critical leadership role. This appointment is reflected in the Roles and Responsibilities statement of several Lookout security documents.

Secure operations are ensured by requiring that the authorizing official authorize the information system before commencing operations.

The security authorization is updated in accordance with OMB A-130 requirements or when a significant change occurs that affects the system or operating environment.

4.7 CONTINUOUS MONITORING

A process for a continuous monitoring strategy and program is established and implemented. The continuous monitoring strategy and program includes the following characteristics and criteria:

Establishment of metrics identified by the FedRAMP Continuous Monitoring Strategy Guide, Appendix A to be monitored.

Establishment of continuous monitoring and annual monitoring for assessments supporting such

monitoring.

Ongoing security control assessments in accordance with organizational continuous monitoring strategy.

Ongoing security status monitoring of Lookout-defined metrics, per the continuous monitoring strategy.

Correlation and analysis of security-related information generated by assessments and monitoring.

Response actions to address results of the analysis of security-related information.

Security status reporting of Lookout and the information system to the appropriate FedRAMP and client organizational officials monthly.

Assessors or assessment teams with a FedRAMP accredited 3PAO are employed to monitor the security controls in the information system on an ongoing basis.

Assessors or assessment teams (Third Party Assessment Organizations (3PAO)) with appropriate accreditation are employed to monitor the security controls of the information security and privacy management system on an ongoing basis.

4.7.1 PENETRATION TESTING

A penetration test is conducted at least annually on all MES components.

An independent penetration agent or penetration team is employed to perform penetration testing on the system or components.

5.0 Configuration Management

5.1 REVIEWS AND UPDATES

The Configuration Management Policy is to be reviewed and updated by the Sr. Director of Security and Sr.Director of Compliance with approval by The CFO, at least every three (3) years. Changes or revisions to this policy are communicated to all privileged users associated with the MES environment. Employees within applicable departments must acknowledge and comply with changes to the policy. Management of the configuration of all system components in the Lookout MES environment is crucial to validating and ensuring the security and confidentiality of all customer data and information that traverses the Lookout MES authorization boundary. The following configuration management requirements, mechanisms, and provisions are to be applied for all employees, management, contractors, and other users who operate within the Lookout information system boundary:

5.2 POLICY REQUIREMENTS

Lookout must develop, disseminate, and review/update at least every three (3) years a formal, documented Configuration Management Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

5.3 BASELINE CONFIGURATION

Lookout develops, documents, and maintains under configuration control a current baseline configuration of the information system.

At least annually or when significant changes occur, the baseline configuration of the information system, including all network devices and machines, is reviewed and updated.

The baseline configuration of the information system is updated at least weekly or whenever directed by the JAB (such as versions or release numbers, descriptions of new or modified features, and security implementation guidance), MES customer requests, or industry requirements.

The baseline configuration of the information system is updated as an integral part of the information component installations and upgrades.

Automated mechanisms are employed to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the MES.

Previous versions of the baseline configuration are retained for at least six (6) months to support rollback.

Production-system related devices or components are not issued to Lookout personnel who are traveling to locations that are deemed to be of significant risk.

5.4 CONFIGURATION CHANGE CONTROL

A formal change control process has been developed and implemented. The change control

process includes the following types of processes:

A process to identify the types of changes to the information that are configuration controlled.

A process to approve changes to the system with explicit consideration for security impact analysis.

A process to document approve changes to the system.

A process to retain and review records of changes to the system.

A process to audit activities associated with changes to the system.

A process to coordinate and provide configuration change control oversight through the Change Advisory Board (CAB) that will convene as needed.

All changes to the MES information system are analyzed to identify any potential security impacts prior to change implementation.

Physical and logical access restrictions associated with changes to the information system are enforced. Access restrictions are defined, documented, approved, and enforced.

Lookout enforces access restrictions and supports auditing of the enforcement actions.

Installation of Vendor provided updates without verification that the software and/or firmware has been digitally signed using a certificate that is recognized and approved by Lookout is prevented.

Privileges to change information system components and system-related information within the MES information system are limited.

Privileges are reviewed and reevaluated at least quarterly.

5.5 CONFIGURATION SETTINGS AND LEAST FUNCTIONALITY

Lookout establishes, documents, and implements mandatory configuration settings for information technology products employed within the information system, and ensures these configuration requirements are implemented. Information system configurations align to the Center for Internet Security (CIS) Level 1 Benchmarks Guidelines, reflecting the most restrictive mode consistent with operational requirements.

Only defined and documented configuration settings are implemented in the MES information system, and any exceptions are identified, documented, approved, and support explicit operational requirements.

Changes to the configuration settings are monitored and controlled in accordance with current policies and procedures.

Automated mechanisms are employed to centrally manage, apply, and verify configuration settings for databases, operating systems, and servers.

Information systems are configured with the least functional capability, providing only essential capabilities. The use of ports, protocols, and services is restricted in accordance with CIS Level 1 Benchmarks Guidelines.

Information systems are reviewed monthly to identify and eliminate unnecessary functions, ports, protocols, and services.

The MES information system prevents program execution in accordance with the Configuration Management Policy regarding software program usage and restrictions.

Defined software programs not authorized to execute on the information system are identified and an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs

on the information system is employed. The unauthorized software programs list is reviewed and updated at least annually or when there is a change.

5.6 INFORMATION SYSTEM COMPONENT INVENTORY

An inventory of information system components has been developed, documented, and implemented. The inventory includes the following characteristics:

Accurately reflects the current information system.

Consistent with the authorization boundary of the information system.

Granular enough to support tracking and reporting purposes.

Includes information deemed necessary to achieve effective proper accountability.

Is available for review and audit by designated organizational officials

The information system component inventory is reviewed and updated at least monthly.

Updating the inventory of information system components is integrated into the processes for all component installations, removals, and information system updates.

Automated mechanisms are employed continuously, using automated mechanisms with a maximum five-minute delay to detect the presence of unauthorized hardware, software, and firmware components within the information system. Upon the detection of unauthorized components, the component is isolated, and the Security team is notified.

Lookout reviews and verifies that all components within the authorization boundary of the information system are inventoried as part of the system or recognized by another system as a component within that system.

5.7 CONFIGURATION MANAGEMENT PLAN

A formal Configuration Management Plan has been developed, documented, and implemented by Lookout for the information system.

The Lookout Configuration Management Plan identifies key roles, responsibilities, and configuration management processes and procedures.

A process to identify configuration items throughout the system development life cycle, and a process for managing the configuration of the configuration items are established within the Configuration Management Plan.

Configuration items for the information system are defined in the Configuration Management Plan, including when in the system development life cycle, the configuration items are placed under configuration management.

The Configuration Management Plan is protected from unauthorized disclosure and modification.

5.8 SOFTWARE USAGE RESTRICTIONS AND USER-INSTALLED SOFTWARE

Usage of software and associated documentation that is in accordance with contract agreements and copyright laws is enforced.

The use of software and associated documentation protected by quantity licenses to control copying and distribution is tracked. The use of Peer-to-Peer (P2P) software to restrict its participation in the unauthorized distribution, copying, display, or performance of copyrighted work is controlled and documented.

The use of open source software is restricted. Policies governing the installation of software by users are established, installation policies through logging and monitoring and defined administration permission levels are enforced, and policy compliance is monitored continuously.

6.0 Contingency Planning Policy

6.1 REVIEWS AND UPDATES

The Contingency Planning Policy is to be reviewed and updated by the Sr. Director of Security and Sr. Director of Compliance with approval by The CFO, at least every three (3) years. Changes or revisions to this policy are communicated to all privileged users associated with the MES environment. Employees within applicable departments must acknowledge and comply with changes to the policy.

6.2 POLICY REQUIREMENTS

Managing the Contingency Planning cycle for the Lookout MES environment is crucial to validating and ensuring the security and confidentiality of all customer data and information that traverses the Lookout MES authorization boundary, and reinforces the ability for Lookout to maximize the availability of the MES environment for its customers. The following contingency planning requirements, mechanisms, and provisions are to be applied for all employees, management, contractors, and other users who operate within the Lookout information system boundary.

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented Contingency Planning Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

6.3 CONTINGENCY PLAN

A formal Contingency Plan for the information system has been developed. The Lookout Contingency Plan includes the following characteristics:

Identifies essential missions and business functions and associated contingency requirements.

Provides recovery objectives, restoration priorities, and metrics.

Addresses contingency roles, responsibilities, and assigned individuals with contact information.

Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure.

Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented.

Is reviewed and approved by the Director of Incident Response.

A process to coordinate contingency planning activities with incident handling activities is employed.

Copies of the Contingency Plan are distributed to Lookout employees with Disaster Recovery (DR) responsibilities.

The Contingency Plan for the information system is reviewed at least annually. In addition to annual reviews, the Contingency Plan is revised to address changes to the organization, information system, or environment of operation and problems encountered during the Contingency Plan implementation, execution, or testing.

Changes to the Contingency Plan are communicated to Lookout employees with Disaster

Recovery (DR) responsibilities.

The Contingency Plan is protected from unauthorized disclosure and modification.

As part of the contingency planning process, the information system's Contingency Plan development is coordinated with organizational elements responsible for related plans.

Capacity planning is conducted in order to ensure information processing, telecommunications, and environmental support exists during contingency operations.

Lookout plans for the resumption of essential missions and business functions within no more than thirty (30) minutes of Contingency Plan activation.

Critical information system assets supporting essential missions and business functions are identified.

6.4 CONTINGENCY TRAINING AND TESTING

Key personnel assigned to contingency roles are trained on their responsibilities for the information system. Training is conducted:

Within ten (10) days of assuming a contingency role or responsibility.

When required by the information system changes.

At least annually thereafter.

The Lookout Contingency Plan is tested or exercised at least annually through functional exercises. Upon the completion of all functional exercises, the results are reviewed, and corrective actions are initiated to remediate any deficiencies.

Contingency Plan testing or exercises are coordinated with organizational elements responsible for related plans.

6.5 ALTERNATE STORAGE AND PROCESSING SITES

An alternate storage site, including necessary agreements to permit the storage and recovery of information system backup information is established. The alternate storage site provides information security safeguards equivalent to that of the primary site.

The current alternate storage site is separated from the primary storage site to prevent susceptibility of the same hazards.

Processes to identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster are in place. Explicit mitigation actions are defined for those potential accessibility problems.

An alternate processing site is established, including necessary agreements to permit the resumption of information system operations for essential mission and business functions within defined RTOs when primary processing capabilities become unavailable.

Processes to ensure that equipment and supplies required for the resumption of operations at the alternate processing site (or contracts to support delivery to the site that support the time period for the resumption of business operations) are in place.

Priority-of-service provisions are developed within alternate processing site agreements.

6.6 TELECOMMUNICATIONS SERVICES

Alternate telecommunication services are established to permit the resumption of information system operations for essential mission and business functions when the primary telecommunications capabilities become unavailable. Cloud Service Provider defined requirements for alternate telecommunication services are defined and documented (Ref.

Availability (low/moderate/high) in the Contingency Plan.

Priority-of-service provisions for primary and alternate telecommunications service agreements, including RTOs, are in place. Additionally, a process to request telecommunications service priority for all telecommunications services used for national security emergency preparedness in the event that the primary or alternate telecommunication services are provided by a common carrier is in place.

Alternate telecommunication services that reduce the likelihood for the sharing of a single point of failure with primary telecommunication services are obtained.

6.7 BACKUPS AND INFORMATION SYSTEM RECOVERY

Mechanisms are in place to conduct backups of user-level information, system-level information, and information system documentation on daily incremental and weekly full cycles. Backup storage capabilities are defined by maintaining three (3) of user and system-level information and information system documentation.

All backup information is protected at the defined storage locations in order to preserve confidentiality and integrity.

Backup information is tested at least annually in order to verify its reliability and integrity.

Backup copies of critical information software and security-relevant information are stored in a separate facility or in a fire-rated container.

Mechanisms and processes are in place to recover and reconstitute the information system to a known state following a disruption, compromise, or failure.

For systems that are transaction-based, mechanisms are in place to implement transaction recovery.

7.0 Identification and Authentication Policy

7.1 REVIEWS AND UPDATES

The Identification and Authentication Policy is to be reviewed and updated by the Sr. Director of Security and Sr. Director of Compliance with approval by The CFO, at least every three (3) years. Changes or revisions to this policy are communicated to all privileged users associated with the MES environment. Employees within applicable departments must acknowledge and comply with changes to the policy.

7.2 POLICY REQUIREMENTS

Identification and Authorization for all users, accounts, and actions within the Lookout MES environment is crucial to validating and ensuring the security and confidentiality of all customer data and information that traverses the Lookout MES authorization boundary. The following identification, authorization, and authentication requirements, mechanisms, and provisions are to be applied for all employees, management, contractors, and other users who operate within the Lookout information system boundary:

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented Identification and Authentication Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

7.3 USER IDENTIFICATION AND AUTHENTICATION

The MES information system uniquely identifies and authenticates all organizational users (or processes).

Multifactor authentication techniques are implemented for network access to privileged and non-privileged accounts.

Multifactor authentication techniques are implemented for local access to privileged accounts.

If group authenticators were used, individuals would be required to be authenticated with an individual authenticator when a group authenticator is employed.

Lookout deploys replay-resistant authentication mechanisms for network access to privileged accounts.

Multifactor authentication for remote access to privileged and non-privileged accounts is implemented for the information system such that one of the factors is provided by a device separate from the system gaining access and the devices meets FIPS 140-2.

The MES information system accepts and electronically verifies Personal Identity Verification (PIV) credentials via SAML integration with identity providers providing this capability.

The MES information system uniquely identifies and authenticates all hosts within the environment before establishing a remote connection.

The7 customer is responsible for authenticating their internal account credentials to access the Cloud through the use of SAML integration. The 7customers rely on their own account management infrastructure. Customers are also responsible for implementing strong identification and authentication in accordance with their own FISMA/FedRAMP requirements. Through the

synchronization process, federal customers authenticate to their instance using their own PIV authenticators and/or FICAM third party credentials.

7.4 IDENTIFIER MANAGEMENT

Information system identifiers for users and devices are managed by:

Utilizing a process to receive authorization from Management who assign user or device identifier.

Selecting an identifier that uniquely identifies an individual or device. Ensuring a process to assign the identifier to the intended user or device is developed and maintained.

Preventing the reuse of identifiers for at least two (2) years.

Disabling the user identifier after ninety (90) days for user identifiers.

Contractors that have access to the system are uniquely identified.

7.5 AUTHENTICATION MANAGEMENT AND CONTENT

Mechanisms to authenticate users and devices, including procedures to protect authenticator content, are implemented by:

At a minimum, verifying the identity of the device or individual receiving the initial authenticator content.

Defining initial authenticator content.

Ensuring authenticators have sufficient strength of mechanism for their intended use.

Developing and implementing procedures for all authenticator distribution, lost/compromised or damaged authenticators, and authenticator revocation.

Changing the default content of all authenticators upon system installation.

Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators.

Changing and/or refreshing authenticators every thirty (30) seconds with Okta.

Protecting authenticator content from unauthorized disclosure and modification.

Requiring users to take, and implementing, specific measures to safeguard authenticators.

Changing authenticators for group/role accounts when membership to those accounts' changes. Lookout does not have group/role accounts.

Password-based authentication for the MES information system:

Enforces a minimum password complexity requirement of (does not apply to mobile devices):

Enforces at least one (1) character change when new passwords are created.

Enforces the encryption of passwords in storage and in transmission.

Enforces password minimum and maximum lifetime restrictions of at least one (1) day and at most one-hundred eighty (180) days.

Prohibits password reuse for twenty-four (24) generations.

Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Lookout employs public key infrastructure (PKI) authentication that:

Is capable of validating certificates by constructing a certification path with status information to an accepted trust anchor.

Will be capable of enforcing authorized access to the corresponding private key.

Will be able to map the authenticated identity to the user account.

Implements a local cache of revocation data to support path discover and validation in case of inability to access revocation information via the network.

This control is not applicable. Lookout does not use hardware or biometric authenticators.

Password authenticators are sufficiently strong upon creation to satisfy NIST SP 800-63 requirements.

Authenticators commensurate with the security category of the information to which the use of the authenticator permits access are protected.

Unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

This control is not applicable. Lookout does not use hardware or biometric authenticators.

The MES information system obscures feedback of authentication information during the authentication process (e.g. asterisk or bullet symbols displayed on a screen when a user enters their password).

Mechanisms are employed to apply cryptographic modules to authenticator content in order to meet any requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

8.0 Incident Response Policy

8.1 POLICY REQUIREMENTS

Proper management of the Incident Response process for the Lookout MES environment is crucial to validating and ensuring the security and confidentiality of all customer data and information that traverses the Lookout MES authorization boundary. The following incident response requirements, mechanisms, and provisions are to be applied for all employees, management, contractors, and other users who operate within the Lookout information system boundary

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented Incident Response Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This policy is reviewed by the Sr. Director of Compliance, Sr. Director of Security and Sr. Director of Operations and Incident Response and is approved by The CFO.

8 .2 INCIDENT RESPONSE TRAINING AND TESTING

A formal incident response program is implemented for the MES information system, to include training personnel in the incident response roles and responsibilities. Personnel receive training before assuming an incident response role/responsibility.

Incident response training is conducted at least annually for refresher purposes and when required by information system changes.

In order to determine the effectiveness of its incident response capability, the incident response capability for the information system is tested at least annually using mock security incidents in the form of tabletop exercises. The testing results of the incident response exercise are documented.

Incident response testing is coordinated within elements responsible for related plans.

8.3 INCIDENT HANDLING, MONITORING, REPORTING, AND ASSISTANCE

The incident handling capability includes mechanisms that are capable of the following phases:

Preparation

Detection and Analysis

Containment

Eradication

Recovery

Incident handling activities are coordinated with contingency planning activities.

For ongoing incident handling activities, lessons learned are incorporated into all incident response procedures, training, and tests/exercises, implementing changes accordingly.

Automated mechanisms are implemented to support the incident handling process.

Mechanisms are employed to track and document information system security incidents.

All suspected security incidents are reported to the Incident Response Team and Security team immediately.

Security incidents are reported to US-CERT, in accordance with applicable laws and regulations.

Automated mechanisms are employed to support the reporting of security incidents.

An incident response support resource that provides user advice, assistance, and guidance on incident handling and reporting, is provided.

Automated mechanisms are utilized to increase the availability of incident response related information and support.

A direct, cooperative relationship has been established between the incident response capability and external providers of information system protection capability.

Organizational incident response members are identified to external providers.

8.4 INCIDENT RESPONSE PLAN

The Incident Response Team and Security team review the Incident Response Plan at least annually.

An Incident Response Plan has been developed that:

Provides a roadmap for implementing incident response capabilities.

Describes the structure and organization of the incident response capability.

Provides a high-level approach for how the incident response capability fits the organization overall.

Meets the unique requirements of the organization, which relate to mission, size, structure, and functions.

Defines reportable incidents.

Provides metrics for measuring the incident response capability within the organization.

Defines the resources and management support needed to effectively maintain and mature incident response capability.

Copies of the Incident Response Plan are distributed to Engineering and the Incident Response Team.

The Incident Response Plan is revised as necessary to meet changing needs as a result of plan implementation, execution, or testing.

Changes to the Incident Response Plan are communicated to the Incident Response Team.

The Incident Response Plan is protected from unauthorized disclosure and modification.

8.5 INFORMATION SPILLAGE RESPONSE

Information spillage responses include identifying the specific information involved, isolating and eradicating the contaminated information system or component, and performing lessons learned documentation exercise.

The Incident Response Team is alerted of the information spill using a method of communication not associated with the spill.

Incident Response Team personnel are assigned the responsibility of responding to information spills.

Information spillage response training is provided at least annually.

Information spillage response processes are implemented to ensure that personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are

undergoing corrective actions.

Information spillage training and non-disclosure agreements are employed for personnel exposed to information not within assigned access authorizations.

9.0 SYSTEM MAINTENANCE POLICY

9.1 POLICY REQUIREMENTS

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented System Maintenance Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This Policy is reviewed and updated by the Sr. Director of Security and Sr. Director of Compliance with approval by the CFO.

9.2 SYSTEM MAINTENANCE PROCESSES

The AWS Security Assurance Manager is responsible for controlling and managing maintenance activities on all AWS components.

As part of timely maintenance, Lookout relies on AWS to obtain maintenance support and/or spare components for critical/vital network and storage devices for MES within the time period defined in component SLAs in accordance with the MES RTO.

9.3 SYSTEM MAINTENANCE TOOLS

AWS is responsible for managing all maintenance tools for AWS components.

9.4 NON-LOCAL AND REMOTE MAINTENANCE

Lookout relies on AWS to have processes in place to authorize, monitor, and control non-local maintenance and diagnostic activities.

Non-local and maintenance tools will only be allowed as directed in Lookout security policies and these allowed instances are documented in the System Security Plan for the information system.

In order to mitigate vulnerabilities associated with non-local sessions, Lookout relies on AWS to employ strong identification and authentication techniques in the establishment of non local maintenance and diagnostic sessions.

Lookout relies on AWS to maintain records for all non-local maintenance and diagnostic activities.

Lookout relies on AWS to have mechanisms and processes in place to terminate all sessions and network connections when non-local maintenance is completed.

If non-local maintenance and diagnostic connections are used on the information system, Lookout relies on AWS to document the installation and use within its System Security Plan.

9.5 SYSTEM MAINTENANCE PERSONNEL

AWS is responsible for managing maintenance personnel or all AWS components.

10.0 Media Protection Policy

10.1 POLICY REQUIREMENTS

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented Media Protection Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This Policy is reviewed and updated by the Sr. Director of Security and Sr. Director of Compliance with approval by the CFO.

10.2 MEDIA ACCESS AND USE

AWS is responsible for implementing and managing all media protection controls inclusive of media access and use for all AWS components.

10.3 MEDIA MARKING, STORAGE, AND TRANSPORT

AWS is responsible for all implementing and managing all media protection controls inclusive of media marking, storage, and transport for all AWS components.

10.4 MEDIA SANITIZATION

AWS is responsible for implementing and managing all media protection controls inclusive of media sanitization and disposal for all AWS components.

11.0 Physical and Environmental Protection Policy

11.1 POLICY REQUIREMENTS

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented Physical and Environmental Protection Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This Policy is reviewed and updated by the Sr. Director of Security and Sr. Director of Compliance with approval by the CFO.

11.2 PHYSICAL ACCESS AUTHORIZATIONS AND CONTROL

AWS is responsible for implementing and managing all physical and environmental protection controls inclusive of access authorizations for all AWS components.

11.3 ACCESS CONTROL FOR TRANSMISSION MEDIUM, OUTPUT DEVICES, POWER EQUIPMENT, AND CABLING

AWS is responsible for implementing and managing all physical and environmental protection controls inclusive of access controls for transmission mediums, output devices, and power equipment and cabling for all AWS components.

11.4 MONITORING PHYSICAL ACCESS AND VISITOR CONTROLS

AWS is responsible for implementing and managing all physical and environmental protection controls inclusive of monitoring physical access and managing visitor access records.

11.5 EMERGENCY SHUTOFF, EMERGENCY POWER, AND EMERGENCY LIGHTING

AWS is responsible for implementing and managing all physical and environmental protection controls inclusive of managing emergency shutoff, emergency power, and emergency lighting capabilities for all AWS components.

11.6 FIRE AND WATER PROTECTION

AWS is responsible for implementing and managing all physical and environmental protection controls inclusive of managing fire protection water damage capabilities for all AWS components.

11.7 TEMPERATURE AND HUMIDITY CONTROLS

AWS is responsible for implementing and managing all physical and environmental protection controls inclusive of managing temperature and humidity controls for all AWS components.

11.8 DELIVERY AND REMOVAL, ALTERNATE WORK SITES

AWS is responsible for implementing and managing all physical and environmental protection controls inclusive of managing delivery and removal activities and alternate work sites for all AWS components.

12.0 Security Planning Policy

12.1 POLICY REQUIREMENTS

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented Security Planning Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This Policy is reviewed and updated by the Sr. Director of Security and Sr. Director of Compliance with approval by the CFO.

12.2 SYSTEM SECURITY PLAN

For any certification, accreditation, or authorization process, a system security plan is developed that meets the following requirements:

Consistency with the organization's enterprise architecture;

Explicitly defines the authorization boundary for the system;

Describes the operational context of the information system in terms of missions and business processes;

Provides the security categorization of the information system, including supporting rationale;

Describes the operational environment for the information system;

Describes relationships with or connections to other information systems;

Provides an overview of the security requirements for the system;

Identifies any relevant overlays, if applicable;

Describes the security controls in place or planned for meeting those requirements, including a rationale for the tailoring and supplementation decisions; and

Be reviewed and approved by the authorizing official or designated representative prior to plan implementation.

Changes to the information system/environment or operation are reviewed and updated annually in order to address problems identified during the system security plan implementation or security control assessments. Copies of the system security plan are communicated and distributed to personnel managing and operating the system, and 3PAO representatives.

The System Security Plan is protected from unauthorized disclosure and modification.
Security-related activities affecting the information system are planned and coordinated with all applicable parties before conducting such activities in order to reduce the impact on other Lookout entities.

12.3 RULES OF BEHAVIOR

Guidance that governs the acceptable use of information and information systems has been established and documented. These documented rules of behavior requirements are readily available to all information system users.

Before authorizing any access to information or the information system, each user must sign and

acknowledge to affirm they have:

Read,understood; and agreed to abide by the rules of behavior.

The rules of behavior are reviewed and updated at least every three (3) years and individuals who have signed a previous version of the rules of behavior are required to read and resign when the rules of behavior are revised or updated.

The rules of behavior include explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

12.4 INFORMATION SECURITY ARCHITECTURE

An information security architecture has been developed for the information system that:

Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of information;

Describes how the information security architecture is integrated into and supports the enterprise architecture; and

Describes any information security assumptions about, and dependencies on, external services.

The information security architecture is reviewed and updated annually to reflect updates in the enterprise and ensure that planned changes are reflected in the system security plan, the security Concept of Operations (CONOPS), and procurement/acquisitions.

13.0 Personnel Security Policy

13.1 POLICY REQUIREMENTS

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented Personnel Security Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This Policy is reviewed and updated by the Sr. Director of Security and Sr. Director of Compliance with approval by the CFO.

13.2 POSITION CATEGORIZATION

Processes to assign a risk designation of low, moderate, or high to all positions have been developed and executed.

Screening criteria have been established for individuals filling all positions for the MES environment.

Position risk designations are reviewed and revised at least every three (3) years.

13.3 PERSONNEL SCREENING

Personnel screening requirements are in place and working in tandem with risk-designation requirements. These mechanisms include the following requirements:

Personnel screening prior to authorizing access to the information system;

Rescreening is required every five (5) years as appropriate for national security clearances.

Individuals accessing an information system that processes, stores, or transmits information requiring special protections have valid access authorizations and satisfy personnel screening criteria as required by the level of the specific information.

13.4 PERSONNEL TERMINATIONS

A formal process is in place to terminate individual information system access the same day of their termination. The employee's direct manager, Human Resources, and the Security team are notified within twenty-four (24) hours.

Upon the termination of an individual's employment, Human Resources and the Security teams conduct exit interviews with the terminated employee that include continuous obligations in relation to confidentiality and non-disclosure or non-compete agreements and retrieve all security-related information system-related property.

Any information or systems formally controlled by the terminated individual are retained by Lookout.

13.5 PERSONNEL TRANSFERS

A formal personnel transfer process is in place that includes the review and confirmation of current logical and physical access authorizations to information systems and facilities upon reassignment.

Actions to ensure system access no longer required is removed are defined, documented, and implemented. These actions are completed within twenty-four (24) hours of a transfer.

Access authorizations are modified as needed to correspond with any changes in operational needs due to reassignment or transfer and notify the transferring employee's direct manager, Human Resources, and IT within twenty-four (24) hours.

13.6 ACCESS AGREEMENTS

Access agreements for Lookout information systems have been developed and documented.

All access agreements are reviewed and updated at least annually.

All individuals are required to read and sign appropriate access agreements to the information and information systems prior to being granted access and resign agreements to maintain access annually or when access agreements have been updated.

13.7 THIRD-PARTY PERSONNEL SECURITY

Security requirements for third-party personnel have been established and documented and include security roles and responsibilities. Third-party personnel are required to comply with Lookout security policies and procedures.

Third-party providers are required to notify Human Resources and Lookout Relationship Managers of any personnel transfers or terminations of third-party personnel who possess Lookout credentials and/or badges or who have current information system privileges the same day.

Third parties are monitored for compliance with all required personnel security requirements.

13.8 PERSONNEL SANCTIONS

A formal process for personnel sanctions has been developed and implemented for those personnel who fail to comply with Lookout's security policies and procedures, including a requirement for notification to the employee, the employee's direct manager and Human Resources immediately when a formal personnel sanctions process is initiated, identifying the individual sanctioned and the reason or the sanction.

14.0 Risk Assessment Policy

14.1 POLICY REQUIREMENTS

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented Risk Assessment Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This Policy is reviewed and updated by the Sr. Director of Security and Sr. Director of Compliance with approval by the CFO.

14.2 SECURITY CATEGORIZATION

A process to categorize information and the information system is developed, maintained, and employed in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Security categorization results (including supporting rationale) are documented in the System Security Plan for the information system.

All security categorization decisions for information and information systems are reviewed by the authorizing official or authorizing official designated representative.

14.3 RISK ASSESSMENT

A process to conduct risk assessments against information systems and their environments has been developed, documented, and maintained. Risk assessments include (at a minimum) the likelihood and magnitude of harm resulting from one of the following events:

Unauthorized access,

Unauthorized use,

Unauthorized disclosure,

Unauthorized disruption,

Unauthorized modification, or

Unauthorized destruction.

The results of conducted risk assessments on Lookout information and information systems are documented in a formal security assessment report. Documented risk assessment results are reviewed in accordance with OMB A-130 requirements or when a significant change occurs.

Risk assessment results are disseminated to security personnel and risk assessments are updated in accordance with OMB A-130 requirements or whenever there are significant changes to the information system, environment of operation, or other conditions that may impact the security state of the information system.

14.4 VULNERABILITY SCANNING

Vulnerability scanning mechanisms are deployed in the information system and on hosted applications that are configured to scan monthly. These mechanisms also scan when new vulnerabilities relevant to Lookout systems and applications are identified.

Operating systems, infrastructure, web applications, and databases are scanned monthly.

Vulnerability scanning tools and techniques are utilized to promote interoperability features among tools and automate parts of the vulnerability management process by using standards for:

Enumerating platforms, software flaws, and improper configurations;

Formatting and making transparent checklists and test procedures; and

Measuring vulnerability impact.

Scan reports and results from security control assessments are analyzed and assessed.

In accordance with risk assessment requirements, all legitimate vulnerabilities are remediated within:

Thirty (30) days for high-risk vulnerabilities;

Ninety (90) days for moderate-risk vulnerabilities; and

One-hundred eighty (180) days for low-risk vulnerabilities.

A process to share information obtained from the vulnerability scanning process and security control assessments with security personnel has been developed in order to help eliminate similar vulnerabilities in other information systems.

Vulnerability scanning tools that have the configuration capability to update the list of information system vulnerabilities scanned are employed.

Information system vulnerabilities scanned are updated prior to a new scan.

Vulnerability scanning procedures that can demonstrate the breadth and depth of coverage required are in place.

Controlled privileged access authorization to operating systems, infrastructure, databases, and web applications for all scans is allowed in order to facilitate more thorough scanning.

Automated mechanisms are in place to compare results of vulnerability scans over time to determine trends in information system vulnerabilities.

Historic audit logs are reviewed to determine if high vulnerabilities identified in the system have been previously exploited.

15.0 System and Services Acquisition Policy

15.1 POLICY REQUIREMENTS

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented System and Services Acquisition Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This Policy is reviewed and updated by the Sr. Director of Security and Sr. Director of Compliance with approval by the CFO.

15.2 ALLOCATION OF RESOURCES

Lookout determined and includes the security requirements for MES in mission/business process planning.

Processes are in place to determine, document, and allocate resources required to protect MES as part of its capital planning and investment control process. Additionally, a discrete line item for information security is accounted for in Lookout's programming and budgeting documentation for the information system.

15.3 LIFECYCLE SUPPORT AND SECURITY ENGINEERING PRINCIPLES

Lookout implements a formal system development life cycle (SDLC) for MES that includes information security considerations.

As part of the SDLC, Lookout identifies, defines, and documents information security roles and responsibilities.

Information security risk management processes are integrated into SDLC activities.

Processes are in place to apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

15.4 DEVELOPER CONFIGURATION MANAGEMENT AND SECURITY TESTING

MES developers/integrators ensure to:

Apply configuration management processes during information system development, implementation, and operation;

Document, control, and manage all changes to the information system configuration items; and

Implement only approved changes and ensure all changes are documented.

A formal security assessment plan is implemented as part of developer security testing. Unit, integration, system, and regression testing/evaluation are performed at depth and coverage in accordance with the Lookout SDLC processes, producing evidence of plan execution and results. Flaws identified during testing are corrected. Additionally, a verifiable flaw remediation process is implemented to correct any weaknesses and deficiencies identified during the security testing

and evaluation process. Furthermore, the results of security testing/evaluation and remediation action are documented and reported to the Security team.

Developers of the information system, system component, or information system service enable integrity verification of software and firmware components.

Developers of the information system, system component, or information system service employ static code analysis tools to identify common flaws and document results of analysis.

Developers of the information system, system component, or information system service perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

Developers of the information system, system component, or information system service employ dynamic code analysis tools to identify common flaws and document results of the analysis.

15.5 ACQUISITIONS AND SUPPLY CHAIN PROTECTION

A formal acquisition process is used that explicitly includes:

Security functional requirements;

Security strength requirements;

Security assurance requirements;

Security-related documentation requirements;

Requirements for protecting security-related documentation;

A description of the information system development environment and the environment in which the system is intended to operate; and

Acceptance criteria.

Any and all acquisitions require the developer of the information system, component, or service to provide a description of the functional properties of the security controls to be employed.

Developers of the information system, system component, or information system service provide design and implementation information for the security controls to be employed that include security-relevant interfaces, high-level design information, and implementation documentation sufficient to meet Lookout requirements.

Developers of the information system, system component, or information system service provide a plan for the continuous monitoring of security control effectiveness that contains the minimum requirements as defined in FedRAMP's continuous monitoring control

Developers of the information system, system component, or information system service identify, early in the SDLC, the functions, ports, protocols, and services intended for organizational use.

Only information technology products from the FIPS 201-approved products list of Personal Identity Verification (PIV) capability are implemented within organizational information systems.

15.6 INFORMATION SYSTEM DOCUMENTATION

Mechanisms are employed to protect information administrator documentation, including any documentation that describes the following:

Secure configuration, installation, and operation of the information system;

Effective use and maintenance of security features/functions; and

Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

Documentation for the information system is obtained, protected, and made available to authorized personnel users and describes:

User-accessible security features/functions and how to effectively use those security features/functions;

Methods for user interaction with the information system that enable individuals to use the system in a more secure manner; and

User responsibilities in maintaining the security of the information and information system.

Lookout documents or logs any attempts to obtain information system documentation when the documentation is not available or does not exist and develop the documentation or request documentation from the vendor.

Documentation is protected in accordance with risk management strategy and distributes documentation to Lookout authorized personnel.

15.7 EXTERNAL INFORMATION SYSTEM SERVICES

Prior to any acquisition with external information system services, external providers are required to comply with Lookout information system security requirements and to have implemented FedRAMP Moderate baseline security controls if federal information is processed or stored within the external system. This security control compliance is monitored by the provider in accordance with FedRAMP continuous monitoring requirements for external systems where federal information is processed or stored.

Government oversight and user roles and responsibilities for external information system services are required to be defined and documented.

An organizational assessment of risk is conducted prior to the acquisition or outsourcing of dedicated information security services.

The acquisition or outsourcing of dedicated information security services must be approved by the CISO and CDO.

All existing outsourced security services are documented.

Providers of all external systems where Federal information is processed or stored are required to identify the functions, ports, protocols, and other services required for the use of such services.

Risk assessments and security documentation requests are used to ensure that the interest of all external systems where Federal information is processed and stored are consistent with and reflect organizational interests.

The location of information processing, information data, and information services is restricted to the United States based on FedRAMP and agency requirements.

16.0 System and Communications Protection Policy

16.1 POLICY REQUIREMENTS

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented System and Communications Protection Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This Policy is reviewed and updated by the Sr. Director of Security and Sr. Director of Compliance with approval by the CFO.

16.2 APPLICATION AND INFORMATION PARTITIONING,

INFORMATION IN SHARED RESOURCES

Mechanisms are in place to separate user functionality (including user interface services) from information system management functionality.

Mechanisms to prevent unauthorized and unintended information transfer through shared system resources are in place.

16.3 DENIAL-OF-SERVICE (DOS) PROTECTION AND RESOURCE PRIORITY

The MES information system is protected against DoS attacks, to include compute, storage, and network-based attacks by employing AWS security primitives and controls.

16.4 BOUNDARY PROTECTION

Mechanisms have been implemented to monitor and control communications at the external boundary of the information system and at key internal boundaries within the information system (e.g., firewalls, load balancers, routers, etc.). The MES information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices.

Virtual Private Clouds (VPCs) and subnetworks have been implemented for publicly accessible information system components that are physically or logically separated from internal networks.

The number of access points to the information system is limited to provide for a more comprehensive monitoring of inbound and outbound traffic.

As part of the security requirements, Lookout:

Implemented a managed interface for each external telecommunication service;

Established a traffic flow policy for each managed interface;

Employed security controls to protect the confidentiality and integrity of information being transmitted;

Documents each exception to the traffic flow policy, including the supporting business rationale;

Reviews exceptions to the traffic flow policy at least annually; and

Removes traffic flow policy exceptions that are no longer needed.

At each managed interface, a deny-all network traffic rule is implemented and only network traffic through exception is allowed.

Mechanisms are employed to prevent remote devices that have established a non-remote connection with the information system from communicating outside of the communications path with resources in external networks.

Internal communications are routed to external networks through AWS Security Groups and AWS Internet Gateways.

Host-based boundary protection mechanisms are implemented for information system components.

Security tools, mechanisms, and support components are isolated from other internal information system components by implementing physically separated subnetworks with managed interfaces to other components of the information system.

The information system fails securely in the event of an operational failure of a boundary protection device.

16.5 ENCRYPTION AND KEY MANAGEMENT

Keys for required cryptography employed within the MES information system are established and managed in accordance with applicable requirements for key generation, distribution, storage, access, and destruction.

Symmetric cryptographic keys are produced, controlled, and distributed using FIPS compliant key management technology and processes.

Asymmetric cryptographics are produced, controlled, and distributed keys using NSA approved key management technology and processes.

Where required by applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance Lookout implements any required FIPS validated modules within MES. At a minimum, FIPS-validated cryptography to protect unclassified information is employed.

Public key certificates are issued under a formalized certificate policy or obtained under an appropriate certificate policy from an approved service provider.

Information considered to be “at rest” is protected for confidentiality and integrity purposes. Cryptographic mechanisms are implemented to prevent unauthorized disclosure and modification of user-level and system-level information on information system components.

16.6 NETWORK DISCONNECT, SESSION AUTHENTICITY,

RESOURCE AVAILABILITY

The availability of resources is protected by allocating additional resources.

Mechanisms to ensure that network connections to the information system are terminated at the end of a communication session or after 30 minutes of inactivity for RAS-based sessions and after 60 minutes for non-interactive user sessions are in place.

Mechanisms to protect the authenticity of communications sessions are employed.

16.7 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Mechanisms are in place to protect the confidentiality and integrity of transmitted information.

Cryptographic mechanisms are employed to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by alternative physical safeguards.

16.8 COLLABORATIVE COMPUTING DEVICES, MOBILE CODE, VOICE-OVER-INTERNET-PROTOCOL (VOIP)

Collaborative computing devices are prohibited within the MES environment.

All acceptable and unacceptable mobile code and mobile code technologies are defined and documented. Additionally, usage restrictions and implementation guidance have been established. Furthermore, the use of acceptable and unacceptable mobile code and mobile code technologies within the information system are authorized, monitored, and controlled.

Usage restrictions and implementation guidance are established for any VoIP technologies used within the information system. The use of VoIP technologies within the information system is authorized, monitored, and controlled.

16.9 SECURITY NAME/ADDRESS RESOLUTION SERVICES

The MES information system has the capability to provide additional data origin and integrity artifacts along with authoritative data that the information system returns in response to any name/address resolution queries.

The MES information system provides the means to indicate the security status of child zones and to enable verification of chain of trust among parent and child domains when operating as part of a distrusted, hierarchical namespace.

Mechanisms are employed so that the information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the information system receives from authoritative sources.

Information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

16.10 PROCESS ISOLATION

A separate execution domain is maintained for each executing process for the information system.

17.0 System and Information Integrity Policy

17.1 POLICY REQUIREMENTS

Lookout develops, disseminates, and reviews/updates at least every three (3) years a formal, documented System and Information Integrity Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

17.2 FLAW REMEDIATION

Mechanisms and processes are in place to identify, report, and correct information system flaws.

Software updates related to flaw remediation are tested for effectiveness and potential side effects before installation, incorporating flaw remediation into the configuration management process.

Security-relevant software and firmware updates are installed within thirty (30) days of the release of the updates.

Automated mechanisms are in place to determine the state of flaw remediation for the information system at least monthly.

17.3 MEMORY AND MALICIOUS CODE

Malicious code mechanisms are implemented for the information system, including at all information system entry and exit points, to detect and eradicate malicious code.

Mechanisms are in place to automatically update the malicious code mechanisms whenever new releases are available.

Malicious code protection mechanisms have been configured to perform periodic scans of the information system at least weekly and real-time scans of files at all endpoints if they are downloaded, opened, or executed. In the event that malicious code is detected or identified, the malicious code protection mechanisms alerts the Security team and Incident Response Team.

Procedures are in place to address the reception of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Malicious code mechanisms are centrally managed.

Non-signature based malicious code detection mechanisms are implemented.

The information system employs modern operating system technologies to protect its memory from unauthorized code executions.

17.4 INFORMATION SYSTEM MONITORING

Monitoring mechanisms and processes are in place to monitor events on the MES information system for information system attacks, which include the following:

Attacks and indicators of potential attacks to ensure the system operates in an optimal, resilient, secure manner; and

Unauthorized local, network, and remote connections.

System and information event monitoring capabilities are in place to identify any unauthorized use of the information system.

Monitoring devices are deployed in strategic locations to collect Lookout-essential information and at ad-hoc locations within the system in order to track specific types of transactions considered to be of interest.

Information obtained from intrusion-monitoring tools is protected from unauthorized access, modification, and deletion.

Processes are in place to heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Legal opinion with regard to information system monitoring activities is obtained in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

Alerts and notifications on unexpected events are provided to the Incident Response Team (IRT) as events are detected.

Individual intrusion detection tools are connected and configured into an information system-wide intrusion detection system.

Automated mechanisms and tools are implemented to support near real-time analysis of information system monitoring events.

All inbound and outbound communications relating to the information system are monitored continuously for any unusual or unauthorized activities or conditions.

At a minimum, the information system monitoring mechanisms alert the Security team and Incident Response Team when indicators of a compromise or potential compromise occur, including:

Auditing functionality has been disabled or modified to reduce audit visibility;

Audit or log records have been deleted or modified; and

System reports failed logins or password changes for administrative or key service accounts.

A wireless intrusion detection system is employed to identify rogue wireless devices and to detect attack attempts and potential compromise or breach of the information system.

Information is correlated from monitoring tools employed throughout the information system.

Host-based monitoring mechanisms are implemented on information system components.

17.5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Processes are in place for Lookout personnel to receive information system security alerts, advisories, or directives from US-CERT on an ongoing basis.

Internal security alerts, advisories, or directives are generated when necessary and disseminated to system security personnel and administrators with configuration/patch management responsibilities.

Security directives are implemented in accordance with established time frames or the issuing organization is notified of the degree of noncompliance.

17.6 SECURITY FUNCTIONALITY VERIFICATION, SOFTWARE INFORMATION INTEGRITY

The correct operation of security functions is verified upon startup at least monthly.

The Security team and Incident Response Team are notified of failed security verification tests. The information system is restarted, and the Security team and Incident Response Team are notified when anomalies are discovered.

Mechanisms and processes are employed to detect unauthorized changes to and reassess the integrity of critical OS configuration files by performing continuous integrity scans of the MES.

The detection of unauthorized security relevant changes to the information system is incorporated into the incident response capability.

17.7 INFORMATION INPUT VALIDATION, ERROR HANDLING, INFORMATION OUTPUT HANDLING, AND RETENTION

Mechanisms and processes are in place to check and verify the validity of information inputs.

Potential security-relevant error conditions are identified, error messages for sensitive or confidential information are screened, and messages are only revealed to the Security team. Error messages do not reveal:

Username and password combinations;

Attributes used to validate a password reset request (e.g., security questions);

Personally identifiable information (excluding unique username identifiers provided as a normal part of a transactional record);

Biometric data or personal characteristics used to authenticate identity;

Sensitive financial records (e.g., account numbers, access codes); or

Content related to internal security functions (i.e., private encryption keys, whitelist or blacklist rules, object permission attributes and settings).

In accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements, processes have been developed and mechanisms have been implemented to handle and retain information within, and output from, the information system.

17.8 SPAM PROTECTION

The Lookout MES information system does not accept any inbound email. All email protocols are blocked or turned off.