DATA AND SYSTEM SECURITY SCHEDULE

All third-parties accessing or retaining M&T's Confidential Information, or accessing M&T's computer systems and networks, or both, must maintain suitable security controls commensurate with the level of risk and classification of data or system being accessed. Accordingly, with respect to information systems that retain, process, or otherwise access M&T Confidential Information or M&T computer systems or networks, Company shall establish, maintain, and enforce security measures that meet or exceed the requirements of this Schedule in order to protect against the destruction, loss, unauthorized access, use, or alteration of M&T Confidential Information, or systems, or any combination thereof. Notwithstanding the requirements of this Schedule, for so long as Company retains M&T's Confidential Information or has access to M&T's Confidential Information, computer systems, or networks, Company shall : (a) use commercially reasonable efforts to meet the ever-evolving risks facing the security of Confidential Information and computer systems and networks; (b) comply with all applicable privacy and security laws, regulations, and standards; and (c) maintain security measures that are no less rigorous than appropriate financial industry standards. In the event that Company subcontracts, outsources, or otherwise relies on a third-party in support of M&T or Company's obligations under the Agreement, Company shall ensure that such third-parties (including Subcontractors) meet the following requirements, and that Company exercises suitable oversight, to the extent applicable to the third-party's performance.

1. ACCESS CONTROL

a. Access: Company denies all access to information systems and resources by default. Access is granted by request for specific business purposes and requires approval by management. Company maintains appropriate usage restrictions and configuration/connection requirements for information systems (including wireless) access, which requires prior authorization for access to the systems prior to allowing such connections.

b. Account Management: Company configures its information systems and resources to enforce access control policies and standards and employs automated mechanisms to support information system account management, which removes, or disables, or both, temporary, emergency, and inactive accounts after a pre-determined time period for each type of account and requires or forces users to log out after a pre-determined amount of inactivity.

c. Access Control for Mobile Devices: Company maintains appropriate usage restrictions, configuration/connection requirements, and implementation guidance for organization-controlled mobile devices, and authorizes (as described above) the connection of mobile devices to organizational information systems.

d. Separation of Duties: Company employs the principle of separation of duties of individuals to reduce the risk of potential abuse and malevolent activity, documents the separation of such duties and individuals, and defines information system access authorizations.

e. Least Privilege: Company employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks and business functions. Company controls the use of administrative privileges by tracking, preventing, and correcting the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

f. No Non-Domestic Access: Company may not export or access from outside of the United States of America any M&T Confidential Information without M&T's express prior written consent, which may be withheld in M&T's sole discretion.

g. Premises Access: Company agrees that M&T in its sole discretion, but in compliance with law, may require Company to remove any person or entity from M&T property or prevent the access of any person or entity to M&T's systems, in which case that person or entity may not be reassigned to another M&T location.

2. AWARENESS AND TRAINING

a. Security Awareness Training/Role-Based Training: Company maintains, documents, and distributes a suitable security awareness and training policy that addresses the purpose, scope, roles, responsibilities, coordination among organizational entities, and compliance with the policy. Company maintains procedures that implement a suitable security awareness training policy. The program must be reviewed and updated regularly to reflect changes in the organizational risk management strategy and industry best practices and standards. Company provides role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the information system and as needed thereafter.

b. Security Training Records: Company documents and retains individual information security training activities, including basic security awareness training and specific information system security training.

3. AUDIT AND ACCOUNTABILITY

a. Audit Records:

i. Company's information systems will generate audit records containing the type of event, the date and time of the event, the location of the event, the source of the event, the outcome of and response to the event, the individual(s) associated with the event and any other information relevant to the event and provide such information to M&T upon request.

ii. Company agrees that M&T may, upon reasonable request (but not more than once every twelve (12) months), conduct a security audit of Company systems and physical facility which shall cover, at a minimum Company's security measures for its computer systems and physical facilities and its security policies, procedures, and controls, and prepare a confidential report thereon ("Security Report"). Such audit, which will occur during Business Hours, may be conducted by M&T's personnel. M&T's right to conduct a security audit and to have Company answer M&T's Security Questionnaire and conduct follow-up interviews shall not in any way diminish or alter Company's duties and liabilities under this Agreement.

iii. Company must either; provide a BITS Financial Institution Shared Assessment Program audit conducted annually and deliver to M&T the results of each audit ("FISAP Report") within thirty (30) days of its completion, the FISAP Report must include the Standardized Information Gathering ("SIG") questionnaire conducted in accordance with the BITS Agreed Upon Procedures ("AUP") and audit requirements as documented in the BITS guidance (Information can be obtained via WWW.BITSINFO.ORG/FISAP); or respond to M&T's information security questionnaire ("Security Questionnaire") that is designed to allow M&T to assess the status of Company's information security policies and procedures and controls including physical security and business continuity planning, operational security, and access controls.

b. Standardized Audit Reporting: Company will engage at least annually an independent certified public accounting firm acceptable to M&T to (i) conduct investigations of the general controls and practices associated with the facilities of Company and Company's vendors and contractors, as well as those associated with the Services, third parties, and the programs used to support Company's performance under this Agreement; and (ii) prepare a SSAE 18 Type II compliance report and certification based on such investigations ("SSAE 18 Report"). The scope of such investigations should include attestations of availability, security, privacy, processing integrity, disaster recovery, backup, and contingency plans and systems, and confidentiality, as appropriate.

c. Non-Repudiation: Information systems enforce non-repudiation to protect against an individual (or process acting on behalf of an individual) falsely denying having performed certain tasks, including creating information, sending and receiving messages, approving information, signing contracts, and approving procurement requests.

d. Audit Information:

i. Information systems protect audit information, including audit records, audit settings, audit reports, and audit tools from unauthorized access, modification, and deletion. Audit information must be backed up onto a physically different system or system component that the system or component being audited. The information systems implement cryptographic protection to ensure the integrity of audit information.

ii. Company retains audit records to provide support for after-the-fact investigations of Security Incidents and to meet regulatory and organizational information retention requirements.

4. SECURITY ASSESSMENT AND AUTHORIZATION

a. System Interconnections: Company authorizes connections between its information system and other information systems through the use of Interconnection Security Agreements. Company documents the interface characteristics, security requirements, and the nature of the information communicated for each interconnection, and reviews and updates the Interconnection Security Agreements regularly. Company prohibits the direct connection of any sensitive or Confidential Information system to a public network and employs a deny-all, permit-by-exception ("whitelisting") policy for allowing Company information systems to connect to external information systems.

b. Security Authorization: Company assigns a senior-level executive or manager as the authorizing official for the information systems, ensures that such official authorizes the information systems for processing before commencing operations, and periodically updates the security authorization as needed.

c. Continuous Monitoring: Company maintains a suitable Data Loss Prevention ("DLP") strategy and continuously monitors information systems to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information. Company's continuous monitoring program includes establishing metrics to be monitored, the frequency for monitoring, and for assessments for supporting such monitoring, ongoing security control assessments and ongoing security status monitoring of organization-defined metrics, in accordance with Company's continuous monitoring strategy, correlation and analysis of security-related information generated by assessments and monitoring, response actions to address the results of such analysis, and reporting the security status of the Company and information system to the appropriate personnel.

5. CONFIGURATION MANAGEMENT

a. Baseline Configuration: Company develops, documents, and maintains a current baseline configuration of the information systems. Baseline configurations are formally reviewed, and regularly updated, including when needed, as an integral part of information system component installations and updates. Company retains previous versions of baseline configurations of the information systems to support rollback, and maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration. Company establishes, implements, and actively tracks, corrects, and reports on the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

b. Configuration Change Control: Company establishes, implements, and actively manages the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to, in part; prevent attackers from exploiting vulnerable services and settings. Company: (a) determines the types of changes to the information systems that are configuration-controlled; (b) reviews proposed configuration-controlled changes to the information systems and approves or disapproves such changes with explicit consideration for security impact analyses; (c) documents configuration change decisions; (d) implements approved changes; (d) retains records of changes; (e) audits and reviews activities associated with configuration-controlled changes to the systems; and (f) coordinates and provides oversight for configuration change control activities. Company employs automated mechanisms to document proposed changes to the information system. Company tests, validates, and documents changes to the information systems before implementing the changes on the operational systems, and requires that an information security representative be a member of the configuration change control team.

c. Information System Component Inventory: Company develops and documents an inventory of information system components that accurately reflect the current information systems, which includes all components within the authorization boundary of the system, is at the level of granularity deemed appropriate for tracking and reporting, and reviews and updates the information system component inventory regularly and as needed. Company tracks and corrects all hardware devices on its non-public networks so that only authorized devices are given access, and tracks and corrects all software on such networks so that only authorized software is installed and can execute. All unauthorized or unmanaged devices and software are found and prevented from gaining access, installing, or executing.

d. Configuration Management Plan: Company develops, documents, and implements a configuration management plan for the information systems that addresses roles and responsibilities, as well as defines detailed processes and procedures for how configuration management is used to support the system development lifecycle. The plan describes how to move changes through the system, how to update baselines and configuration settings, how to maintain system component inventories, and how to control development, test, and operational environments.

6. CONTINGENCY PLANNING

a. Contingency Plan: Company develops a contingency plan for the information systems, which identifies essential business missions/functions and associated contingency requirements, provides recovery objectives and restoration responses, addresses contingency roles and responsibilities, addresses maintaining essential business functions in the event of system disruption or failure, and addresses full system restoration without deterioration of the security safeguards in place. Such plan must be regularly reviewed and updated as needed.

b. Contingency Training: Company provides contingency training to information system users consistent with assigned roles and responsibilities when an individual assumes a contingency role or responsibility, whenever required by information system changes, and periodically thereafter. Such training must include simulated events and automatic training environments to provide thorough and realistic contingency training.

c. Alternate Storage Site: Company maintains alternate storage locations permitting storage and prompt retrieval of information system backup information and maintaining information security safeguards equivalent to that of the primary site.

d. Information System Backup: Company conducts backups of user-level information, system-level information, and system documentation including security-related documentation, and protects the confidentiality, integrity, and availability of backup information at storage locations.

e. Information System Recovery and Reconstitution: Company provides for the recovery and reconstitution of the information systems to a known state after disruption, compromise, or failure. This recovery plan includes transaction-based recovery, and protects backup and restoration hardware, software, and firmware.

7. IDENTIFICATION AND AUTHENTICATION

a. Identification and Authentication (Organizational Users): Company information systems uniquely identify and authenticate organizational users, or processes (*e.g.* service accounts) acting on behalf of organizational users. Company information systems implement multifactor authentication for network and local access to both privileged and non-privileged accounts, such that one of the factors is provided by a device separate from the system gaining access. Company's systems provide for single-sign on capabilities and implements replay-resistant authentication mechanisms.

b. Identification and Authentication (Non-Organizational Users): Company information systems uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).

c. Authenticator Management: Company manages information system authenticators by: (a) verifying the identity of the individual, group, role, or device receiving the authenticator; (b) establishing initial authenticator content for authenticators defined by Organization; (c) ensuring that authenticators have sufficient strength for their intended use; (d) maintaining administrative procedures for initial authenticator distribution, for lost, compromised, or damaged authenticators, and for revoking authenticators; (e) changing default content of authenticators prior to information system installation; (f) establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; (g) changing/ refreshing authenticators; (h) protecting authenticator content from unauthorized disclosure and modification; (i) requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and (j) changing authenticators for group/role accounts when membership to those accounts changes. Company takes into consideration the type of authentication (e.g., hardware token-based, PKI-based, password-based, biometric-based, etc.) and applies additional security controls as appropriate.

8. INCIDENT RESPONSE

a. Incident Response Training: Company provides incident response training to information system users consistent with assigned roles and responsibilities upon assuming and incident response role or responsibility, when required by system changes, and regularly thereafter.

b. Incident Handling: Company implements security incident handling procedures that: (a) include preparation, detection, analysis, containment, eradication, and recovery capabilities, (b) coordinates incident handling activities with contingency planning activities, and (c) incorporates past security incidents into ongoing response procedures, training, and testing. Company coordinates with external organizations to correlate and share incident information to achieve cross-organizational awareness and more effective incident responses. This includes coordinating incident handling activities involving supply chain events with other organizations involved in the supply chain.

c. Incident Notification: In the event that Company discovers or is notified of any Security Incident, Company shall (i) immediately notify M&T thereof in writing, but no later than seventy two (72) hours from the time Company becomes aware of a Security Incident, including disclosing (a) the date, time, and cause of the incident if known, (b) the M&T Data, systems, or both which were exposed or at risk of exposure, and (c) whether Covered Information was accessed; (ii) promptly, in consultation with M&T, investigate the Security Incident; (iii) remediate, mitigate, or remediate and mitigate, the risk to the M&T Data or systems or effects of the Security Incident; (iv) preserve all related records and other evidence; (v) implement a plan to prevent such a Security Incident from reoccurring; and (vi) provide M&T with a written report on the outcome of its investigation including any risk to M&T Data or systems, the corrective action Company will take, or has taken, to respond to the breach or potential breach and such other information as M&T may reasonably request. Company maintains automated mechanisms to assist in the reporting of Security Incidents.

9. MAINTENANCE

a. Nonlocal Maintenance: Company: (a) approves and monitors nonlocal maintenance and diagnostic activities; (b) allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; (c) employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; (d) maintains records for nonlocal maintenance and diagnostic activities; and (e) terminates session and network connections when nonlocal maintenance is completed. Company protects nonlocal maintenance sessions by employing replay-resistance authenticators and separating the maintenance sessions from other network sessions by either physically or logically separated communication paths based upon encryption.

b. Timely Maintenance: Company obtains maintenance support, or spare parts, or both for information system components in a timely manner following system or component failure. Company performs preventative maintenance on critical information system components at regular intervals to ensure that they are in operating condition.

10. MEDIA PROTECTION

a. Media Use: Company prohibits the use with information systems of (a) portable storage devices when such devices have no identifiable owner and (b) sanitation-resistant media. Further, Company shall not store unencrypted Covered Information on any electronic device that is portable (including smartphones, tablets, laptops, PDAs, hard drives, USB drives, CD, DVD, flash memory device, or floppy disks.

b. Media Storage: Company physically controls and securely stores both digital and non-digital media, and protects information system media until such media are destroyed or sanitized using secure data destruction techniques that render data unrecoverable. Company employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access gained.

c. Media Transport: Company: (a) protects and controls information system media during transport outside of controlled areas using physical and technical safeguards; (b) maintains accountability for information system media during transport outside of controlled areas; (c) documents activities associated with the transport of information system media; and (d) restricts the activities associated with information system media to authorized personnel. Information systems implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside controlled areas.

d. Media Sanitation: Company sanitizes information system media prior to disposal, release from organizational control, or release for reuse in accordance with organizational policies, employing sanitation mechanisms with the strength and integrity commensurate with the security category or classification of the information. Company: (a) reviews and approves media to be sanitized to ensure effectiveness and compliance with records-retention policies and (b) tracks and documents the media sanitation process, including personnel who handled such media, and verifies that that sanitation of the media was effective prior to disposal. Company regularly tests the effectiveness of sanitation equipment to verify that the intended sanitation is being achieved. The information systems, system components, and system devices are capable of being purged/wiped remotely to protect data obtained by unauthorized individuals. The following methods of destruction are suggested by M&T for Company's consideration and selection: (i) burn, pulverize, or cross-shred papers so that they cannot be read or reconstructed; (ii) destroy or erase electronic files or media so that the they cannot be read or reconstructed, and (iii) engage a competent document destruction service to dispose of it. Company shall certify destruction of M&T Confidential Information in writing at M&T's request.

11. PHYSICAL AND ENVIRONMENTAL PROTECTION

a. Physical Access Control: For facilities housing information systems, Company: (a) enforces physical access authorizations at facility entrance/exit points by verifying individual access authorizations before granting access to the facility; (b) maintains physical access audit logs for entry/exit points; (c) uses security safeguards to control access of such facilities, including the use of security guards and physical access control devices (*e.g.* alarms, card swipe, keypads); (d) escorts visitors and monitors their activity; (e) secures, through direct and indirect means, physical access devices (*e.g.* keys, cards, combinations, credentials); (f) inventories physical access devices regularly; and (g) changes physical access devices when lost or compromised, or when individuals who are possession thereof are transferred or terminated.

b. Power Equipment and Cabling:

i. Company protects power equipment and power cabling for the information systems from damage and destruction.

ii. Company employs physically separate, redundant power cables to ensure that power continues to flow in the event that one cable is cut or otherwise damaged, as well as automatic voltage controls for critical information system component.

c. Location of Information System Components: Company positions information system components within the facility to minimize potential damage from environmental hazards (*e.g.* flooding, fire, tornados, earthquakes, hurricanes, vandalism, acts of terrorism, electromagnetic pulse, electrical interference, etc.) as well as physical hazards, including the opportunity for unauthorized access.

12. PLANNING

Information Security Architecture: Company maintains information security architecture for the information systems that includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The information security architecture is reviewed and updated regularly to reflect updates in the enterprise architecture, external impacts, and industry practices. These changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

13. PERSONNEL SECURITY

a. Personnel Screening: Company screens individuals prior to authorizing access to the information system and performs rescreening on individuals as needed. Company ensures that individuals accession an information system processing, storing, or transmitting classified information are cleared to the highest classification level of the information to which they have access.

b. Personnel Termination: Upon termination of an individual, Company promptly: (a) disables the individual's information system access; (b) terminates/revokes any authenticators/credentials associated with the individual; (c) conducts exit interviews that include information security topics; (d) legally binds the individual to prevent post-employment information disclosure; (e) retrieves all security-related organizational information system-related property (*e.g.* hardware authentication tokens, system administration technical manuals, keys, identification cards, building passes, etc.); and (f) retains access to organizational information and information systems formerly controlled by terminated individual.

14. RISK ASSESSMENT

a. Risk Assessment: Company: (a) conducts a risk assessment, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information systems and the information they process, store, or transmit; (b) documents and reviews the risk assessment results; and (c) updates the risk assessment regularly, and whenever there are significant changes to the information system or environment of operation (*e.g.* the identification of new threats and vulnerabilities).

b. Vulnerability Scanning: Company: (a) scans for vulnerabilities in the information systems and hosted application at least annually and when new vulnerabilities potentially affecting the system/applications are identified and reported; (b) employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for enumerating platforms, software flaws, and improper configurations, formatting checklists and test procedures, and measuring vulnerability impact; (c) analyzes vulnerability scan reports and results from security control assessments; (d) remediates legitimate vulnerabilities in accordance with organizational risk assessment; (e) shares information from the vulnerability scanning and security control assessments with appropriate personnel to help eliminate similar vulnerabilities in other information systems; (f) tracks, controls, prevents, and corrects the security use of wireless local area networks ("LANS"), access points, and wireless client systems; and (g) employs periodic external vulnerability scanning and periodic penetration testing to assess the overall strength of the Company's defenses (technology, processes, and employees).

15. SYSTEM SERVICES AND ACQUISITION

a. System Development Life Cycle: Company manages information systems using industry standard System Development Life Cycle ("SDLC") that incorporates information security considerations, defines and documents information security roles and responsibilities throughout the SDLC, identifies individuals having such roles or responsibilities, and integrates Company's information security risk management process into SDLC activities.

b. Developer Configuration Management: Company requires the developer of the information systems, system components, or system service ("Developer") to (a) perform configuration management during system, component, or service design, development, implementation, and operation; (b) document, manage, and control the integrity of changes to those systems, components, or designs; (c) implement only approved changes to the system, component, or service, and documents such approved changes and the potential security impact of each change; (d) track security flaws and flaw resolution within the system, component, or service, and report findings to appropriate personnel; and (e) maintain integrity verification of hardware, software, and firmware components.

c. Developer Security Testing and Evaluation: Company requires Developer to: (a) maintain a security assessment plan, and produce evidence and results thereof; (b) perform unit, integration, system, and regression testing and evaluation, and produce evidence and results thereof; (c) implement a verifiable flaw remediation process; and (d) remediate identified flaws. Company employs static and dynamic code analysis tools to identify common flaws and document the results of such analysis.

d. Supply Chain Protection: Company (a) protects against supply chain threats to the information systems, components, or service by employing security safeguards as part of a comprehensive information security strategy, including the use of secure acquisition strategies, contract, tools, and procurement methods for purchasing of information systems, components, and services from suppliers; (b) conducts supplier reviews prior to engaging into a contractual agreement to acquire information systems, components, or services; (c) maintains security safeguards to limit harm from potential adversaries targeting the organizational supply chain; and (d) conducts assessments of the information systems, components, or services prior to selection, acceptance, or update.

e. Development Process, Standards, and Tools: Company (a) requires Developer to follow a documents development process that explicitly addressed security requirements, identifies the standards and tools used in the development process, documents specific tool options used in the development process, and documents, manages, and ensures the integrity of changes to the process, tools, or both used in the development; (b) requires Developer to define quality metrics at the beginning of the development process and provide evidence of meeting such quality metrics; and (c) regularly reviews the development process, as well as the standards, tools, and tool options/configurations to determine if they adequately address the risks and meet industry standards.

16. SYSTEM AND COMMUNIATIONS PROTECTION

a. Security Function Isolation: Information systems isolate security functions from non-security functions using isolation boundaries to control access to and protect the integrity of hardware, software, and firmware that perform security functions, and implement code separation. Company implements security functions as a layered structure minimizing interactions between layers of the design and avoiding dependence by lower layers on the functionality or correctness of higher layers.

b. Boundary Protection: Information systems monitor and control communications at the external boundary of the system at key internal boundaries within the system, implement sub-networks for publicly accessible system components that are physically and logically separated from internal Company networks, and connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture. Company limits the number of external network connections. Information systems at managed interfaces deny network communications traffic by default and allow network communications traffic by exception for both inbound and outbound communications. Company manages the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

c. Transmission Confidentiality and Integrity: Information systems protect the confidentiality and integrity of transmitted information through the use of both physical and logical means, including employing protected distribution procedures and limiting access to peripherals (*e.g.* servers, computers, printers, scanners, facsimile machines), and through the use of encryption.

d. Protection of Information at Rest: Information systems protect the confidentiality and integrity of information at rest through the use of encryption or other suitable measures (*e.g.* storing such information off-line in a secure location).

e. Encryption: Any Covered Information retained or transmitted by an information system shall be encrypted at a rate of at least 256-bit encryption. Use of encryption shall be compliant with any and all applicable export laws, rules, and regulations.

f. Process Isolation: Information systems maintain a separate execution domain for each executing process through assigning each process a separate address space, or hardware separation mechanisms.

17. SYSTEM AND INFORMATION INTEGRITY

a. Flaw Remediation: Company: (a) identifies, reports, and corrects information system flaws; (b) tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; (c) installs security-relevant software and firmware updates once they are available; and (d) incorporates flaw remediation into the organizational configuration management process. Company centrally manages the flaw remediation process, which measures the time between flaw identification and flaw remediation and establishes a process for taking corrective actions.

b. Malicious Code Protection: Company: (a) employs Malicious Code protection mechanisms at information system exit and entry points (including web browsers and email) to detect and eradicate malicious code; (b) updates Malicious Code protection mechanisms whenever new releases are available and maintains organizational configuration management policy and procedures for managing such updates; (c) configures Malicious Code protection mechanisms to perform periodic scans of the information systems and real-time scans of files from external sources, as the files are downloaded, opened, or executed; (d) blocks, quarantines, or both, Malicious Code and maintains systems that send alerts to system administrator(s) in response to Malicious Code detection; and (e) addresses the receipt of false positives during Malicious Code detection and eradication, as well as all resulting potential impact on the availability of the information systems.

c. Information System Monitoring: Company: (a) monitors the information systems to detect attacks and indicators of potential attacks, and unauthorized local, network, and remote connections and identifies unauthorized use of the information system; (b) deploys monitoring devices strategically within the information system and at ad hoc locations within the system; (c) protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; (d) heightens monitoring activity when increased risk to organizational operations, assets, individuals, other organizations, or the nation is indicated; (e) obtains legal opinion with regard to information system monitoring activities in accordance with applicable laws, Executive Orders, directives, policies, or regulations; and (f) provides information system monitoring information to appropriate personnel as needed.

d. Software, Firmware, and Information Integrity: Company maintains integrity verification tools to detect unauthorized changes to software, firmware, and information. Company performs regular integrity checks and employs automated tools that provide notification to appropriate personnel upon the discovery of discrepancies during integrity verification, as well as automated response mechanisms to integrity violations. Such tools are centrally managed.

e. Security Alerts, Advisories, and Directives: Company receives information security alerts, advisories, and directives from the federal government, its Regulators, or other designated organizations with the authority to issue such directives on an ongoing basis and generates internal security alerts, advisories, and directives as deemed necessary. Company disseminates security alerts, advisories, and directives to the appropriate personnel, and implements security directives in accordance with established time frames, or notifies the issuing Company of the degree of noncompliance. Company employs automated mechanisms to make security alerts and advisory information available throughout the organization.