CYBERSECURITY
VENDOR COMPLIANCE PROGRAM (VCP)

SV Microwave, Inc.

PUBLIC

Public Release Authorized

Table of Contents

INSTRUCTIONS TO VENDORS

SV Microwave's data protection strategy includes the requirement to ensure the security of data protection controls, regardless of the location or the party responsible for those controls. As a vendor, you serve a crucial role to achieve this goal and your cooperation is greatly appreciated.

All vendors are expected to meet the minimum controls identified in this document. In some cases, SV Microwave may require a written response that may be an attestation of compliance, a submission of supporting documentation, or both.

If SV Microwave requests a written response from your organization, you are required to submit an electronic copy of the document(s) confirming compliance. If there are any requirements that are out of scope or that cannot be complied with, those requirements must be fully explained with a business justification and if there are any compensating controls that may exist to reduce risk associated with one of SV Microwave's vendor requirements not being met.

Please note that if your organization processes, stores or transmits SV Microwave data that is considered “sensitive,” additional data protection controls may be required.

VENDOR COMPLIANCE POLICY

Vendors must protect the confidentiality, integrity, and availability of SV Microwave, Inc. (SV Microwave) data and systems, regardless of how the data is created, distributed or stored. Vendors' security controls must be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system, in accordance with all legal obligations.

Management Intent: The successful implementation of SV Microwave's program depends on the successful implementation of each vendor's security controls.

MANAGEMENT DIRECTION FOR VENDOR INFORMATION SECURITY

The objective of this Vendor Compliance Program (VCP) is to provide direction to vendors for information security requirements that are in accordance with SV Microwave's business requirements, as well as relevant laws and other legal obligations for data security and privacy. [1]

SV Microwave is committed to protecting its employees, partners, clients and SV Microwave from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every vendor that interacts with SV Microwave data and/or systems. Therefore, it is the responsibility of VENDOR to be aware of and adhere to SV Microwave's information security requirements.

Protecting SV Microwave data and the systems that collect, process, and maintain this data is of critical importance. Therefore, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure the confidentiality, availability, and integrity of the data:

- Confidentiality – Confidentiality addresses preserving restrictions on information access and disclosure so that access is restricted to only authorized users and services.
- Integrity – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- Availability – Availability addresses ensuring timely and reliable access to and use of information.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes against accidental loss or destruction.

SCOPE

The requirements of the VCP applies to all vendors, contractors, consultants, interns or other third-parties that support SV Microwave.

INTENT

SV Microwave's **Minimum Security Requirements (MSR)** for information security are comprehensive in nature. Therefore, SV Microwave expects VENDOR to also have a comprehensive set of information security policies, standards and controls to protect SV Microwave's data and systems.

VENDOR's information security program must be reasonably designed to achieve the objectives to:

- Ensure the Confidentiality, Integrity, and Availability (CIA) of sensitive Personally Identifiable Information (sPII) and SV Microwave business information;
- Protect against any anticipated threats or hazards to the confidentiality, availability or integrity of such information; and
- Protect against unauthorized access to or use of such information.

[1] ISO/IEC 27002:2013 – 5.1

Best Practices Alignment

The National Institute of Technology & Standards (NIST) Special Publication 800-53 revision 4 (rev 4) represents leading industry-accepted best practices for information security. Therefore, SV Microwave's minimum security requirements for its vendors are consistent with NIST 800-53 rev 4 moderate baseline requirements to ensure due care and due diligence in maintaining its information security program.

Information Security Documentation

In order to reduce possible confusion, VENDOR must be aware of and abide by SV Microwave's use of terminology for information security documentation:

(1) Core policy that establishes management's intent;
(2) Control objective that identifies the condition that should be met;
(3) Standards that provides quantifiable requirements to be met;
(4) Procedures that establish how tasks must be performed to meet the requirements established in standards; and
(5) Guidelines are recommended, but not mandatory.

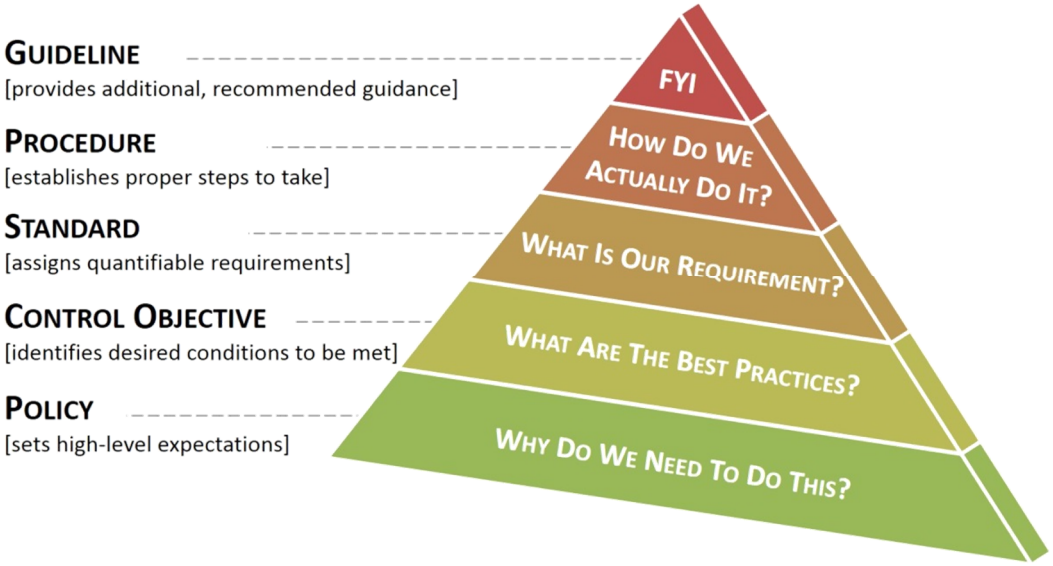

Figure 1: Information Security Documentation Framework

INFORMATION SECURITY PROGRAM MANAGEMENT (PM)

VENDOR is expected to implement IT security program management controls to provide a foundation for VENDOR's Information Security Management System (ISMS).

INFORMATION SECURITY PROGRAM

1. Security Policy: VENDOR must have a documented Information Security policy in place which meets applicable industry standards and which is subject to review by SV Microwave under a Non-Disclosure Agreement (NDA). This policy must be reviewed on a regular basis by VENDOR.

2. Information Security Management: VENDOR must develop a data security program that documents the policies, standards, and controls in use that relate to the provisions outlined below. This security plan must include organizational, administrative, technical, and physical safeguards and standards appropriate to the size and complexity, the scope of the activities and the sensitivity of the information at issue.

3. Management Commitment: VENDOR must have executive-level direction on information security and be able to demonstrate management commitment.

INFORMATION SECURITY GOVERNANCE

1. Contract: Before VENDOR can collect, use, transfer or store SV Microwave business information or systems, VENDOR must have a valid contract, statement of work, or purchase order with the privacy and security language in place.

2. Information Security Function: VENDOR must have an established information security function that has VENDOR's enterprise-wide responsibility for promoting information security.

3. SV Microwave-Specific Security Coordination: VENDOR must appoint an individual to coordinate the information security arrangements specific to SV Microwave.

4. Security Audit / Review: The VENDOR's information security program must be subject to thorough, independent and regular security audits/reviews.

5. Security Architecture: VENDOR must establish an information security architecture that provides a framework for the application of standard security controls throughout the VENDOR's enterprise.

COMPLIANCE

1. Statutory / Regulatory / Contractual Compliance. VENDOR must maintain a process to be aware of and be compliant with all applicable statutory, regulatory and contractual compliance requirements. Examples include but are not limited to PCI DSS, HIPAA, SOX, and GLBA.

2. Compliance Status: VENDOR must have a process to document non-compliance of any statutory, regulatory or contractual requirement:
    a. VENDOR must identify and quantify the risks and mitigation plans and document the business decision for alternate controls or risk acceptance; and
    b. The mitigation plan and business decision must be signed off by the Chief Information Officer (CIO) or an authorized individual who can accept responsibility and accountability on behalf of the VENDOR.

3. Breach Notification: VENDOR must maintain a documented breach notification process that meets all applicable legal and contractual requirements. The SV Microwave business owner of the solution must:
    a. Approve VENDOR breach notification process; and
    b. Own the SV Microwave response process.

4. Payment Card Industry Data Security Standard (PCI DSS): If VENDOR's solution processes, stores or transmits SV Microwave customers' cardholder data, VENDOR falls within scope of SV Microwave's PCI DSS compliance and therefore must:

a. Maintain documented compliance with the most current version of the PCI DSS;
b. Conduct quarterly network scans by an Approved Scanning Vendor (ASV); and
c. Obtain a Report of Compliance (ROC) from an annual on-site PCI Data Security Assessment with a Qualified Security Assessor (QSA).
    i. VENDOR may provide an annual Self-Assessment Questionnaire (SAQ) in lieu of an annual ROC that is issued by a QSA.

HUMAN RESOURCES SECURITY

1. Requirements for Employment: VENDOR must maintain contractual agreements with employees, contractors, consultants and/or other third party staff that formally documents their responsibilities for information security.

2. Roles and Responsibilities: VENDOR must define and document security roles and responsibilities of employees, contractors and third party users to incorporate SV Microwave's data protection control requirements, to the extent permitted by applicable law:
    a. All employees, contractors, and third-party users must be notified of the consequences for not following your security policy in handling SV Microwave data.
    b. All assets used to manage or store SV Microwave data must be protected against unauthorized access, disclosure, modification, destruction or interference.
    c. All employees, contractors and third party users must be provided with education and training in privacy and security procedures and the correct information processing requirements.
    d. All personnel with access to sensitive Personally Identifiable Information (sPII) must complete a privacy training class and be knowledgeable of any specific privacy requirements for the data being handled. Refresher training is required at least on an annual basis.

3. Assigned Ownership: VENDOR must assign ownership of critical and sensitive information, business applications, computer systems and networks to individuals (e.g., business managers) and document the responsibilities of these assigned owners.
    a. Responsibilities for protecting critical and sensitive information, business applications, computer systems and networks must be communicated to and accepted by owners.

4. Personnel Screening: VENDOR must ensure a secure workforce. Background verification checks on all VENDOR's candidates for employment should be carried out in accordance with relevant laws, regulations, and ethics and should be proportional to the business requirements and the classification of the information that may be accessed.

5. Staff Agreements: VENDOR must establish agreements with VENDOR's employees and/or VENDOR's employee representative that specify information security responsibilities. This agreement must be incorporated into the contracts of VENDOR's employees, contractors, consultants and/or other third party staff and be taken into account when screening applicants for employment.

ACCESS CONTROL (AC)

VENDOR is expected to implement logical access controls to limit access to systems and processes to authorized users.

LOGICAL ACCESS CONTROL

1. Access Control: VENDOR must restrict access to the application and associated information to authorized individuals. This must be enforced accordingly to ensure that only authorized individuals to gain access to business applications, systems, networks and computing devices, that individual accountability is assured and to provide authorized users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

2. User Authorization: VENDOR must ensure that all users have authorization before they are granted access privileges.
    a. User access privileges must be reviewed at least every six (6) months; and
    b. Access must be revoked within forty-eight (48) hours of a user's change in role or employment status.

3. User Authentication: VENDOR must ensure strong user authentication is implemented throughout the VENDOR's enterprise:
    a. All users must be authenticated by an individual identifier, not group or shared identifiers; and
    b. Strong authentication mechanisms must be used in conjunction with the identifier (e.g., strong passwords, smart cards or biometric devices) before the user can gain access to systems or data.

Privileged Account Management

1. Privileged Accounts: VENDOR must ensure that accounts with privileged access are separate from a user's normal, non-privileged account.

Off-Site Logical Security Considerations

1. Off-Premise Access Control: Whenever technically feasible, VENDOR must ensure cloud solutions offer the option to be federated to SV Microwave systems for authentication using SV Microwave credentials.

Awareness & Training (AT)

VENDOR is expected to ensure that users are made aware of the security risks associated with their roles and that users understand the applicable laws, policies, standards, and procedures related to the security of systems and data.

Security Awareness Program

1. Security Awareness: VENDOR's employees, contractors, consultants and/or other third party staff must be made aware of the key elements of information security, why it is needed, and understand their personal information security responsibilities. A security awareness program must be undertaken to promote security awareness to all individuals who have access to the information and systems of the VENDOR's enterprise.

Security Training

1. Security Education: VENDOR's employees, contractors, consultants and/or other third party staff must be trained in how to run systems correctly, as well as how to develop and apply security controls.

Audit & Accountability (AU)

VENDOR is expected to create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity by ensuring that the actions of individual users and systems can be uniquely traced.

Event Logging

1. Event Logging: VENDOR must log all key information security events, including but not limited to:
    a. All actions taken by any individual with root or administrative privileges;
    b. Access to all audit trails;
    c. Invalid logical access attempts;
    d. All individual user accesses to cardholder data;
    e. Use of and changes to identification and authentication mechanisms, including but not limited to:
    f. Creation of new privileged accounts and elevation of privileges; and
    g. All changes, additions, or deletions to accounts with root or administrative privileges;
    h. Initialization, stopping, or pausing of the audit logs; and
    i. Creation and deletion of system-level objects.

2. Intrusion Detection / Prevention: VENDOR must implement and monitor Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) mechanisms on all critical systems and networks.

Monitoring & Review

1. System Network Monitoring: VENDOR is required to develop and implement a process to review logs and security events for all system components to identify anomalies or suspicious activity that includes:
    a. Reviewing the following, at least daily:
    b. All security events;
    c. Logs of all system components that store, process, or transmit cardholder data, or that could impact the security of cardholder data;
    d. Logs of all critical system components; and
    e. Logs of all servers and system components that perform security functions. This includes, but is not limited to:
        i. Firewalls;
        ii. Intrusion Detection Systems (IDS);
        iii. Intrusion Prevention Systems (IPS); and
        iv. Authentication servers (e.g., Active Directory domain controllers); and
    f. Following up exceptions and anomalies identified during the review process.

Security Assessment & Authorization (CA)

VENDOR is expected to periodically assess systems to determine if IT security controls are effective and ensure IT security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

Control Testing

1. Testing: VENDOR must ensure that all elements of a system (e.g., application software packages, system software, hardware, and services) are rigorously tested before the system is promoted to a production environment.

2. Test Data: VENDOR must ensure any sensitive SV Microwave business information copied from the production environment must be protected by:
    a. Depersonalizing sensitive business information;
    b. Restricting access to business information in the development environment; and
    c. Erasing copies of SV Microwave business information once testing is complete.

3. Post-implementation Review: VENDOR must ensure a post-implementation review is conducted for all newly-promoted systems to the production environment.

Configuration Management (CM)

VENDOR is expected to maintain accurate inventories of its systems and enforce security configuration settings for information technology products employed in support of its business operations.

Configuration Management

1. Configuration Management: VENDOR must implement configuration standards for all system components that address known security vulnerabilities and are consistent with industry-accepted system hardening standards.

Change Management

1. Change Control: VENDOR must document and manage operating procedures for its change control process(es).

2. Change Management: VENDOR must ensure that changes to any systems, applications or networks, including “emergency” changes, are reviewed, tested, approved and applied using a change management process.

3. Change Documentation Retention: VENDOR must ensure that documentation of changes is retained for at least three hundred and sixty-five (365) days.

CONTINGENCY PLANNING (CP)

VENDOR is expected to establish, implement and maintain plans for the continuity of operations (COOP) in emergency situations to ensure the availability of critical information resources.

BUSINESS CONTINUITY & DISASTER RECOVERY

1. Business Continuity & Disaster Recovery: VENDOR must develop, support and routinely test a viable Business Continuity and Disaster Recovery (BCDR) plan that addresses all reasonably-foreseen contingency arrangements.

2. Resilience: VENDOR's applications, systems, and networks must be run on robust, reliable hardware and software, supported by alternative hardware or duplicate facilities.

3. Data Backups: VENDOR must ensure that backups of essential information and software are performed on a regular basis, according to a defined cycle discussed with and approved by SV Microwave.

IDENTIFICATION & AUTHENTICATION (IA)

VENDOR is expected to implement mechanisms are employed to properly identify system users, processes acting on behalf of users, or devices, and authenticate the identities of those users, processes, or devices.

USER ACCOUNTS

1. User Identification: VENDOR must assign all users a unique identification (ID) before allowing them to access systems. In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
    a. Something you know, such as a password or passphrase;
    b. Something you have, such as a token device or smart card; or
    c. Something you are, such as a biometric.

2. Unique Accounts: VENDOR must ensure proper user identification and authentication management for all standard and privileged users on all systems, as follows:
    a. Ensure that only authorized users are provided with user IDs;
    b. Ensure that user names and service accounts are uniquely named and in a manner consistent with organizationally defined guidelines; and
    c. Require written authorization by a supervisor or manager to receive a user ID.

3. Privileged Users: Where technically feasible, VENDOR must implement multifactor authentication for the system and network access from privileged accounts.

PASSWORD MANAGEMENT

1. Password Management: VENDOR must enforce strong passwords for all user and service accounts.

INCIDENT RESPONSE (IR)

VENDOR is expected to establish an actionable IT security incident handling capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities.

INFORMATION SECURITY INCIDENT MANAGEMENT

1. Incident Management: VENDOR must document all information security incidents and maintain a documented information security event management process that covers the incident response, escalation, and remediation of Information security events and incidents.

2. Reporting Incidents: VENDOR must inform SV Microwave without delay about any information security incident that could have an impact on SV Microwave's business operations with the VENDOR.

3. Integrity Requirements: VENDOR must assess and immediately escalate to SV Microwave about the impact of business information being accidentally corrupted or deliberately manipulated. The analysis of integrity requirements must determine how the accidental corruption or deliberate manipulation of information could have an impact on SV Microwave's business operations with the VENDOR.

4. Availability Requirements: VENDOR must assess and immediately escalate to SV Microwave about the impact of business information being unavailable for any length of time. The analysis of availability requirements must determine how a loss of availability of information could have an impact on SV Microwave's business operations with the VENDOR.

5. Forensic Investigations: VENDOR must have an established process for managing incidents that require forensic investigation, since it is the VENDOR's responsibility to preserve evidence and maintain the chain of custody for incidents within the VENDOR's areas of responsibility.

MAINTENANCE (MA)

VENDOR is expected to perform periodic and timely maintenance on systems, so that SV Microwave assets are protected from the latest threats.

MAINTENANCE

1. Maintenance: VENDOR must:
    a. Schedule, perform, document, and review records of maintenance and repairs on systems in accordance with manufacturer or vendor specifications and company requirements;
    b. Control all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
    c. Require explicit management approval for the removal of the systems or system components from company facilities for off-site maintenance or repairs;
    d. Sanitize equipment to remove all information from associated media prior to removal from company facilities for off-site maintenance or repairs; and
    e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

VULNERABILITY MANAGEMENT

1. Vulnerability Management: VENDOR must ensure a vulnerability management program exists to eliminate vulnerabilities that could be exploited by malware or other technical methods (e.g., exploitation through technical vulnerabilities). This includes, but is not limited to:
    a. Vulnerability remediation;
    b. Software and firmware patching; and
    c. Hardware maintenance.

2. Web-Enabled Applications: VENDOR must implement and manage specialized technical controls for web-enabled applications to ensure that the increased risks associated with web-enabled applications are minimized:
    a. All internets facing websites must be scanned for security vulnerabilities that potentially open the site up to malicious behavior.
    b. SV Microwave's minimum list of validation is the Open Web Application Security Project (OWASP) Top 10 vulnerabilities (e.g., cross-site scripting (XSS), SQL injection, Admin access, open directories, insecure data transfer, etc.).

MEDIA PROTECTION (MP)

VENDOR is expected to protect system media, both hardcopy and digital, by limiting access to authorized users and sanitizing or destroying media so that unauthorized data recovery is technically infeasible.

DATA CLASSIFICATION

1. Security Classification: VENDOR must utilize an information security classification scheme that applies throughout the VENDOR's enterprise.

ASSET & MEDIA HANDLING

1. Asset Management: VENDOR must manage essential information about hardware, software, and data flows/extracts/interfaces (e.g., unique identifiers, version numbers, data recipients, physical locations) in inventory:
    a. SV Microwave will generally inform the VENDOR of the classification of SV Microwave data provided to VENDOR. In the event VENDOR is not certain of the classification of any item of SV Microwave data, VENDOR will seek clarification from its SV Microwave business contact.
    b. An appropriate set of procedures for labeling and handling must be developed and implemented by VENDOR.
    c. Personal use of SV Microwave equipment and data is not allowed.

2. Handling Information: VENDOR must ensure additional protection is provided for handling sensitive material or transferring sensitive information.
    a. Files containing personal information or business sensitive information are transferred (e.g., email, faxes, etc.) via secure/encrypted file transfer protocols;
    b. Sensitive information is encrypted on all devices, including portable devices, such as laptops, portable media (flash drives) and data backups; and
    c. SV Microwave's minimum encryption requirement is 128-bit AES.

RETENTION & SECURE DESTRUCTION

1. Records Retention: VENDOR must maintain a formal records retention program.

2. Secure Destruction: VENDOR must ensure methods of destruction are formally implemented, based on the type of media:
    a. Physical, paper-based media;
    b. Physical, digital media; and
    c. Electronic, digital data.

PHYSICAL & ENVIRONMENTAL PROTECTION (PE)

VENDOR is expected to implement physical access controls to limit access to systems, equipment, and the respective operating environments to authorized individuals. VENDOR shall provide appropriate environmental controls in facilities containing SV Microwave systems.

PHYSICAL PROTECTION MEASURES

1. Facilities: VENDOR must secure facilities where SV Microwave data is stored, processed or transmitted:
    a. The number of entrances to the information processing facilities in which SV Microwave data is stored must be limited.
        i. Every entrance into these areas requires screening. (e.g., security guard, badge reader, electronic lock, a monitored closed caption television (CCTV)).
        ii. Access logs must be recorded and maintained.
    b. Physical access must be restricted to those with a business need.
        i. Access lists must be reviewed and updated at least once per quarter.
    c. Process, training, and policies must be in place to determine visitor access, after-hours access, and prevent tailgating into controlled areas.
    d. Emergency exits in controlled areas must sound an alarm when opened and include automatic closure.
        i. Any alarms must trigger an emergency response.

2. Physical Protection: VENDOR must actively manage the physical security controls and ensure all buildings throughout the VENDOR's enterprise that house critical IT functions (e.g., data centers, network facilities, and key user areas) are physically protected from unauthorized access.

3. Hazard Protection: VENDOR must ensure computer equipment and facilities are protected against natural and man-made hazards.

4. Power Supplies: VENDOR must protect critical computer equipment and facilities against power outages.

PROCESSING FACILITIES

1. Comingling of Data: VENDOR must ensure that when SV Microwave business information is co-located with non-SV Microwave data, (e.g., virtual servers, cloud solutions, etc.) the non-SV Microwave data must at least be logically separated from SV Microwave business information.

2. Physical Location of Data: VENDOR is responsible for notifying SV Microwave before relocating any physical storage location of SV Microwave business information to a country different from the one(s) documented in VENDOR's statement of work or contract so that potential implications for privacy can be addressed.

3. Virtualization & Cloud Solutions: If VENDOR utilizes a cloud solution, VENDOR must adhere to the same security principles required by VENDOR's IT security policies and applicable government regulations, laws, or directives as used throughout vendor's enterprise:
    a. The geographic location of provider infrastructure resources must be made clear to SV Microwave. SV Microwave must be able to control data location in cloud services to ensure compliance with local laws that restrict the cross-border flow of data.
    b. Vendors providing cloud services must:
        i. Provide a process for data destruction and secure deletion of any and all SV Microwave data as needed;
        ii. Have an established method of encrypting sensitive data in storage and in transit following industry-recognized leading practices;
        iii. Securely handle SV Microwave related data, compute resources, virtual machines resources by providing logical isolation and secure migration;
        iv. Include methods or options for multi-factor authentication for cloud administrator roles;
        v. Provide SV Microwave the capability to fully audit SV Microwave user access and activity within the cloud service. Audit logs must be capable of being exported from the cloud service;
        vi. Limit employee access to the least privilege needed to perform their duties.
        vii. Maintain documented audits or established compliance roadmaps in alignment with Industry Standard Certifications for Cloud Security. Examples include ISO27001/2, SSAE16, FEDRAMP, CSA STAR, FIPS 140-2, and Open Data Alliance;
        viii. Demonstrate adherence to Security Development best practices for all code, APIs, and applications deployed and implemented in support of the cloud service;
        ix. Process and advise SV Microwave of any security breach involving SV Microwave data or services utilized by SV Microwave; and
        x. Provide SV Microwave with the means to monitor in near real-time service and resource availability; and
    c. All access to cloud computing sites must encrypt data in transit.
        i. Any SV Microwave data stored in a cloud environment must be encrypted either by the VENDOR or the application so that data cannot be read by other users in a multi-tenant environment.

PLANNING (PL)

VENDOR is expected to develop, document, implement, and periodically update measures to protect its critical systems.

SECURITY COORDINATION

1. Coordinated Security Operations: VENDOR must plan and coordinate security-related activities affecting the information system potentially affected parties before conducting such activities in order to reduce the impact on other business operations.

RULES OF BEHAVIOR

1. Acceptable Use: VENDOR must developing usage policies and define proper use of VENDOR's technologies.

PERSONNEL SECURITY (PS)

VENDOR is expected to ensure that published rules of behavior are followed by users and employ a method of formal sanctions for personnel who fail to comply with IT security policies and standards.

HUMAN RESOURCES SECURITY

1. Security Roles: VENDOR must ensure that all security-related positions are staffed by qualified individuals and those individuals have the skill set necessary to perform the information security-related job functions.

2. Personnel Screening: VENDOR must screen potential personnel prior to hiring in an effort to minimize the risk of compromise from internal sources.

3. Personnel Termination: VENDOR must ensure that upon termination of a VENDOR employee' employment system access accounts are disabled with twenty-four (24) hours of the termination action.

4. Confidentiality Requirements: Non-disclosure agreements must be signed by Vendors prior to being granted access to SV Microwave information.
    a. VENDOR must assess and immediately escalate to SV Microwave about the impact of business information being accidentally or deliberately released to unauthorized parties.
    b. The analysis of integrity requirements must determine how the disclosure of information could have an impact on SV Microwave's business operations with the VENDOR.

RISK ASSESSMENT (RA)

VENDOR is expected to periodically assess the risk to operations, assets, and data, resulting from the operation of systems and the associated processing, storage, or transmission of data.

RISK MANAGEMENT

1. Risk Assessments: VENDOR must perform information risk assessments of critical areas of its business to identify key information risks and determine the controls required to keep those risks within acceptable limits.
    a. Assessments must include, but are not limited to:
        i. Business environments;
        ii. Business processes;
        iii. Business applications (including those under development);
        iv. Computer systems, and
        v. Networks.
    b. VENDOR is required to provide SV Microwave with a documented analysis of how key threats, as identified above in section 1(a), are addressed, as it applies to SV Microwave.

System & Services Acquisition (SA)

VENDOR is expected to allocate sufficient resources to adequately protect organizational systems by employing a System Development Life Cycle (SDLC) process that incorporate IT security considerations.

System Acquisition & Development

1. Supply Chain: VENDOR must ensure that reliable and approved hardware and software are acquired that follows consideration of security requirements. Vigilance must be maintained to prevent counterfeit hardware and software from being used anywhere in the VENDOR's enterprise.

2. Specification of Requirements: VENDOR must take into consideration the information security requirements for the system under development when designing the system to ensure SV Microwave's business requirements (including those for information security) are documented and agreed upon before detailed design commences.

3. Quality Assurance: VENDOR must ensure quality assurance activities are performed for critical security controls during the development lifecycle.

4. Development Methodologies and Environment: VENDOR's development activities must be
    a. Carried out in accordance with a documented system development methodology;
    b. Performed in specialized development environments;
    c. Isolated from production environments; and
    d. Protected against disruption and disclosure of information.

5. System Design / Build: VENDOR must ensure system build activities are:
    a. Carried out in accordance with industry-recognized leading practices (e.g., OWASP);
    b. Performed by individuals provided with adequate skills/tools; and
    c. Inspected to identify unauthorized modifications or changes which may compromise security controls.

6. Installation Process: VENDOR must ensure that newly-promoted systems to the production environment are installed in accordance with the VENDOR's documented installation process.

7. Lifecycle Management: VENDOR must define the End of Life (EOL) process for all systems and applications which could include date of EOL and any business triggers that may result in updated EOL date;

Vendor Management

1. Outsourcing: VENDOR must operate a formal process to address due care and due diligence considerations in the selection and management of third-party VENDORS:
    a. These third-party VENDORS must sign agreements that specify the security requirements to be met before commencing work on behalf of VENDOR that could have an impact on SV Microwave's business operations with the VENDOR;
    b. These security requirements must align with the provisions expected of SV Microwave from VENDOR; and
    c. All subcontracted activities involving SV Microwave information must be approved and secured by VENDOR.

2. VENDOR Exit Strategy: VENDOR must ensure a documented termination of service process is in place that ensures SV Microwave business data is recoverable if must VENDOR terminates a service agreement with a third party VENDOR.

3. Indemnification: VENDOR must address indemnification considerations with third-party VENDORS that could have an impact on SV Microwave's business operations with the VENDOR.

System & Communications Protection (SC)

VENDOR is expected to employ industry-recognized leading practice principles that promote effective IT security within systems and the network.

Communications & Operations Management

1. Communications Security: VENDOR must support standards and procedures that ensure confidentiality, integrity, and availability of information and services with continuous oversight on new threats and vulnerabilities by a documented risk assessment process driving risk mitigation implementation on a timely basis.

2. Operations Management: VENDOR must maintain sufficient overall operational control and visibility into all security aspects of how data is processed, stored and transmitted:
    a. System administrators must have adequate training and experience to securely administer the infrastructure within their responsibility;
    b. Vendor must have a separation of duties process to prevent one individual from controlling all key aspects of a critical transaction or business process; and
    c. Vendors are responsible for data protection, privacy compliance, and security control validation/ certification of their sub-contractors.

Cryptography

1. Cryptography: VENDOR's cryptographic solutions must:
    a. Meet or exceed SV Microwave's minimum encryption requirement of 128-bit AES; and
    b. Protect the confidentiality of sensitive information that is subject to legal and regulatory-related encryption requirements.

2. Cryptographic Key Management: VENDOR must manage cryptographic keys, in accordance with industry-recognized leading practices for key management:
    a. Documented standards and procedures must exist; and
    b. Cryptographic keys must be protected against unauthorized access or destruction to ensure that these keys are not compromised (e.g., through loss, corruption or disclosure).

Network Security

1. Defense In Depth (DiD): VENDOR must secure its computer networks using multiple layers of access controls to protect against unauthorized access. In particular, VENDOR shall:
    a. Group network servers, applications, data, and users into security domains;
    b. Establish appropriate access requirements within and between each security domain; and
    c. Implement appropriate technological controls to meet those access requirements consistently, including (for example) firewalls.

2. Network Controls: VENDOR must ensure that all data and communications networks are secured to ensure the transmission of data is kept confidential.
    a. Applications, ports, services, and similar access points installed on a computer or network facility, which are not specifically required for business functionality, must be disabled or removed;
    b. Network segments connected to the Internet must be protected by a firewall which is configured to secure all devices behind it;
    c. Network segments where SV Microwave data resides should be isolated from non-SV Microwave data, logically or physically unless approved by SV Microwave Security;
    d. User connection capability must be documented with regard to messaging, electronic mail, file transfer, interactive access, and application access;
    e. All production servers must be located in a secure, access controlled location;
    f. Firewalls must be configured properly to address all reasonably-known security concerns;
    g. Infrastructure diagrams, documentation, and configurations must be up to date, controlled and available to assist in issue resolution; and
    h. Systems must have the ability to detect a potential hostile attack. (e.g., IDS/IPS)
        i. All systems must be updated to the current release and actively monitored.

3. Wireless Access: Wireless access must be authorized, authenticated, encrypted and permitted only from approved locations.

4. Remote Access: Remote access to a network containing SV Microwave data must be done via a secure connection (e.g., VPN).
    a. All extranet connectivity into SV Microwave must be through SV Microwave-approved and authorized secure remote connections.

System & Information Integrity (SI)

VENDOR shall correct flaws in its systems in a timely manner and ensure mechanisms are in place to protect systems from malicious code.

Malware Protection

1. Malware Controls: VENDOR must implement and manage enterprise-wide detection, prevention and recovery controls to protect against malware that includes having procedures and assigned responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks.

2. Malware Prevention: VENDOR must ensure the installation and regular update of malware detection and repair software to scan systems and media as a precautionary control, or on a routine basis. The scan carried out should include:
    a. Scan any files received over networks or via any form of storage medium, for malware before use;
    b. Scan electronic mail attachments and downloads for malware before use; and
    c. Scan web pages for malware.

System Configuration

1. Host System Configuration: VENDORS must configure host systems according to an industry standard.
    a. Systems must be configured to function as required and to prevent unauthorized actions.
    b. Examples of best practice configuration include, but are not limited to:
        i. Center for Internet Security (CIS)
        ii. US Department of Defense Secure Technical Implementation Guides (STIGs)
        iii. OEM best practices (e.g., Microsoft, VMware, Oracle, etc.)

2. Mobile Devices: VENDOR must maintain policies, standards, and procedures covering the use of mobile/portable devices.
    a. The use of mobile devices (e.g., smartphone, iPad, tablet, USB memory sticks, external hard disk drives, MP3 players, e-book readers, etc.) must be:
        i. Subject to approval; and
        ii. Access must be restricted.
    b. Controls must be implemented to ensure that sensitive information stored on these devices is protected from unauthorized disclosure.

Privacy - Authority & Purpose (AP)

VENDOR is expected to identify the authority to collect Personally Identifiable Information (PII) and specify the purposes and/or activities for which PII is collected.

Privacy - Accountability, Audit & Risk Management (AR)

VENDOR is expected to implement effective controls to ensure that adequate privacy protection requirements are in place to minimize overall privacy risk.

Privacy - Data Quality & Integrity (DI)

VENDOR is expected to implement controls to ensure Personally Identifiable Information (PII) collected and maintained by is accurate, relevant, timely, and complete for the purpose for which it is to be used.

PRIVACY - DATA MINIMIZATION & RETENTION (DM)

VENDOR is expected to implement data minimization and retention controls applicable to the collection, use, and retention of Personally Identifiable Information (PII) in order to ensure PII is relevant and necessary for the specified purpose for which it was originally collected.

PRIVACY - INDIVIDUAL PARTICIPATION & REDRESS (IP)

VENDOR is expected to enable individual requests about the collection and use of Personally Identifiable Information (PII).

1. Notification of Inquiries: VENDOR must immediately inform SV Microwave, in writing of any:
    a. Request for access to any Personal Information received by VENDOR from an individual who is (or claims to be) the subject of the data, or a request to cease or not begin processing, or to rectify, block, erase or destroy any such Personal Information;
    b. Request for access to any Personal Information received by VENDOR from any government official (including any data protection agency or law enforcement agency), or a request to cease processing, or to rectify, block, erase or destroy any such Personal Information;
    c. Inquiry, claim or complaint regarding the Processing of the Personal Information received by VENDOR;
    d. Other requests with respect to Personal Information received from SV Microwave's employees or other third parties, other than those set forth in the agreement or a request to cease or not begin processing, or to rectify, block, erase or destroy any such Personal Information.

PRIVACY - SECURITY (SE)

VENDOR is expected to implement controls to ensure safeguards are in place to protect Personally Identifiable Information (PII) against loss, unauthorized access, or disclosure.

1. Information Privacy: VENDOR must establish responsibilities for managing information privacy and data security controls for handling sensitive Personally Identifiable Information (sPII).

2. Alignment with SV Microwave Privacy: VENDOR must ensure sPII is collected, used, stored, transferred, and destroyed according to SV Microwave's privacy requirements.

PRIVACY - TRANSPARENCY (TR)

VENDOR is expected to implement methods for disclosing data privacy practices and activities for consumer-related data.

PRIVACY - USE LIMITATION (UL)

VENDOR is expected to implement controls to ensure that the scope of Personally Identifiable Information (PII) use is limited to justifiable business needs.

GLOSSARY: ACRONYMS & DEFINITIONS

ACRONYMS

BCP. Business Continuity Plan
PDCA. Plan-Do-Check-Act
CDE. Cardholder Data Environment
CERT. Computer Emergency Response Team
CIRT. Computer Incident Response Team
DRP. Disaster Recovery Plan
EPHI. Electronic Protected Health Information
IRP. Incident Response Plan
ISMS. Information Security Management System
FACTA. Fair and Accurate Credit Transaction Act
HIPAA. Health Insurance Portability and Accountability Act
NIST. National Institute of Standards and Technology
PCI DSS. Payment Card Industry Data Security Standard
SOX. Sarbanes-Oxley Act

KEY INFORMATION SECURITY TERMINOLOGY

In the realm of IT security terminology, the National Institute of Standards and Technology (NIST) IR 7298, Revision 1, *Glossary of Key Information Security Terms*, is the primary reference document that SV Microwave uses to define common IT security terms.[2] Deviations to terminology from NIST IR 7298 are at the discretion of Corporate IT Security (CIS). Key terminology to be aware of includes:

Asset: Any piece of information of any physical item that can be linked to a SV Microwave business objective in an asset. The loss, disclosure to unauthorized people, or any other compromise of an asset could have a measurable, negative impact on SV Microwave.

Asset Owner: Person who is ultimately accountable for ensuring appropriate classification, handling, and/or controls are in place for the asset. Ownership responsibilities may be formally delegated to another user, but accountability for assets remains with the asset owner.

Asset Custodian / Data Steward: A term describing a person or entity with the responsibility to assure that the assets are properly maintained, to assure that the assets are used for the purposes intended, and assure that information regarding the equipment is properly documented.

Cardholder Data Environment (CDE): A term describing the area of the network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment

Control: A term describing any management, operational, or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help SV Microwave accomplish stated goals or objectives.

Control Objective: A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized leading practice to align SV Microwave with accepted due care requirements.

Data: A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies.

[2] NIST IR 7298 - http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Encryption: A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.

Guidelines: A term describing recommended practices that are based on industry-recognized leading practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.

Information Security: A term that covers the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, and Availability (CIA) of data.

Information System (System): A term describing an asset; a system or network that can be defined, scoped, and managed. Includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls, and mobile devices.

Least Privilege: A term describing the theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.

OTHER INFORMATION SECURITY DEFINITIONS

The National Institute of Standards and Technology (NIST) IR 7298, Revision 1, *Glossary of Key Information Security Terms*, is the approved reference document used to define common IT security terms. [3]

[3] NIST IR 7298 - http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf