VMEC

VERMONT MANUFACTURING EXTENSION CENTER

A System and Communications Policy defines how the data that is transmitted by an information system is protected. This policy is meant to manage and mitigate risks associated with data communication and unauthorized access of transmitted data.

Recommended Actions:

- Identify and document internet connection points
- Utilize firewalls and routers to protect communication at internet connection points
- Encrypt data in transit where possible
- Periodically review and update configuration changes

The following template may be used to help with the creation and implementation of your own policies and procedures.

For more information related to Access Control and other fundamental areas please visit the following link:

CMMC Assessment Guide Level 1

- SC.L1-B.1.X – BOUNDARY PROTECTION

Policy #:	Title:	Effective Date:
	System and Communications Protection Policy	

PURPOSE

To establish guidelines for system and communications protection for Information Technology (IT) resources and information systems.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-53a - System and Communications Protection (SC), NIST SP 800-12, NIST SP 800-28, NIST SP 800-41, NIST SP 800-52, NIST SP 800-56, NIST SP 800-57, NIST SP 800-58, NIST SP 800-77, NIST SP 800-81, NIST SP 800-95, NIST SP 800-100, NIST SP 800-111, NIST SP 800-113; NIST Federal Information Processing Standards (FIPS) 140-2, FIPS 197, FIPS 199

POLICY

This policy is applicable to all departments and users of resources and assets.

1. APPLICATION PARTITIONING
   IT Department shall:

   a. Separate user functionality from information system management functionality either logically or physically.

      Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access.

2. INFORMATION IN SHARED RESOURCES
   IT Department shall:

   a. Prevent unauthorized and unintended information transfer via shared system resources.

      This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems.

3. DENIAL OF SERVICE PROTECTION
   IT Department shall:

a. Ensure that the information system protects against or limit the effects of the following types of denial of service attacks: [entity defined types of denial of service attacks] by employing [entity defined security safeguards].

b. The information system restricts the ability of individuals to launch [entity defined denial of service attacks] against other information systems.

4. BOUNDARY PROTECTION
IT Department shall:

a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system.

b. Implement sub-networks for publicly accessible system components that are [physically; logically] separated from internal organizational networks, and connected to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within security architecture.

5. TRANSMISSION CONFIDENTIALITY AND INTEGRITY
IT Department shall:

a. Deploy information systems that protect the [confidentiality; integrity] of transmitted information.

This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).

6. NETWORK DISCONNECT
IT Department shall:

a. Ensure information systems are configured to terminate the network connection associated with a communications session at the end of the session or after [entity defined time period] of inactivity; this control applies to both internal and external networks.

Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.

7. CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
   IT Department shall:

   a. Establish and manage cryptographic keys for required cryptography employed within the information system in accordance with [entity defined requirements for key generation, distribution, storage, access, and destruction].

8. CRYPTOGRAPHIC PROTECTION
   IT Department shall:

   a. Implement [entity defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal and state laws, directives, policies, regulations, and standards.

      Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals.

9. COLLABORATIVE COMPUTING DEVICES
   IT Department shall:

   a. Prohibit remote activation of collaborative computing devices with the following exceptions: [entity defined exceptions where remote activation is to be allowed]

   b. Provide an explicit indication of use to users physically present at the devices.

      Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

10. PUBLIC KEY INFRASTRUCTURE CERTIFICATES
    IT Department shall:

    a. Issue public key certificates under a [defined certificate policy] or obtain public key certificates from an approved service provider.

b. Manage information system trust stores for all key certificates to ensure only approved trust anchors are in the trust stores.

11. MOBILE CODE
IT Department shall:

a. Define acceptable and unacceptable mobile code and mobile code technologies.

b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

c. Authorize, monitor, and control the use of mobile code within the information system.

Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously.

12. VOICE OVER INTERNET PROTOCOL
IT Department shall:

a. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

b. Authorize, monitor, and control the use of VoIP within the information system.

13. SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
IT Department shall:

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.

14. SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)
IT Department shall:

a. Ensure information systems that requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

   Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers.

15. ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE
IT Department shall:

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

b. Employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server, to eliminate single points of failure and to enhance redundancy.

   Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers.

16. SESSION AUTHENTICITY
IT Department shall:

a. Ensure the information system protects the authenticity of communications sessions.

   This control addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

17. PROTECTION OF INFORMATION AT REST
IT Department shall:

a. Ensure the information system protects the [confidentiality; integrity] of [entity defined information at rest]____.

This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

18. PROCESS ISOLATION
IT Department shall:

a. Ensure the information system maintains a separate execution domain for each executing process.

Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	
Date Reviewed:	