[Insert Company Name and Logo]	
Title: Cataloging External Information Systems	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Information Technology**

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

Scope
This policy applies to all employees and other members of the workforce (whether paid or volunteer) working in all facilities under the organization's ownership.

Definitions: N/A

Procedure

1. The organization is required to establish controls asserted to be implemented on external systems consistent with other organizations owning, operating and/or maintaining external systems, allowing authorized individuals to:
   a. Access the system from external systems; and
   b. Process, store or transmit company-controlled information using external systems; or
   c. Establish, maintain, and update an inventory of all systems, applications, and projects that process sensitive information.

2. Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and verify that the acquisition or outsourcing of dedicated information security services is approved by the Security Officer or company Administrator.
   a. Require that providers of external system services comply with organizational security and privacy requirements.
   b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and
   c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [company-defined processes, methods, and techniques].

3. External systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls or the determination of the effectiveness of implemented controls on those systems. External systems include personally owned systems, components, or devices and privately-owned computing and communications devices resident in commercial or public facilities. This requirement also addresses the use of external systems for the processing, storage, or transmission of sensitive information, including accessing cloud services (e.g., infrastructure as a service, platform as a service,

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

or software as a service) from organizational systems.

4. There are circumstances where individuals using external systems (e.g., contractors, coalition partners) need to access organizational systems. In those situations, organizations need confidence that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been effectively implemented can be achieved by third-party, independent assessments, attestations, or other means, depending on the assurance or confidence level required by organizations.

5. Regarding the protection of sensitive information across an organization, the organization may have systems that process sensitive and others that do not. Among the systems that process sensitive information there are likely access restrictions for such information that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered “external" to that system.

6. Limits on the use of company-controlled portable storage devices in external systems include complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

7. All cloud-based services used by the company’s mobile devices and Bring Your Own Device (BYOD) shall be pre-approved for usage and the storage of company business data.

8. The Security Officer establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

   a. Access the information system from external information systems; and
   b. Process, store, or transmit organization-controlled information using external information systems.

9. External information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems.

10. This organization:

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

a. Requires that providers of external information system services comply with organizational information security requirements and employ company-defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Employs company-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

Violations: Employees who violate these policies may be subject to appropriate disciplinary action up to and including termination as well as both civil and criminal penalties. Non-employees, including 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 according to company policy.

Attachments:

Related Policies: IT Asset Management

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.