






An Acceptable Use Policy outlines how users can interact with an organization's network, websites, and or other technology resources. Just as the name suggests, the policy defines what is considered acceptable behavior when accessing and using an organization's information technology resources. They are meant to protect an organization's digital assets and comply with other legal requirements.

### Recommended Actions:

-  Create a list of rules for using company devices, networks, and email
-  Tell staff not to download random software
-  Prohibit personal use of company systems without permission
-  Educate employees to recognize phishing and social engineering
-  Require administrative sign off

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](#)

- AC.L1-b.1.i – Authorized Access Control [FCI Data]

<b>Information Technology Standard</b>	<b>No:</b>
<b>IT Standard:</b>  <b>Acceptable Use of Information Technology Resources Policy</b>	<b>Updated:</b>
	<b>Issued By:</b>  <b>Owner:</b>

## 1.0 Purpose and Benefits

Appropriate organizational use of information and information technology ("IT") resources and effective security of those resources require the participation and support of the organization's workforce ("users"). Inappropriate use exposes the organization to potential risks including virus attacks, compromise of network systems and services, and legal issues.

## 2.0 Authority

---

## 3.0 Scope

This policy applies to users of any system's information or physical infrastructure regardless of its form or format, created or used to support the organization. It is the user's responsibility to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand the organization's Information Security Policy and its associated standards.

## 4.0 Information Statement

Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of the organization's IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed or captured in any manner, including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of systems used, including but not limited to: all computer files; and all forms of electronic communication (including email, text messaging, instant messaging, telephones, computer systems and other electronic records). In addition to the notice provided in this policy, users may also be notified with

a warning banner text at system entry points where users initially sign on about being monitored and may be reminded that unauthorized use of the organization's IT resources is not permissible.

The organization may impose restrictions, at the discretion of their executive management, on the use of a particular IT resource. For example, the organization may block access to certain websites or services not serving legitimate business purposes or may restrict user ability to attach devices to the organization's IT resources (e.g., personal USB drives, iPods).

Users accessing the organization's applications and IT resources through personal devices must only do so with prior approval or authorization from the organization.

### **Acceptable Use**

All uses of information and information technology resources must comply with organizational policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws including Federal, State, local and intellectual property laws.

Consistent with the foregoing, the acceptable use of information and IT resources encompasses the following duties:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information;
- Protecting organizational information and resources from unauthorized use or disclosure;
- Protecting personal, private, sensitive, or confidential information from unauthorized use or disclosure;
- Observing authorized levels of access and utilizing only approved IT technology devices or services; and
- Immediately report suspected information security incidents or weaknesses to the appropriate manager and the Information Security Officer (ISO)/designated security representative.

### **4.1 Unacceptable Use**

The following list is not intended to be exhaustive but is an attempt to provide a framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions during their authorized job responsibilities, after approval from organizational management, in consultation with organization IT staff (e.g., storage of objectionable material in the context of a disciplinary matter).

Unacceptable use includes, but is not limited to, the following:

- Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information;
- Unauthorized use or disclosure of organization information and resources;
- Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;
- Attempting to represent the organization in matters unrelated to official authorized job duties or responsibilities;
- Connecting unapproved devices to the organization's network or any IT resource;
- Connecting organizational IT resources to unauthorized networks;
- Connecting to any wireless network while physically connected to the organization's wired network;
- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with organizational policies;
- Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (organizations must recognize the inherent risk in using commercial email services as email is often used to distribute malware);
- Using an organization's IT resources to circulate unauthorized solicitations or advertisements for non-organizational purposes including religious, political, or not-for-profit entities;
- Providing unauthorized third parties, including family and friends, access to the organization's IT information, resources or facilities;
- Using organization IT information or resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);
- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using organizational IT resources; and
- Tampering, disengaging, or otherwise circumventing an organization or third-party IT security controls.

## **4.2 Occasional and Incidental Personal Use**

Occasional, incidental and necessary personal use of IT resources is permitted, provided such use: is otherwise consistent with this policy; is limited in amount and

duration; and does not impede the ability of the individual or other users to fulfill the organization's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. Exercising good judgment regarding occasional and incidental personal use is important. Organizations may revoke or limit this privilege at any time.

### **4.3 Individual Accountability**

Individual accountability is required when accessing all IT resources and organization information. Everyone is responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system, and protecting your credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure. Credentials must be treated as confidential information, and must not be disclosed or shared.

### **4.4 Restrictions on Off-Site Transmission and Storage of Information**

Users must not transmit restricted organization, non-public, personal, private, sensitive, or confidential information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct the organization's business unless explicitly authorized. Users must not store restricted organizational, non-public, personal, private, sensitive, or confidential information on a non-organizational issued device, or with a third-party file storage service that has not been approved for such storage by the organization.

Devices that contain organizational information must be attended at all times or physically secured and must not be checked in transportation carrier luggage systems.

### **4.5 User Responsibility for IT Equipment**

Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to the organization and must be immediately returned upon request or at the time an employee is separated from the organization. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the organization. Should IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances surrounding the incident. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. The organization has the discretion to not issue or re-issue IT devices and equipment to users who repeatedly lose or damage IT equipment.

### **4.6 Use of Social Media**

The use of public social media sites to promote organizational activities requires written pre-approval from the Public Information Office (PIO). Approval is at the discretion of the PIO and may be granted upon demonstration of a business need, and a review and approval of service agreement terms by organization's Counsel's Office. Final approval by the PIO should define the scope of the approved activity, including, but not limited to, identifying approved users.

Unless specifically authorized, the use of organizational email addresses on public social media sites is prohibited. In instances where users access social media sites on their own time utilizing personal resources, they must remain sensitive to expectations that they will conduct themselves in a responsible, professional, and secure manner with regard to references to the organization and staff. These expectations are outlined below.

#### **a. Use of Social Media within the Scope of Official Duties**

The PIO, or designee, must review and approve the content of any posting of public information, such as blog comments, tweets, video files, or streams, to social media sites on behalf of the organization. However, PIO approval is not required for postings to public forums for technical support, if participation in such forums is within the scope of the user's official duties, has been previously approved by his or her supervisor, and does not include the posting of any sensitive information, including specifics of the IT infrastructure. In addition, PIO approval is not required for postings to private, organization approved social media collaboration sites (e.g., Yammer). Blanket approvals may be granted, as appropriate.

Accounts used to manage the organization's social media presence are privileged accounts and must be treated as such. These accounts are for official use only and must not be used for personal use. Passwords of privileged accounts must follow information security standards, be unique on each site, and must not be the same as passwords used to access other IT resources.

#### **b. Guidelines for Personal Use of Social Media**

Staff should be sensitive to the fact that information posted on social media sites clearly reflects on the individual and may also reflect on the individual's professional life. Consequently, staff should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the information. It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to retract, as it often lives on in copies, archives, backups, and memory cache.

Users should respect the privacy of the organization's staff and not post any identifying information of any staff without permission (including, but not limited to, names, addresses, photos, videos, email addresses, and phone numbers). Users may be held liable for comments posted on social media sites.

If a personal email, posting, or other electronic message could be construed to be an official communication, a disclaimer is strongly recommended. A disclaimer might be: "The views and opinions expressed are those of the author and do not necessarily reflect those of the organization."

Users should not use their personal social media accounts for official business, unless specifically authorized by the organization. Users are strongly discouraged from using the same passwords in their personal use of social media sites as those

used on organizational devices and IT resources, to prevent unauthorized access to resources if the password is compromised.

## 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

## 6.0 Definitions of Key Terms

Term	Definition

## 7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

\_\_\_\_\_

## 8.0 Revision History

This policy shall be reviewed at least once every year to ensure relevancy.

Date	Description of Change	Reviewer

## 9.0 Related Documents