Frank Cowan Company

Acceptable Use Policy

Instructions

This template will enable you to create an Acceptable Use Policy that meets the needs of your organization.

Acceptable Use Policies (AUPs) are unique. They are generally the only policies that directly affect every person in the organization. They are also the only policies that every employee and every contractor who has access to computing systems should be required to sign.

In the policy requirements section there are a number of statements, not all of which will apply to your organization. These can be freely modified or deleted. The organization must decide what is or is not acceptable use of its computing resources. Sections that refer to illegal acts, or acts for which the organization could be held liable, will likely need to be included in the AUP.

Perform a full document replacement of **<Organization>** with the proper name of your organization. Areas within the template that are required to be reviewed and changed are **highlighted**.

When you have customized the policy to your satisfaction, you can simply delete these instructions and paste the remaining text into your own policy document format. Alternatively, you may modify the footer in this document to suit your organization.

Policy Change Log

Date	Change	Edited by:	Approved by:
	Policy creation		

Table of Content

Purpose of the Policy

The purpose of this policy is to outline the acceptable use of information systems and computing equipment at <Organization>. These rules are in place to protect the employee and <Organization>. Inappropriate use exposes <Organization> to risks including malware attacks, compromise of network systems and services, loss of confidential information, and legal issues.

Scope of the Policy

This policy applies to all <Organization> devices, employees, and contractors. All employees and contractors with access to <Organization> computing devices or information systems shall comply with this policy as it applies to their job duties.

Definitions

Protected Information is information that is highly sensitive and that must be safeguarded in accordance with legislative or regulatory requirements. Protected Information is often subject to privacy breach notification laws, and the loss of this information could have severe consequences for the organization. Examples include Protected Health Information, Payment Card Information and most forms of Personally Identifiable Information (PII).

PII (Personally Identifiable Information) is defined in NIST Special Publication 800-122 as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Confidential Information is information owned by the organization or entrusted to the organization that is not intended for sharing with the public. Security protections must be applied to this information to safeguard its confidentiality, integrity and availability.

Responsibility for Policy Implementation

The<Organization> Security Officer or other authorized representative shall be responsible for ensuring implementation of all items listed in the Policy Requirements section. Responsibility for the creation and implementation of specific procedures may be assigned to internal staff or contractors as appropriate.

Policy Requirements

General and Internet Use

Employees and contractors shall not, under any circumstances, use <Organization> computing devices or information systems to:

1. Engage in any activity that is illegal or violates the rights of any person.
2. Download or install software of any type on <Organization> computing devices without authorization.
3. Copy or distribute any copyrighted material without authorization.
4. Access the personal information of others without authorization, except as part of the employee’s or associate’s assigned duties.
5. Make any claims on behalf of <Organization> unless authorized to do so.
6. Associate <Organization>’s name with any activity that would harm the reputation of the organization.
7. Visit websites exhibiting sexually explicit material, gambling sites or sites related to illegal activities.
8. Visit websites that encourage discrimination or the violation of the rights of any group or individual, except in the course of authorized research.
9. Visit websites which share music or other files on a peer-to-peer basis, or otherwise share content in violation of copyright laws.
10. Engage in any activity that interferes with the ability of another organization or individual to conduct computing activities (e.g. denial of service attacks).
11. Provide information about <Organization> or its employees, clients, customers, patients, or associates to any outside party, unless explicitly authorized to do so.
12. Post comments or other information to social networking sites or blogs on behalf of, or using the name of the organization, unless explicitly authorized to do so.

Personal Internet Use

Activities of a personal nature such as non-business online shopping, access to personal email, job searching and access to personal pages of social networking sites are **[prohibited] or [permitted only during the hours listed below] or [permitted, within the limitations of this policy] or [permitted, subject to the restrictions listed below]**. Work related to accessing official <Organization> information is not personal use of the internet and is an exception.

[Add additional restrictions for Internet use or hours designated for personal Internet use here.]

Online File Sharing, Backup and Synchronization Services

Online file sharing, backup and synchronization services, such as Dropbox, Google Drive, OneDrive, etc. are very convenient ways to store and share files online, but increase the risk that Confidential Information or Protected Information will be inappropriately shared. The following controls must be followed:

1. Protected Information **[and Confidential Information]** must not be copied to or stored on any online file sharing or backup system without specific authorization from the Security officer or other authorized <Organization> representative.
2. Use of online file sharing, backup and synchronization services for information that is not Protected Information is **[prohibited] or [restricted to the following services]**:

[List approved file-sharing services here. You should restrict file sharing to specific services or to one service. Allowing the use of multiple services increases the risk of information leakage.]

Transmission of Protected Information

1. Employees and contractors must not transmit any Protected Information in any email or via any instant messaging or chat service.
2. All Protected Information must be transmitted via a secure file transfer method.

Authorized Storage Locations for Protected Information

All Protected Information shall be processed and stored within the applications authorized by the organization. No employee or contractor may copy any Protected Information to any other location unless directed to do so by an authorized <Organization> representative.

Email Usage

Email is an important communication tool, but also has the potential to cause damage to the organization. Inappropriate use of email can result in the loss of sensitive or company confidential data or intellectual property, damage to public image, damage to critical internal systems, and unintentional employee exposure to inappropriate content or material.

<Organization> employees and contractors must not engage in any of the following:

1. Sending unsolicited email messages, including sending "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Harassment in any form, whether through language, frequency, or size of messages.
3. Creating or forwarding "chain letters" or "Ponzi" or other "pyramid" schemes of any type.
4. Sending similar email messages from multiple email addresses with the intent to harass or elicit replies.
5. Using unsolicited email originating from within the organization's networks or other Internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by the organization.
6. Posting the same or similar non-business-related messages to large numbers of internet posting sites.
7. Unauthorized use, or forging, of email header information.

Downloading or Installing Software

<Organization> employees and contractors may not download or install any software application without the authorization of an authorized company representative.

Social Media

Social media sites are places on the internet where people can share information, interact and communicate with each other (e.g. Facebook, LinkedIn, and Twitter). Social media can be a valuable tool for the promotion of the organization, its goals, and its values. It can also be used as a means of sharing valuable information for the purpose of helping others improve security and reduce risk. However, messages posted to social media sites must be carefully considered, because once posted, these messages cannot be recalled or removed easily, if at all.

No employee or contractor shall post to any social media site on behalf of the organization or purport to represent the organization in any way, without authorization.

All employees and contractors who are authorized to post to social media sites on behalf of the organization must adhere to the following standards:

1. Be respectful of the organization, as well as its employees, associates, and competitors. Do not post derogatory, malicious, demeaning, insulting or inflammatory comments about anyone or any organization.
2. Use the first person (I, not we) and always appropriately identify yourself.
3. Be accurate.
4. Cite source material. If you have obtained information from an online or other resource, cite the source. If possible, cite the original source. If you are stating an opinion, rather than a fact, make sure this is clearly represented.
5. Clearly state that your opinions are your own, and that they are not the official opinions of <Organization>.
6. Do not use profanity, ethnic slurs or abusive language.
7. If you make an error regarding facts, post a correction or retraction as soon as possible.
8. Protect confidential and proprietary information. Do not identify coworkers, clients, business partners or suppliers without permission.
9. Do not use copyrights, trademarks, or logos without permission.
10. Be professional. Any blog or social media posting that mentions or can be associated with <Organization> becomes a part of the organization's public image. Restrict your comments to those subjects about which you have knowledge. Make sure your posts are making a positive contribution to both the organization's image and to your personal image as an employee or contractor.

Remote Access and Personal Wireless Networks

1. No employee or contractor is permitted to install any wireless networking device that connects to the organization's systems without authorization from the IT administrator, or other appropriate party.
2. No employee or contractor may install any software or application that allows access to the organization's systems from a remote location without appropriate authorization from <Organization>.

Reporting Security Incidents

1. All employees and contractors must report the following as security incidents to the Security Officer or another authorized <Organization> representative:
   a. Any observed unauthorized disclosure of Protected Information or Confidential Information, whether intentional or unintentional.
   b. Any observed attempt to view or access Protected Information or Confidential Information beyond by a person not authorized to view or access that information.
   c. Any unauthorized attempt to gain physical access to, or install unauthorized software applications on, any server or workstation.
   d. Any telephone, email, or other communication that include an unauthorized attempt to receive or access Protected Information or Confidential Information.
   e. Any unusual computer behavior (unusual error messages, unusual pop-up windows, website redirection, etc.). When unusual computer activity is observed, the computer should not be turned off to preserve valuable evidence. The Security Officer or other authorized <Organization> representative should be contacted immediately.

Protecting the Organization from Cyber Threats

1. Phishing and “social engineering” attacks: Sooner or later you will be the target of an attempt to trick you into disclosing Protected Information or Confidential Information or installing malicious software on <Organization> systems. Be aware that social engineers often conduct extensive research in preparation for their attacks and may present you with names, events, or other information that you would not expect to be known to anyone outside your organization. Be aware of the following considerations:
   a. Exercise caution with email attachments and links in email messages. If the message is unexpected or if you have any doubt about whether it is genuine, contact the sender. Do not reply to the email. Contact the sender using contact information you have previously recorded.
   b. Be suspicious if anyone asks you for a password, account information, or other confidential information. Phishing email messages can be made to look exactly like legitimate messages you have received in the past.
   c. Never send Protected Information or Confidential Information, enter passwords, or provide account information over an insecure connection. A secure connection will always start with https:// in the browser address bar.
   d. Do not click on banner ads or the ads along the top, sides, or bottoms of web pages. These ads are designed to be tempting, but some may link to malicious websites.
   e. Understand that you will be targeted by cyber-criminals and that they want to steal confidential information from all businesses, both large and small. Be constantly vigilant

Acknowledgment

I have read, understand, and agree to abide by, this <Organization> Acceptable Use Policy:

____ Date________________