Sample Organization Acceptable Use Policy

Establishment date, effective date, and revision procedure

This policy was established and approved by [*Organization Name*] on mm,dd,yyyy. The [*Organization Name*] Information Security department of shall review this policy at least once a year, and at any additional time when there are changes that may affect corporate management with respect to Information Security. In the event that amendment or repeal of this policy becomes necessary as a result of such review, the [*Organization Name*] Information Security department shall prepare a draft and apply for authorization, and with prior confirmation of the Corporate Executive(s) in charge of the area(s) that will be affected by amendment or repeal, the [*Organization Name*] CISO/Security Director will authorize the amendment or repeal.

Table of revision history

Version	Date	Details of change	Issued by	Approved by

Introduction

Purpose

This policy describes the acceptable use of [*Organization Name*] computer equipment.

Scope

This policy applies to all users of information technology within the [*Organization Name*].

Policy

Employees are responsible for exercising good judgment regarding reasonable personal use.

Physical security

- Employees are required to safeguard all [*Organization Name*] equipment assigned to their exclusive or shared use, and all [*Organization Name*] equipment within their work area.
- Employees traveling with laptop computers will always carry them in carry-on baggage and not in checked baggage.

Information security

- Data created on [*Organization Name*] systems remains [*Organization Name*]'s property. The organization cannot guarantee the confidentiality of information stored on any network device.
- Any information considered sensitive or vulnerable must be encrypted.
- For security and network maintenance purposes, individuals authorized by the IT Manager may monitor equipment, systems, and network traffic at any time.
- Secure all PCs, laptops, and workstations with a password-protected screensaver with the automatic activation feature set at 10 minutes.

Self-help

All users of [*Organization Name*] equipment are expected to take charge of their own training:

- Attend in-house classes provided by the IT department.
- Review and become familiar with software documentation.

Unacceptable use

- Employees are never authorized to disable the anti-virus software on their workstation.
- Hacking systems and databases or acting to disrupt systems or cause unnecessary network congestion or application delays.
- Use of remote control software on any internal or external host personal computers or systems not specifically set up by the IT staff.
- Any use of computer equipment that violates state or U.S. law and regulations.
- Creating or forwarding of chain mail regardless of content, sources, or destinations. Posting [*Organization Name*] information to external newsgroups, bulletin boards, or other public forums without authority.
- Using [*Organization Name*] equipment for personal profit, political fundraising, gambling activity, non-business-related instant messaging or chat room discussions, and downloading or display of offensive material.