EC Murphy Walsh

White Paper:

Information Technology Acceptable Use Policies

A practical guide for protecting IT assets from the largest single IT Security threat – inappropriate use of IT services, including desktops, email, internet, and business applications. You will learn why Acceptable Use Policies are important and what specific guidelines are needed in each area.

Prepared by:
M. Brian Yale
Principal
EC Murphy Walsh
byale@ecmurphywalsh.com

Information Technology Acceptable Use Policies

Introduction

Your company needs a safe, secure computing environment. Unfortunately, this is a daunting task for all but the smallest of enterprises. There are many threats and vulnerabilities to consider. Computer viruses and worms, spyware, spam attacks, hackers, disgruntled employees, failed hardware, unlicensed software and software malfunctions all can disrupt IT services and compromise confidentiality and privacy of information.

Businesses need a comprehensive IT Security Policy backed up with enforcement and compliance controls to address these issues. The stakes are high. Inadvertent release of customer records or patient records has serious liability consequences for your business. Increased government regulations require publicly held companies to meet stringent IT control standards. In the United States, Sarbanes Oxley governance controls extend to IT with the CoBIT controls regulations. US health care regulations – HIPPA and FERPA – are very specific and require the implementation of comprehensive patient privacy controls and protection. Many states and provinces have implemented additional controls and remedies, particularly for the theft or exposure of customer credit card information.

Acceptable Use Policies play an important role. Because 85% of all IT Security issues are caused by internal employees, your business needs to make the implementation and enforcement of Acceptable Use Policies a priority. This provides several business benefits:

- You establish a clear definition of what is and is not acceptable. This is important for regulatory compliance and for progressive discipline of employees that violate policies.
- You will have fewer IT service disruptions.
- You will realize productivity gains by eliminating inappropriate use activities.
- Your IT staff will be more effective as they will not need to deal with the consequences of inappropriate use.
- Your written acceptable use polices and your compliance efforts will limit your exposure to litigation. For example, you may not be able to prevent an employee from secretly installing unlicensed software on their desktop, but you have written policies that forbid this practice. Without a policy in place, there is little defense to issues of hostile work environment, privacy breaches and theft of company information.

Every business will have unique usage issues and concerns, so the policies in this document are just a starting point. Categories of Acceptable Use are:

- Desktops and Laptops
- Internet
- Email
- Business Applications

Policies are an important first step, but they do not assure success. You'll need compliance and enforcement initiatives as well. Emerging technology solutions can really help. For example, Spam filters, Internet Access controls and automated asset tracking tools all can be employed to detect and prevent policy violations.

Acceptable Use Policy – Desktops and Laptops

This policy defines end-user acceptable use of company IT equipment. The policy applies to desktops, laptops, printers and other equipment provided by the company. Anyone that uses company equipment ("Users"), including employees, vendors, contractors and visitors, must adhere to this policy. Acceptable use applies to proper care and maintenance of equipment as well as following documented security policies relating to equipment use.

1. User Responsibilities

Users shall use company provided IT equipment responsibly and for company business purposes only. Appropriate use policies are –

- Active desktops and laptops may not to be left unattended for prolonged periods of time. Users should secure their workstation when leaving the workstation unattended.
- Company information displayed on screens or on reports shall be treated as confidential and private. Users must guard company information from unauthorized access or use. Any employee-signed confidentiality agreement shall fully apply to information accessed with company IT equipment.
- Managers are responsible to ensure that their employees are adequately trained on appropriate use of IT equipment and that they adhere to this policy.
- Users may not grant access to non-employees, including vendors or contactors, without approval of their manager or approval by the IT Department.
- Users shall keep their equipment clean and free from dust. Users shall maintain "breathing space" around equipment in accordance with equipment installation instructions.
- Users shall not eat or drink at their workstation.
- Desktop acceptable use policies apply equally to portable devices, including laptops, notebooks, PDA's and Smartphones.
- All acceptable use polices apply equally to non-company provided equipment if the equipment accesses company information or company networks.
- Users who access company information and computer systems from remote locations must adhere to this policy.
- Non-company provided equipment shall be kept in a secure manner so that the employee's household members and others do not have access to the device when not in the office.
- Users should not store company information or files locally. The use of shared or network drives for all company information is required.
- Users are responsible for backing up files stored on their desktop or laptop. The company does not provide backups at the desktop level.

2. Prohibited Practices

Any activity, action or lack of action on the part of a user that damages the company or compromises security or confidentiality is prohibited. Examples of prohibited practices include:

- Installing new desktops or equipment without prior approval by the IT Department.
- Upgrading equipment or adding peripheral equipment without the prior approval of the IT Department.
- Downloading and/or installing programs that are not specifically approved by the IT Department.
- Using unlicensed software. Users may not copy and share software that is installed on their desktops or laptops with other users.
- Using programs or Internet web sites that compromise the privacy of customers or employees.
- Removing or compromising desktop virus protection programs.
- Opening email attachments that are inappropriate or from someone you do not know.
- Using company provided IT equipment for non-business reasons or for personal gain.
- Unauthorized attempts to break into any workstation.
- Unauthorized access to company files, programs, databases or confidential information.
- Sending or posting confidential files to unauthorized persons.
- Failing to fully cooperate with IT security investigations.
- Allowing co-workers or other users to use your desktop without approval of your manager or by the IT Department.
- Sharing password information or displaying it in plain view on or around your desktop. Users must secure their passwords and not reveal them to others.

3. Compliance

The IT Department will monitor and report violations of all acceptable use policies. This will be done through a combination of remote monitoring and on-site visits. Whenever an IT professional is on-site at a branch or corporate location, he or she should test compliance levels at the individual desktop level.

Users that violate this policy will be disciplined and may be terminated for serious or multiple violations.

Acceptable Use Policy – Email

This policy defines end-user acceptable use of company provided email services. This policy applies equally to on-site usage as well as remote usage of company email.

When using company email, users shall follow these guidelines:

1. User Responsibilities

- Email users shall use email in accordance with general communications policies of the company.
- Company provided email generally shall be used for business communications only. Users may use company email for personal communication as authorized by their company department manager.
- Users understand and agree that they shall not have a right to privacy when using company email or company assets for electronic communications, even if those communications are of a personal nature.

2. Prohibited Practices

- Users should not open emails or email attachments from persons unknown to them. Opening of unknown or suspicious attachments can have serious consequences for the company in terms of viruses or computer worms. Users should contact the IT Department if there is even a slight concern about an email attachment.
- Users should not respond to spam emails or unsolicited advertisements. Responding will multiply the amount of spam received. Unsolicited emails should be deleted or reported to the IT Department.
- Users may not send large amounts of data or attachments through email.
- Users may not use email to solicit employees for any purpose, including charitable purposes, without the written approval of their department manager.
- Users may not forward or promote spam or joke emails, and particularly may not send spam or joke emails to group email addresses.
- Users may not use email for purposes that violate legal or company policies regarding gambling, hate, pornography or other inappropriate purposes.

3. Compliance

The IT Department will monitor and report violations of all acceptable use policies. The company has the right to monitor email usage and individual emails at its sole discretion. Users should report inappropriate emails or policy violations to the IT Department immediately

Users that violate this policy will be disciplined and may be terminated for serious or multiple violations.

Acceptable Use Policy – Internet

This policy defines end-user acceptable use of company provided Internet access. This policy applies equally to non-company provided Internet access made while on company premises.

When using Internet, users shall follow these guidelines:

1. User Responsibilities

- Company provided Internet access generally shall be used for business purposes only. Users may use Internet for personal reasons as authorized by their company Department manager.
- Users shall install and use anti-virus and anti-spyware software under the direction of the IT Department. Weekly or monthly desktop. scanning is normally required to eradicate spyware and latent viruses.
- Users understand and agree that they shall not have a right to privacy when using Internet on company provided equipment.
- Users understand and agree that the company may severely limit access, including the use of controls that prevent access to sites deemed inappropriate by the company. The company has the right to monitor and control internet usage at its sole discretion.

2. Prohibited Practices

When using internet, users must follow these guidelines:

- Users should not download software or images unless they are from a trusted source, and then only if authorized by the IT Department. Opening of unknown or suspicious programs or images can have serious consequences for the company in terms of viruses or computer worms. Users should contact the IT Department before they download any files from the internet.
- Users should not provide their email address when registering at a web site unless the web site has a clear policy that they will protect email privacy.
- Users should not use the Internet for on-line radio or television access without permission from the IT department. Sites that provide streaming content have a significant impact on network resources and impact network performance and responsiveness.
- Users may not use internet for purposes that violate legal or company policies regarding gambling, hate, pornography or other inappropriate purposes.

3. Compliance

The IT Department will monitor and report violations of all acceptable use policies. The company has the right to monitor internet usage at its sole discretion. Users should report inappropriate internet usage to the IT Department immediately

Users that violate this policy will be disciplined and may be terminated for serious or multiple violations.

Acceptable Use Policy – Business Applications

This policy defines end-user acceptable use of company business application software. This policy applies to all software identified by the company as a business application. General Accounting software, Customer Relationship Management, Patient Records and Inventory Control are examples of business applications. Anyone that uses company business applications (“Users”), including employees, vendors, contractors and visitors, must adhere to this policy.

1. User Responsibilities

Users shall use company provided application software responsibly and for company business purposes only. Appropriate use policies are –

- All IT Infrastructure Acceptable Use Policies fully apply to application software usage. This includes the requirement that active desktops and laptops may not to be left unattended for prolonged periods of time. Users should secure their workstation when leaving the workstation unattended.
- Company information display on equipment or on reports shall be treated as confidential and private. Users must guard company information from unauthorized access or use. Any employee-signed confidentiality agreement shall fully apply to information accessed with company IT Equipment.
- Managers are responsible to ensure that their employees are adequately trained on appropriate use of company software applications and that they adhere to this policy.
- Managers are responsible to assure that users have adequate access to applications, but do not have access that is inappropriate for their job function or otherwise represents an unnecessary security risk for the company.
- Users may not grant access to non-employees, including vendors or contactors, without approval of their manager or approval by the IT Department.
- Users who access company information and computer systems from remote locations must adhere to this policy.
- Users should promptly report software problems or apparent defects to their manager. Managers should work with the company software primary contact to determine if the issue is software related, and if so, how best to have it fixed.

2. Prohibited Practices

Any activity, action or lack of action on the part of a user that damages the company or compromises security or confidentiality is prohibited. Examples of prohibited practices include:

- Installing new software applications without prior approval by the IT Department. This includes downloading software from the Internet, even if there is no charge for the software. Downloading applications for evaluation purposes is also prohibited unless approved in advance by the IT Department.

- Sharing passwords with other users. Users shall not post or display their passwords where they can be seen by others.
- Attempting to access applications without approval. Employees shall not attempt to gain access or hack into an application that they are not authorized to access.
- Using unlicensed software. Users may not copy and share software that is installed on their desktops or laptops with other users.
- Using programs or Internet web sites that compromise the privacy of customers, patients or employees.
- Unauthorized access to company files, programs, databases or confidential information.
- Sending or posting confidential files to unauthorized persons.
- Failing to fully cooperate with IT security investigations.

3. Compliance

The IT Department will monitor and report violations of all acceptable use policies. This will be done through a combination of remote monitoring and on-site visits. Whenever an IT professional is on-site at a branch or corporate location, he or she should test compliance levels with this policy.

Users that violate this policy will be disciplined and may be terminated for serious or multiple violations.