it squared™

IT Policy & Security

Starter Kit

Introduction

As the technology department for our customers, IT Squared strives to add value in all aspects of their business, including helping structure polices and sharing best practices. These materials were developed to provide sample IT policies, security guidelines and other tools that your organization can use as a starting point when managing your IT. All policy information provided is of a general nature; you should work with your Human Resources and Legal Departments when creating your own policies. We hope these documents are useful in helping your small business or non-profit begin thinking about how to structure policies and procedures which are appropriate to your organization. *

Sample Policies

Employee Conduct

Every employee is expected to act in a professional, responsible, and courteous manner at all times. Clearly, such behavior fosters a positive and productive working environment. Conversely, inappropriate or unprofessional behavior is disruptive and unproductive. Moreover, inappropriate conduct is cause for discipline, up to and including immediate termination. It is impossible for [COMPANY] to identify all standards of conduct that are unacceptable. Again, [COMPANY] demands that employees act in a professional and courteous manner. We expect that employees will use common sense and good judgment in achieving this goal. However, [COMPANY'S] judgment, and not that of any individual employee, is the benchmark for what is acceptable and what is not. An employee's conduct is not made acceptable solely because the employee believes it to be. Nor may an employee excuse his or her conduct because this manual does not specifically prohibit the objectionable conduct. The company expects that employees recognize that inappropriate conduct, from rudeness to theft, is unacceptable. The decision as to what is inappropriate is left in [COMPANY'S] hands and sole discretion.

Property Rights

All records, files, messages, contacts, data resource materials, supplies or equipment made by a [COMPANY] employee within the scope of his/her employment with [COMPANY] shall be and remain the sole and exclusive property of [COMPANY], and may not be removed without permission of the [specify official].

Email, Internet

[COMPANY] provides employees with a host of electronic technologies and services, including computers, email, voicemail and Internet services. These technologies and services are intended to be

used for business purposes only and are meant to assist employees in completing job responsibilities as effectively as possible. Personal use of these technologies and services is prohibited. It is imperative that employees not abuse or misuse these technologies and services. Employees must ensure that only business-related information is contained or maintained on the [COMPANY's] systems or devices. This is particularly important when using email, the World Wide Web, or any other part of the Internet. At minimum, employees must be guided by common sense when using the computer technologies. Given the ever-changing nature of these technologies, it is impossible to catalogue all possible abuse or misuse. Nevertheless, employees are strictly prohibited from using any technology to view, listen to or communicate offensive, defamatory or disruptive content. Such content includes, but is not limited to, material of a sexual or sexually suggestive nature, racial, ethnic or gender-specific slurs, or any other visual/audio/verbal content that offends or is intended to offend someone because of his or her age, sex, religion, national origin, disability or other lawfully protected trait. The use of passwords does not imply any privacy. The systems administrator can override personal passwords. Employees shall not disclose their codes or passwords to others. All passwords and all software used to encrypt email are considered company property. Employees may not use personal encryption software for email sent via company facilities. The [COMPANY] will periodically audit its systems, including email and Internet access, to determine whether there is evidence of abuse or misuse. Employees who abuse or misuse any [COMPANY] technology will be disciplined, up to and including immediate termination.

External Chat Sites, Blogs, Bulletin Boards and Newsgroups

Users are prohibited from using company systems to post information to or otherwise communicate in external chat sites, blogs, electronic bulletin boards, newsgroups, or other similar services. Further, when accessing or using any of these services through non-company systems (e.g., home computers), users are prohibited from referencing or identifying [COMPANY] (including as their employer) or disclosing any information (including proprietary information) learned, created or developed in the course of their relationship with the [COMPANY], or otherwise posting information, including about [COMPANY] employees or clients, in a manner that is inconsistent with [COMPANY] policies (e.g., discriminatory, harassing, defamatory or other inappropriate comments).

Instant Messaging

All communications, including instant messages, that are transmitted, received, or stored on company facilities (e.g., computer, modem, software, network, telephone lines, Internet service provider) are the sole property of the [COMPANY]. Accordingly, the [COMPANY] may access, store, and monitor employee instant messages. The use of passwords does not imply any privacy. The systems administrator can override personal passwords. Employees shall not disclose their codes or passwords to others. All passwords and all software used to encrypt instant messages are considered company property. Employees may not use personal encryption software for instant messages sent via company facilities.

All instant messages are captured by system software and are subject to review by management. The [COMPANY] reserves the right to disclose the content of instant messages to third parties without notice to employees.

Telecommuting

[COMPANY] is committed to creating a work environment where the needs of our customers, employees, and the [COMPANY] are balanced. Therefore, the [COMPANY] tries to be flexible in its approach to work styles and location. Telecommuting arrangements may be made on an “as needed basis” or set up on a regular schedule. In either case, employees are encouraged to spend time working in the office whenever possible. This allows employees to be accessible to customers and creates a sense of consistency and collaboration among work teams. When employees desire to work at home, the [COMPANY] asks that they do so in a manner which is in keeping with a work style of accessibility, communication, and productivity. All telecommuting arrangements are subject to approval by the employee’s manager. In general, the following principles should be used in telecommuting:

- Employees should make arrangements with their manager at least one week in advance of telecommuting.
- Employees should check in with the office regularly.
- Employees should inform their manager of their whereabouts so they may be reached easily.
- Working at home means working, not taking time off.
- Employees should not routinely work at home on days prior to or following vacations or holidays if at all avoidable.
- Under regular circumstances, telecommuting should not comprise more than one day in a given week, or more than three days a month.

Software Downloading

All software transmitted over or used in connection with the [COMPANY’s] systems must be approved by and registered to the [COMPANY]. Individuals are prohibited from installing, downloading or transmitting software. If a software application you require is not available on your desktop, do not download or install it; contact the Sinu Support team. Due to the requirements of their job, personnel whose job responsibility includes the development, testing, evaluation, integration, deployment, or maintenance of software may require an exception to this policy. It is possible that non-certified software will be incompatible with company-approved software, and in some cases such software may interfere with or even disable other software applications. Approval is also required to ensure that the [COMPANY] has all licenses necessary to authorize your use of the software. In addition, downloading software from the Internet and other external sources increases the risk that computer viruses and malicious software will be introduced into the company’s systems. Installing, downloading or using non-certified software may also subject the [COMPANY] and the individual to contractual obligations and legal risk.

Failure to comply with this policy may subject individuals to disciplinary action by the [COMPANY] up to and including termination. In addition, conduct that is unlawful may subject individuals to civil, and in some cases criminal, liability.

Password Security

Passwords are the first line of defense in the protection of information assets contained in the [COMPANY's] systems. All individuals are responsible for taking appropriate steps to select and maintain the security of their passwords.

- Individuals must not disclose their passwords to anyone, whether inside or outside the [COMPANY]. If, on occasion, individuals are required to share their password with other staff, they must change their password once the task is completed.
- Passwords must be constructed according to the [COMPANY's] established complexity standards. Good passwords include a mixture of upper- and lower-case letters, numbers and symbols. They should be at least seven characters long and should not include any English dictionary words.
- Passwords should be changed at least once every 90 days.
- It is recommended that individuals not select the same password to access [COMPANY] systems that they have selected for accessing systems not hosted by the [COMPANY] (including, but not limited to, personal on-line banking services, market data services, personal email accounts, etc).
- Failure to comply may subject individuals to disciplinary action by the [COMPANY] up to and including termination. In addition, conduct that is unlawful may subject individuals to civil, and in some cases criminal, liability.

SECURITY

Security Priorities

IT Squared recommends that organizations approach security practices in order of priority. Listed below are several priorities for consideration in order to begin a conversation about security.

First Priority

- Perimeter (email) spam and virus protection
- Intrusion prevention (firewall)
- Wireless security
- Data protection policy (local and remote backup)
- Server and workstation antivirus protection (viruses)
- Inventory of hardware assets
- Annual risk assessment

Second Priority

- Physical Network Security – locked, climate controlled space
- Web traffic filtering (for malware)
- Password policy
- Permission review
- Legal compliance review
- Business continuity management

Third Priority

- Email encryption
- Email compliance policy and practice
- Laptop recovery software

Information Security

- Information security is the set of business processes and policies that protects information. Information security typically involves both physical and digital security measures to protect data from unauthorized access, use, replication or destruction, and often includes:
- Analysis of the organization's information security risks

- Security policy
- Asset management: inventory and classification of information assets
- Human resources security: security aspects for employees joining, moving, and leaving
- Physical and environmental security: protection of the computer facilities
- Access control: restriction of access rights to networks, systems, applications, functions, and data
- Information systems acquisition, development, and maintenance: building security into applications
- Information security incident management
- Business continuity management: protecting, maintaining, and recovering business-critical systems
- Compliance: ensuring conformance with information security policies, standards, and laws

Laptop Security

Many bad things can happen to a laptop: it can be dropped, knocked into the pool, coffee spilled on it, etc. While it's hard to prevent these kinds of accidents, you can take steps to prevent laptop theft and critical data loss.

Tips to Preventing Laptop Theft

- Always carry your laptop with you.
- Lock your laptop to your desk when in the office, or keep it out of sight. Targus (http://www.targus.com/us/) makes simple cable locks.
- If left in your car, never leave your laptop in plain sight.
- Choose an inconspicuous carrying case.
- Never leave access numbers or passwords in your carrying case.
- Label and tag the laptop and all its accessories.
- Don't leave your laptop in your hotel room or with the front desk.

Preventing Data Loss

No critical data should ever be kept on your laptop. Critical data should always be stored on a server that is backed up. Backup services for laptops are available for a nominal monthly cost. If you do have critical data on your laptop, encrypt it.

Laptop Recovery Services

LoJack for Laptops (http://www.lojackforlaptops.com) is a recovery service that helps law enforcement recover stolen laptops. If your laptop has this service and is stolen, LoJack silently and securely contacts

our monitoring center and reports its location. Other recovery services include zTrace, CyberAngel, and Absolute Software ComputracePlus.

If Laptop is Lost or Stolen

1. Choose secure new passwords for each of your Internet accounts (online banking, online trading, vendors, etc.).
2. Change your password for each of your personal email accounts.
3. Change your network password to help secure access to corporate servers.
4. Report the theft to local authorities, such as the police, and to your IT department.
5. If customer data was on the laptop, contact your account representative, legal representative, or appropriate person at your company so he or she can take the appropriate legal actions.

OTHER IT TOOLS

Relocation Checklist

This section contains IT requirements that must be addressed when your organization moves to a new location.

Connectivity

1. Gather requirements
2. Identify vendors

Phone System

1. Gather requirements
2. Identify vendors

Cabling Infrastructure

1. Determine the appropriate cabling layout for floor plan
2. Order cabling

Network Infrastructure

1. Create network map
2. Determine hardware requirements: firewall, switches, patch panel, etc.
3. Spec appropriate rack and location for gear

Power

1. Verify that you have appropriate power at the server rack
2. Create battery backup plan

Servers

1. Create move and set up plan for servers
2. Set up servers and test them

Workstations

1. Create move plan for workstations
2. Create setup plan for workstations at new location

Peripherals

1. Determine locations for peripherals
2. Confirm cabling and power for peripherals

Move Schedule

The following schedule indicates when you should implement various tasks in the weeks prior and the weeks following your move.

Date	Task
10 Weeks Prior	Order cabling
9 Weeks Prior	Finalize contract with phone and ISP vendors
8 Weeks Prior	Determine network topology, and finalise hardware
7 Weeks Prior	Order any new required hardware
6 Weeks Prior	Finalise hardware move plan
2 Weeks Prior	Test connectivity
Move Date	Move and set up servers, peripherals and workstations
Week After	Troubleshoot transitional issues

Home IT Guidelines

The information provided in this section is provided to help you avoid home computer problems caused by data loss, spam, and spyware.

Email

The free email offered by your Internet service provider is often loaded with spam and has backup and remote access limitations. Instead, choose an email account from Google, Yahoo or Microsoft Outlook. Your email is backed up daily, filtered for spam, and available anywhere you can access the Internet. Set up an auto reply from your old email address for a month to notify your contacts about your email address change.

Internet Connectivity

Check with your Internet service provider for available speed upgrades. You should be able to get high speed access for that's relatively inexpensive. Look into bundled packages from your cable vendor or telephone provider.

Backup

Hard drives do fail and if you do not perform a regular backup, you could lose all of your data. Consider one of the following services to automate your backup and protect your data:

- Mozy (www.mozy.com)
- Carbonite (www.carbonite.com)
- Crashplan (www.crashplan.com)
- Backblaze (www.backblaze.com)

You might also consider an external hard drive to back up your data; several options are available from a wide variety of manufacturers including Lacie, Western Digital, and Seagate.

Anti-Virus Software

You need to protect your computer against viruses. There is a free anti-virus software from AVG (www.avg.com) available which we have found to be effective. If you decide to use AVG, be sure to uninstall any existing anti-virus software before installing AVG software. Run a full scan of your machine after installing the software and configure AVG to run full weekly scans of your machine.