**Boilerplate**

**Purpose**

* This is a “template” Acceptable Use Policy to be used as a “starting point\*” for the sake of helping you develop your own Awareness Program. \*It may not be all-inclusive.

**Copyright / Permission to Use**

* Permission to use this document is implicit in your downloading it directly from the infotex small business resources web page.
* By using this template either in its entirety or any portion thereof, you acknowledge that you agree to the terms of use as dictated in the “Transfer of Copyright Agreement” located at copyright.**infotex**.com. This agreement establishes that when you customize this template to your specific needs, your organization may have copyright of the customized document. However, **infotex** retains copyright to the template. This agreement also establishes that you will not share this or any other template with third parties other than auditors and examiners. You may not transfer ownership of the customized documents to any other organization without the express written permission of **infotex**.

**Instructions**

* Make sure to read through the template carefully as not all situations will pertain to your organization. However, to assist you in customizing the document to your specific needs, we have attempted to color code areas that will need your special attention. Color coding is as follows:
	1. All areas needing customization and/or consideration are in **red**.
	2. Sections that are in **brown** are optional sections according to our definition of best practices. These sections may be removed if they do not match your needs.
	3. Sections in **blue** are merely instructions or additional information for knowledge purposes and should be removed.
	4. Sections in **green** are examples and can be left in if need be.
* Note that you should confirm that all text has been changed to “black” before considering this template final for your organization. If there are any sections in any other color than black, then all situations or customization has not been considered.
* This section (Templates) may be removed once the document has been customized, for at that time we turn ownership of the customized document over to you.

© Copyright 2000 - 2017 **infotex**, Inc. All rights reserved.

**Iterations:**

Date of original iteration: June 2000

**Insert Business Name / Logo**

Acceptable Use Policy

(Approved During DD/MM/YY Board Meeting)

Classified: Internal Use

Contact if found: Name, Title
Business Name
City, State

## **Policy Scope**

This policy applies to all Business Name’s employees, temporary workers, contractors, and consultants who use or modify the organization’s information system.

The Owners is responsible for overseeing the development, implementation, and maintenance of this policy. It should be reviewed at least annually to ensure relevant information is appropriately considered.

[Senior Management / Owner] is responsible for enforcing this policy.

For questions concerning this policy, see [Senior Management / Owner].

## **General Use**

Determine whether you want to completely prohibit personal use or define good judgment. The first approach exposes the business to legal risk. Choose one, thendelete the other.

Business Name prohibits the use of company resources for personal reasons during normal business hours.

Or:

The computing resources of Business Name are to be used predominately for business purposes. Limited personal use of Business Name’s resources during business hours is allowed with good judgment. Security Awareness Training addresses what Business Name means by “good judgment.” Resources may not be removed from Business Name’s premises unless the involved person has first obtained proper authority from the appropriate manager.

## **Company Software**

All software that is available on Business Name’s network is owned and licensed by Business Name. Software that is purchased and licensed for company use is to be used on the Company’s resources only. Taking software home for personal use is not allowed unless authorized by [Senior Management / Owner]. In specific cases, authorization may be given to use company software at home for company purposes only.

At no time will outside software be installed or run on company devices (e.g. workstations, PDAs) without the proper authorization of the [Network Administrator / IT Manager**/**Owner] or the [Information Security Officer / Network Administrator / President / Owner]. This includes downloading software from the Internet, installing plugins for Internet browsers, or installing utilities such as specialized screensavers, etc. This can cause damage and configuration problems that may cost the company money to repair, as well as the possibility of introducing a virus to the network. The unauthorized use of outside disks or other media is not allowed to prevent the introduction of a virus or malware. Peer-to-peer file sharing is also not permitted.

As part of ongoing preventative maintenance procedures and/or troubleshooting operations, Business Name could, at any time and without notice, re-install a standardized configuration on your workstation. Any unauthorized software that has been installed will be erased during this process.

## **Software Updates**

Some software applications are now auto-updating with pop-up windows for the users to click “okay” in order to implement the update. In addition, some Internet sites require the installation of software or plugins. [However, employees are strictly prohibited from performing this action, as any and all updates are to be performed by the Network Administrator / Owner Designee.] OR [However, employees are prohibited from performing this action on all applications except the following:

* List exceptions here

##

## **Antivirus Efforts**

Antivirus software is installed on all computers and servers. Virus definitions are updated weekly or as new definitions become available from the vendor at both the server and desktop level. Antivirus software may not be disabled for any reason. If you notice a problem with your virus software or have a question related to e-mail attachments, virus scans, etc., immediately notify your [Network Administrator / Owner].

Virus definitions are updated weekly or as new definitions become available from the vendor at both the server and desktop level. [Patches and AV DAT updates are pushed during normal business hours to ensure all workstations receive the updates.] OR [Patches and AV DAT updates are performed after normal business hours. Therefore, updates may be scheduled so that all employees will be prepared to leave their workstations turned on when they leave for the day.]

The unauthorized use of outside disks or other media is not allowed to prevent the introduction of a virus. Though Internet e-mail will be scanned for viruses, employees are NOT to open e-mail attachments from unknown sources. Do not open unexpected attachments from known sources without checking with those known sources first.

If you suspect infection by a computer virus, immediately stop using the involved computer and immediately inform your [Network Administrator / IT Manager / Owner]. The infected computer must also be immediately isolated from internal networks. Do not attempt to eradicate viruses yourself. Your [Network Administrator / IT Manager / Owner] will complete this complex task in a manner that minimizes both data destruction and system downtime, while ensuring the source of infection is determined to prevent further damage**.**

## **User Accountability**

You are responsible for all activity that takes place on the Information System and the Network using your user name. If the security of your user login is compromised, you are still responsible and liable for all activity under that user name. Thus, you must learn and take very seriously all issues related to security (such as password practices).

## **Network Password**

You are to choose a password to be used to log into the network. This password should be used exclusively for network login. Nobody except you should know this password. The system will require you to change your password periodically every 90 days. Your Network Login Password should be considered strong. This means the password should be at least 8 characters long and utilize upper and lower case letters, numerical, and special characters. Do not use any word that can be found in a dictionary as your password. Be careful to use passwords which cannot be easily guessed, but that are easy for you to remember. Passwords used at Business Name should be unique to Business Name. The passwords are not to be the same as a password for personal use, such as at a website.

If you forget your password, the [Network Administrator / IT Manager / Owner] will give you a temporary password so that you may log into the network. It is essential that you change that password immediately after login. Again, nobody should know your network password except you.

## **Long Passwords or Passphrases**

## Consider language that gets employees started using passphrases, such as:

## Criminals now use software applications, called “cracker software,” to compromise passwords by automatic guessing, at the speed of a computer, typically going through an entire dictionary in less than 20 seconds. Studies are showing that the longer your password, the harder it is to “crack.” In fact, because of the way passwords are stored using Microsoft Windows, if you use a password that is 15 characters or longer, your password will take a much longer time to crack. Thus, passphrases with strong passwords in them are the strongest type of passwords to use. Examples of passphrases include:

* I\_love\_to\_use\_M@rg2r1n3.
* Criminals\_now\_use\_$0ftw@r3!
* Passphrases\_are\_sTr0ng3r!

All of the above phrases are longer than 15 characters, and would most likely be the last passwords to be cracked. Thus, though this policy does not yet require it, employees are encouraged to begin learning to use passphrases for critical applications, whenever possible.

## **Critical Passwords**

The use of strong and unique passwords should be used on all critical systems. Strong passwords should be at least 8 characters long and utilize upper and lower case letters, numerical, and special characters. Be careful to use passwords which cannot be easily guessed, but that are easy for you to remember. Do not use any word that can be found in a dictionary as your password.

The following critical systems require the use of strong passwords:

 List any critical systems here.

## **Other Passwords**

Some software programs on the network also require passwords. You will also need to choose a password to use when you log in at the application level. Do NOT use your Network or other critical passwords. Again, nobody except you should know this password.

The following applications also require strong passwords:

Accounting Application (Note that QuickBooks does not allow strong passwords).

General Ledger Applications, Accounting Applications

Any applications that store NonPublic Customer Financial Information as required by GLBA.

Any applications that store Personally Identifiable Information as required by GLBA.

Any applications that store ePHI as required by the HIPAA Security Ruling.

Any application used to access a bank account (checking, savings, retirement, etc.) owned by Business.

The network security policy regarding passwords ONLY applies to your network login password. Do not change passwords within individual software programs unless you have the express permission of the [Network Administrator / IT Manager / Owner].

## **Password Themes**

Consider suggesting that employees use password themes, using language such as:

Password themes are a great way to remember several passwords that you use. Critical passwords should be unique and have nothing to do with the user or other passwords. But for the non-critical passwords, themes can be used to help you remember those passwords. Thus, a typical password scenario would look metaphorically like this:

* Windows Password: A
* All other passwords: C1, C2, C3, C4, C5

The following are sample password themes:

* Critical Passwords:
	+ G0ing\_2da^S@! Windows Login Password (Going to the USA)
	+ 1n\_M1\_d3$k! [Proprietary Application] Password (In my desk)
* Non-critical Application Passwords:
	+ mD1@bgS\* My dog is a big German Shepherd.
	+ m!bTd%t! My little Boston Terrier does great tricks!
	+ mDc^1tY! My dogs chase rabbits in the yard!

## **Remembering Passwords:**

Other tricks to remembering your password include:

* Don’t even bother remembering those “once-in-a-while” passwords or non-critical passwords that you are memorizing with your browser (assuming your password policy allows this.) If you forget a third party website (e.g. Orbitz, Facebook, Twitter) password because you got a new computer since the last time you logged in, no problem, (e.g.Orbitz, Facebook, Twitter) will help you set up a new password.
* Never change a password on a Friday. Most programs, as well as Windows and Novell networks, allow grace logins before you actually have to change a password (your IT people can configure this in other ways as well, so talk to them). If you’re asked to change a password on Friday morning, try to get through the grace logins so that you can change it on Monday morning.
* While making up your password, look around you and try to center your password on something that you see. Many times it may be hard to remember a password, but you can remember what you looked at while making up your password, and then the password comes to you!
* Remember; don’t write your password down! If you do, shred the paper once you’re done creating your password.
* Visualize your password as you make it up.
* Once you reset your password, immediately log out and log back in.
* 20 minutes or so after you reset your password, log out and log back in.
* Don’t worry if you do forget your password. The [Help Desk / Network Administrator / IT Manager / Owner] is used to this and everybody has forgotten a password once or twice!

## **Password Protection**

Do not share your passwords with anyone. In addition, passwords must not be:

1. Written in any format
2. Revealed over the phone to anyone
3. Revealed in an e-mail message
4. Revealed on questionnaires or security forms
5. Discussed about in front of others
6. Hinted at or made easy to guess
7. Used in sync with or duplicated by personal passwords or Web accounts
8. Shared with family members
9. Shared when out of the office
10. Typed in or saved in electronic documents

In addition, do not use the “Remember Password” feature found with some applications (e.g. Outlook, Chrome, Messenger, and Mozilla). Anyone gaining access to your system could then easily gain access to confidential information.

## **Wireless Access Points**

The client needs to determine whether they want to prohibit or allow the use of wireless access points. If wireless access is allowed, then this section should be removed and the Client needs to create a Wireless Access Point Procedure.

Business Name prohibits the use of wireless access points. **The Information Security Officer / Network Administrator / President / Owner] will perform regular wireless discovery audits. Any devices found will be immediately disconnected and confiscated. Devices such as laptops with built-in wireless networking cards must have the wireless function disabled at all times.**

## **Leaving Your Computer**

If you leave your computer unattended for any significant period of time (e.g. lunch hour), close all applications and log out of the network. If your computer is going to be unattended for short periods (e.g. breaks, meetings), secure the computer with one of the following methods:

* 1. Close all applications and log out of the network, then turn off your monitor;
	2. Lock the computer with a keystroke combination (-l or Ctrl-Alt-Del), then turn off your monitor. (Some systems have this ability. Check with the [Network Administrator / IT Manager / Owner] if you are unsure whether your computer has this capability.)

You should also take into consideration the exposure your computer has to non-employees and secure the computer accordingly.

Unless otherwise instructed, you should completely shut down your computer and related equipment before leaving at the end of the day.

## **Employee Mailboxes**

Employee mailboxes should be checked regularly and right before leaving at the end of the day. Information that contains nonpublic customer information should be placed in an interoffice envelope, delivered in person, or kept secure for later delivery when confidentially can be assured.

## **Voice Mail**

If you have a voice mailbox, you are required to secure it with a password. See the telephone system documentation or your [Network Administrator / IT Manager / Owner] for instructions on how to do this.

Voice mail is not an unlimited resource. All Users are limited to [equalize to voice mail documentation] of storage space.

Offensive language is prohibited on voice mail. This includes when leaving a message on someone else’s voice mail or on the User’s personal greeting.

## **Access Rights**

The system is set up to automatically give you access rights to all areas (directories, Internet services, etc.) and resources (printers, scanners, etc.) of the network which Business Name has pre-determined you will need. If you believe you need access to areas and/or resources that you do not already have, feel free to request access from your [Network Administrator / IT Manager / Owner].

The [Network Administrator / IT Manager / Owner] is the only person authorized to grant access to users. Any attempt to gain access without involving the [Network Administrator / IT Manager / Owner] is grounds for termination.

## **Information Storage**

You will be trained where you are to store data that you create on the computer. It is essential that you understand the protocols regarding this. NEVER EVER store data on your workstation, unless you have been instructed to do so by the [Network Administrator / IT Manager / Owner].

Data that is not stored correctly is not properly backed up and can be lost. As part of ongoing preventative maintenance procedures and/or troubleshooting operations, Business Name could, at any time and without notice, reinstall a standardized configuration on your workstation. Any data that is not properly stored will be lost during this process.

Historical paper records pertaining to a customer’s account with Business Name, such as completed loan files, that are removed from storage must be returned to the locked location. This policy will be included in the Record Retention Program.

## **Reporting Suspicious Activity and/or Suspected Security Incidents**

****

In the event that you notice activities by other employees, vendors, or customers or you become aware of security incidents, weaknesses, and software malfunctions, or are concerned there may be a virus on your computer, please report such suspicions to your immediate supervisor who will help you “broadcast awareness,” meaning that you will inform all appropriate persons so that they will not “fall victim” to the suspicious activity. After broadcast awareness, the Information Security Officer / Network Administrator / President / Owner] or [Network Administrator / IT Manager / Owner] or his/her supervisor should be informed via e-mail and/or any other means available.

## **Copyrights**

Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission from the [Network Administrator / IT Manager / Owner].

## **Prohibited Activities**

Purposely bypassing built-in security features in software or systems, such as time outs, screen locks, etc. is strictly prohibited.

Only authorized employees, temporary workers, contractors, and consultants are permitted access to the server room.

Without prior written permission from Management, the computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, or any other unauthorized materials. Employees are strictly prohibited from disseminating destructive code (e.g., viruses, Trojan horse programs, etc.).

Occasional limited appropriate personal use of the computer is permitted if such use does not a) interfere with the user’s or any other employee’s job performance; b) have an undue effect on the computer or Business Name’s network performance; or, c) violate any other policies, provisions, guidelines or standards of this agreement or any other agreement of Business Name. Further, at all times, users are responsible for the professional, ethical and lawful use of the computer system.

Personal use of the computer is a privilege that may be revoked at any time.

## **Communication of Trade Secrets**

Unless expressly authorized to do so, users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to Business Name. Unauthorized dissemination of such material may result in severe disciplinary action, as well as substantial civil and criminal penalties under state and federal laws.

## **Visitor Access**

Visitors to the facility must use a single point of entry and sign in/out on the “visitor sign-in sheet” located at the reception desk. In addition, all visitors must be escorted through the facility and wear a visitor badge so they will be easily recognized as guests rather than employees. Facility managers must reconcile the sign-in sheet every night prior to closing down the facility.

## **Keys, Locks, and Combinations**

If you are issued keys, they must be protected at all times. Keys left unattended may be picked up by unauthorized persons who could use a key to gain access to Business Name’s systems. Keys may not be duplicated without prior permission from the [Information Security Officer / Network Administrator / President/ Owner].

If you have access to areas that require locks and combinations, you must keep this information secure and confidential.

## **Clean Desktop Policy**

Office space is frequented by visitors, consultants, vendors, cleaning crews, maintenance and other employees. As it is crucial to protect sensitive information from disclosure, employees are not to leave confidential or sensitive information on their desks. Such items may include:

* User IDs and/or passwords
* IP addresses
* Contracts
* Loan Files
* Account numbers
* Customer lists (including Social Security number, address, telephone number, etc.)
* Intellectual property
* Employee records

Employees are required to keep all sensitive information described above “under lock and key” when they are not in their office for an extended period of time, which could be as low as 5 minutes in high traffic areas, but not more than 15 minutes in private areas. If your door has a lock, and you can lock your entire office, locking it when you leave is sufficient. Otherwise, you should lock sensitive information in your file cabinet, desk, or credenza prior to leaving.

The institution will test for compliance with this policy on a regular basis. Any information classified as Internal Use, Confidential, or Critical discovered in an employee’s office when the employee is not present would be considered to be a breach of this policy.

Many businesses may already include this in their Privacy Policy. If this is the case, we recommend they do NOT have redundancy with the AUP.

## **Security of Customer Records**

It is company policy to keep all customer records private, confidential, and secure. This does not only apply to financial data, but all information collected about our customers. Information must be kept private and confidential. The unauthorized dissemination of any information related to our customers, whether or not financial, is prohibited unless this is done in the normal course of your position or with the prior approval of your [supervisor**/**owner]. Legal counsel has reviewed our website and provided policy statement language to be placed on our website. Owners should ensure this is updated annually.

## **Destruction of Customer and Business Records**

In the event that you end up with paper copies of customer records or business records (for example, they leave an account number on a piece of paper in the lobby), the record must be shredded. Any trash with non-public customer information must be shredded. If you are not sure what to do with a customer’s paper record, ask your [Store Manager / Location Manager / Branch Manager / Department Manager / Owner].

Use this following section if you receive a lot of calls looking for customer information. Consider using this section even if you don’t receive a lot of calls, or at least warn employees of this attack vector during training.

## **Authenticating Nonpublic Customer/Employee Information Requests**

When a person calls asking for sensitive information, they could be a threat instead of a customer. Persons involved in domestic or legal disputes, cyber-criminals looking to gather information, and nosey neighbors/friends/family members could call the business posing as a customer. Improperly revealing account balances, e-mail addresses, even tax-id numbers could not only embarrass us, but it is also considered to be against the law.

To prevent threats from exploiting this social engineering approach, called “pretext calling,” we must authenticate nonpublic customer information requests with “out of wallet questions.” This is especially true if the caller is requesting “Nonpublic Customer/Employee Information,” which can include any information that has any or all of the following:

* Name (any name on an account)
* Address (any or all addresses for any account)
* Phone numbers (any or all, including fax)
* Tax ID numbers
* Social Security numbers
* Account numbers (any or all)
* E-mail addresses
* Account balances
* Any type of “protected health information” including results of tests, diagnoses, etc.

When a customeror business calls asking for any of the above information, you MUST confirm the identity of the caller prior to giving them any of the information listed above. If you do not know a customer /caller, feel free to ask the customer to provide “out-of-wallet” authentication information. “Out-of-wallet questions” seek validation information that can not be found in a person’s lost wallet or purse, or on social media. Out of Wallet Questions are “customer-centric.” The particular question you ask often depends on the person calling. Not every customer will know the answer to every out-of-wallet question, and thus you must seek the customer’s help in finding a legitimate out-of-wallet question. By starting with “For your protection, I need to ask some questions to confirm your identity,” you will enlist the customer’s help in the identification process. Then try to find a question that will prove the customer’s identity, which can NOT be found in a lost wallet or purse or on social media, such as:

* Predefined challenge questions (note: if your system supports this, it would be ideal, but not all customers will have a challenge question and employees should still be taught to use out of wallet questions.)
* Amount of last invoice or transaction on file.
* What was purchased in the last transaction on file?
* Amount / date of automatic payments
* Month and Year account was opened
* Anything that can not be discovered in a lost wallet or purse, or on social media.
* Multiple Choice Questions where none of the choices are correct (use sparingly, and only when customer can’t answer other out-of-wallet questions)

Keep in mind the normal identifying information can be found by a malicious person. Information such as date of birth, tax identification number, mother’s maiden name (found in social media sites), address, and/or account number can be used to verify a member’s identity ONLY if combined with out-of-wallet questions as defined above. The customer information listed above may not be shared with anyone outside of Business Name without permission from your [Store Manager / Location Manager / Branch Manager / Department Manager / Owner].

If you can not find a legitimate out-of-wallet question, there are only three options left: you can call the customer back at a number on file at the business, require the customer to come into the business, or pass the customer along to your supervisor.

## **Use of Information from Remote Site**

Business Name may, from time to time, grant permission for users to work on company information at a remote location, such as their home, the library, etc. In these cases, you will receive a copy of our Remote Access Security Procedure, and you must comply with that.

However, in such a grant, the company does NOT imply permission to take confidential customer and business records home. Business Name strictly prohibits the storage of customer or business records on any workstation, server, PDA, cell phone, etc. that is NOT part of Business Name’s network, unless for normal operations (such as sending records to authorized third party vendors).

It is critical to understand that for security and privacy reasons, employees are required to do their best to ensure that customer and business records do not leave Business Name’s authorized computer equipment, that customer and business records are always secure and private, and that customer and business records are stored in a manner consistent with the efforts of Business Name to protect the privacy rights of customers. It is our policy to make every effort to comply with all applicable laws, rules, and regulations regarding the privacy rights of its customers.

##

## **Zero Privacy Expectations**

Employees are given computers and Internet access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, send or receive using Business Name’s computer equipment. The computer network is the property of Business Name and may be used only for business purposes.

## **Waiver of Privacy Rights**

By signing this policy, users expressly waive any right of privacy in anything they create, store, send or receive using Business Name’s computer equipment or Internet access. Users consent to allow company personnel access to and review of all materials created, stored, sent or received by User through any Business Name network, server, workstation, portable device, or Internet connection.

## **Monitoring of Computer and Internet Usage**

Business Name has the right to monitor and log any and all aspects of its computer system including, but not limited to, monitoring Internet sites visited by Users, monitoring chat and newsgroup usage, monitoring file downloads, and all communications sent and received by users.

Note: This next section might be a bit much for small businesses, but you should develop a classification structure that you communicate to your employees. Often data is breached “unintentionally” because employees do not know that business owners may want to keep the information sensitive. For example, many small business owners would not want employees telling just anybody who calls the name of the company owners. Or who their suppliers are. Or even that they are on vacation. Identifying this up front is a great way to protect your privacy.

## **Data Classification**

The Information Security Officer / Network Administrator / President / Owner] will facilitate a Data Classification Process with each Data Owner on an annual basis. Data classifications will be as follows:

1. Critical
2. Confidential
3. Internal Use
4. Public

A Data Classification Process is a business decision process established to ensure the appropriate security levels are assigned based on information values and sensitivity. Therefore, Business Name has adopted four classifications by which to gauge information value or sensitivity. This project will classify all data owned by the Data Owners in one of the following categories:

1. **Critical**
Business processes and information assigned to the “Critical” classification are generally essential to Business Name’s business, proprietary and/or trade secrets. This would include information protected by law, as well as information that, if disclosed to unauthorized individuals, could reduce Business Name’s competitive advantage or cause other damage to Business Name.

Information classified as “Critical” would include, but is not limited to, the following:

* + 1. Assembled Non-public Customer Financial Information such as account numbers, social security numbers, account balances, and other information that is considered to be personally identifiable financial information protected by federal law
		2. An entire customer database.
		3. Assembled personally identifiable healthcare information protected by the federal law under the Health Insurance Portability and Accountability Act
		4. An entire file of employee health insurance applications.
		5. Access codes or passwords that protect information systems and physically secured resources.
		6. Any assembled information that could be used to facilitate “identity theft” such as credit card numbers, account numbers, driver license numbers, insurance records, etc.
		7. Records containing personal information of several employees that include names, addresses, phone numbers, marital status, performance appraisal ratings, date-of-birth, social security numbers, number of dependents, salaries, etc.
		8. Trade secrets, operating plans, marketing plans, business strategies, proprietary methods and product or system designs; that would damage the institution if revealed.
		9. Information and business processes needed to support key lines of business.
		10. New technology research, descriptions of unique parts or materials, proprietary program software, etc.
		11. Records containing personal information of several shareholders that include names, address, phone numbers, marital status, date-of-birth, social security numbers, number of dependents, etc.
		12. Corporate litigation information “classified as Critical” by any member of Business Name’s management team.
		13. Any information “labeled” as “Critical” by members of Business Name’s management team.

If any of these items can be found freely and openly in public records, Business Name’s obligation to protect from disclosure is waived.  However, issues surrounding potential liability regarding integrity and reputation still apply.

1. **Confidential**Business processes and respective information that, if lost, disclosed, misused, or modified by unauthorized persons, might result in harm to individuals causing monetary loss, criminal or civil liability, or significant damage to Business Name’s reputation.  This information is of a private nature that an individual would not want disclosed to others.
2. Information classified as “Confidential” would include, but is not limited to, the following:
	* 1. Individual Personally Identifiable Information (as opposed to assembled, which would be classified as Critical).
		2. One form with nonpublic customer financial information on it for one individual.
		3. The Personally Identifiable Financial Information protected by federal law.
		4. Personally identifiable healthcare information protected by the federal law under the Health Insurance Portability and Accountability Act.
		5. One health insurance application with one person’s health history on it.
		6. Individual instances as opposed to assembled information or aggregated information.
		7. Records containing personal information of individual employees that include names, addresses, phone numbers, marital status, performance appraisal ratings, date-of-birth, social security numbers, number of dependents, salaries, etc.
		8. Financial information that is not subject to public record such as payroll accounting.
		9. Records containing personal information of individual customers that include names, addresses, phone numbers, marital status, performance appraisal ratings, date-of-birth, social security numbers, number of dependents, etc.
		10. Any information that could be used to facilitate “identity theft” on one person, such as credit card numbers, account numbers, driver license numbers, insurance records, etc.
		11. Records containing personal information of individual shareholders that include names, address, phone numbers, marital status, date-of-birth, social security numbers, number of dependents, etc.
		12. Any personal information that could be used to facilitate “identity theft” such as credit card numbers, account numbers, driver license numbers, insurance records, etc.
		13. Individual Personally Identifiable Information (as opposed to assembled, which would be classified as Critical).
		14. Information and business processes needed to support key lines of business.
		15. New technology research, descriptions of unique parts or materials, proprietary program software, etc.
		16. Any written information that would be covered by the Genetic Information Nondiscrimination Act of 2008 (GINA) would be classified as confidential.
		17. Floor plans, electrical wiring and powering diagrams.
		18. Litigation papers not deemed “Critical” by a member of management.
		19. Corporate litigation information “classified as Confidential” by any member of Business Name’s management team.
		20. Any information “labeled” as “Confidential” by members of Business Name’s management team.
3. **Internal Use**
Business processes and respective information that, if lost, disclosed, misused, or modified by unauthorized persons, might result in significant monetary loss, significant productivity loss or significant damage to Business Name’s reputation.  The information is not to be shared with entities outside Business Name unless it is authorized by management and in direct support of Business Name’s business.

Internal Use information would include, but is not limited to, the following:

* + 1. Internal operating procedures and internal business reports and memorandums.
		2. Information that is subject to nondisclosure agreements with other organizations or individuals.
		3. Business Name’s internal phone directory.
		4. Documented policies, standards, procedures and guidelines.
		5. Aggregated Customer balance information, such as sum of all deposits for the day.
		6. Reports listing just the customer names, but no other personally identifiable information.
		7. Internal announcements and mailing distributions made by management.
		8. Vendor information such as product and services pricing, specific quotes or contracts.
		9. Floor plans, electrical wiring and powering diagrams.
		10. Information and business processes needed to support key lines of business.
		11. New technology research, descriptions of unique parts or materials, proprietary program software, etc.
1. **Unrestricted/Public**
Business processes and respective information used to support Business Name’s business.  This is information that has been authorized to be made available to the public.  Although this information can be published to the general public, copyrighting must be considered.  Integrity of this information is relevant as well.

Unrestricted/Public information would include, but is not limited to, the following:

* Information generated for public consumption such as service bulletins, marketing information, advertisements, annual reports etc.

## **Internet Use**

The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk and Business Name is not responsible for material viewed or downloaded by users from the Internet. To minimize these risks, your use of the Internet is governed by the following policy:

The client needs to determine whether they want to completely prohibit personal use or define good judgment. The first approach exposes the business to legal risk. Choose one:

[Business Name] prohibits the use of company resources for personal reasons during normal business hours.]

Or:

Limited personal use of [Business Name]’s resources during business hours is allowed with good judgment. Security Awareness Training addresses what [Business Name] means by “good judgment.” The viewing of offensive or pornographic sites may result in immediate dismissal. The presence of questionable material in the workplace is not acceptable. All users have a responsibility to use the Internet in a professional, lawful and ethical manner. Abuse of the computer network or the Internet may result in disciplinary action, including possible termination, and civil and/or criminal liability.

To ensure security and avoid the spread of viruses, users accessing the Internet through a computer attached to Business Name’s network must do so through an approved Internet firewall or other security device. Bypassing the organization’s computer network security by accessing the Internet directly by modem or other means is strictly prohibited unless the computer you are using is not connected to Business Name’s network. Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources.

Do not connect any device to the network without approval. Any device that is not owned by Business Name cannot be connected to the organization’s network without the prior approval of the [Information Security Officer / Network Administrator / President / Owner]. Do not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others.

To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to Business Name’s network must do so through an approved Internet firewall or other security device. Bypassing Business Name’s computer network security by accessing the Internet directly by modem or other means is strictly prohibited unless the computer you are using is not connected to Business Name’s network. The business has a separate procedure governing mobile devices called the Portable Devices Security Procedure. This document addresses how devices such as laptops, tablet PCs, or smartphones are to be used. If you are issued a mobile device, or if you are approved to store data on your own mobile device, you must review this procedure and sign the signature page. See your supervisor if you do not have this procedure.

Do not connect any device to the network without approval. Any device that is not owned by Business Name cannot be connected to the business’ network without the prior approval of either the [List positions that are allowed to approve access here. Note: this may need to be equalized to your Access Management Procedure or other procedure governing access.]

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. Do not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters in e-mail, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business related uses of the Internet.

## **Company/Business Information on Personal Blogs / Websites**

Unless expressly authorized to do so, employees of Business Name are strictly prohibited from posting company related information on personal blogs, social networking sites, or other websites not authorized by the Business Name [other than information found in a typical resume].

In practice, this policy has become similar to the “no personal use of computer systems” approach, rather than “limited personal use.” Given that “no personal use” is not being enforced on a widespread basis, to enforce it for one employee would create legal risk. Thus, we recommend a policy position that employees should use “good judgment” in personal use of the systems. Training then focuses on guidelines as to what is good personal judgment versus what may result in disciplinary action. Social media sites create the same type of issue. Many employees believe they have a first amendment right to post whatever they want on their own personal websites, and thus the need for a strong policy and guidelines that allow postings, but govern them.

Therefore, new policy language needs to be created that will allow posts on social networking sites but expect the employee to use good judgment. Then a “guidelines document” should be distributed that spells out what the business expects. The topic should also be addressed in regularly scheduled Security Awareness Training as well as periodic reminders.

**If the above is not the case, do NOT use the above section (delete it), but retain and customize the following section instead.**

## **Social Media Policy**

With the rise of new media and next generation communications tools, the ways in which employees can communicate internally and externally continue to evolve.  While this creates new opportunities for communication and collaboration, it also creates new responsibilities for employees.

Social networks and social media tools have the potential to detract from productivity in the workplace. While the use of social media by employees is acceptable in accordance with the guidelines provided in this policy, it is not always appropriate for the workplace. Therefore, we have established a policy addressing (1) the use of social media at work or while using company equipment and (2) references to the company and/or its customers in social media.

Use of Social Media on Company Equipment or Company Time:

ALTERNATIVE A:

Personal blogs, Facebook, MySpace, LinkedIn, Twitter, Digg, Yahoo! Groups, YouTube, Wikipedia and other sites where text can be posted, and any other blogs or social networking sites (collectively referred to herein as “social media”) are not to be accessed from any equipment owned, leased, or controlled by the business unless, and then only for the purposes that, a supervisor/owner specifically directs you to do so. For purposes of this policy, “business equipment” includes Internet access services provided by Business Name.

In addition, access to social media by employees during work hours is prohibited. You may access social media during any approved break times provided that you use your own equipment to do so.

Employees are hereby notified that all electronic communications via the business’ equipment are subject to monitoring by the business or its designated agent.

**OR**

ALTERNATIVE B

Business Name realizes that employee social networks and social media tools may provide some value to the business. As a result, we have established a policy that allows employees to utilize personal blogs, Facebook, MySpace, LinkedIn, Twitter, Digg, Yahoo! Groups, YouTube, Wikipedia and other sites where text can be posted, and other blogs or social networking sites (collectively referred to herein as “social media”) while at work as long as certain guidelines are met. If you choose to access social media via business equipment (including Internet access services provided by the business) and/or during work hours, you agree to follow the guidelines established by this policy. In addition, you are to receive, read, and agree to follow the User Guidelines for Social Media and / or Management Guidelines for Social Media (depending on individual status within the business). These documents are called “User Guidelines for Social Media” and “Management Guidelines for Social Media.”

Remember to be productive. Social media can be a time sink and can prevent you from completing other work-related tasks. Use good judgment to ensure that you have plenty of time to complete all of your regular work.

Employees are hereby notified that all electronic communications via Business Name’s equipment are subject to monitoring by the organization or its designated agent. Remember to be productive. Social media can be a time sink and can prevent you from completing other work-related tasks. Use good judgment to ensure that you have plenty of time to complete all of your regular work.

Guidelines for Use of Social Media: Please be aware that violation of this policy may result in disciplinary action up to and including termination.

Common sense is the best guide if you decide to post information in any way relating to Business Name. If you are unsure about any particular posting, please contact [the Information Security Officer / the Network Administrator / the President / Human Resources / Management**/**Owner] for guidance.

Approved Content: Do not discuss business customers in social media. Be very careful what you say about the business in general, but never discuss customer relationships, individual customers, or what you don’t like about customers in general. Communications that are not prohibited include statements of fact about the business and its products and services, information that has already been made public, and information from the organizations website. If you are writing about Business Name’s business over which you have responsibility, you should obtain the approval of your supervisor/owner prior to posting such information.

If you choose to post any comments that constitute your personal point of view on any matter related to Business Name, your post must conform to the guidelines set forth herein. Any material presented online in reference to the organization by any employee is the responsibility of the poster. All communication should be made in an identifying manner to establish credibility above all else.

Along with clear identification, you should neither claim nor imply that you are speaking on Business Name’s behalf unless you are authorized to do so in writing by your supervisor. If you identify yourself as an employee of Business Name in any social media posting, or if you refer to products or services provided by Business Name or provide a link to the business’ website, you are required to include the following disclaimer in a reasonably prominent place: “The views expressed in this post are mine and do not necessarily reflect the views of Business Name.”

Employees are encouraged to confine their postings to information within their areas of expertise; to maintain professionalism, honesty, and respect; and to apply a “good judgment” test for every activity related to Business Name.

Communication Protocols: Social media is not a substitute for customer, vendor, and inter-office communications. Business Name information should be transmitted within normal communication channels, not on social media.

Customer inquiries should be referred to [Customer Service / Owner] or other appropriate department rather than handled through social media.

Off-limits Material:Your social media postings should not violate any other applicable Business Name policy, including those set forth elsewhere in the [Acceptable Use Policy / User Policy / Microcomputer Policy / Internet and E-mail Policy / Network Use Policy]. In addition, the following types of social media communications by employees are specifically prohibited:

* Inaccurate or Defamatory Content: Employees may not participate in online communication that is not in the best interest of Business Name. Prohibited online communication may include but is not limited to unverified, inaccurate, distasteful, or defamatory comments or information about Business Name. In general, you must not post any information that would tend to damage thebusiness’ reputation or dissuade anyone from conducting business with Business Name.

In addition to disciplinary action by Business Name, you may be subject to liability if your posts are found to be defamatory, harassing, or in violation of law.

* Intellectual Property, Trade Secrets, or Customer Data: Your social media postings cannot include company logos or trademarks and must respect copyright, intellectual property, privacy, fair use, and other applicable laws. Use of Business Name’s intellectual property and trade secrets are strictly forbidden from any online discourse except through mechanisms managed internally by Business Name.

Of particular importance are federal regulations prohibiting the disclosure of any personally identifiable nonpublic information regarding our customers. Business Name is required to maintain and protect customer data as confidential. Therefore, you must not include any personally identifiable nonpublic customer information in any online communications except through mechanisms managed internally by Business Name.

Be aware that you may also be personally liable if your postings include confidential or copyrighted information.

* Note: This bullet point offers two alternatives. The business could forbid recommendations completely, or the business could forbid “formal” recommendations. The latter should be accompanied by a mitigating disclosure.

Select which paragraph fits your needs, and then delete the remaining paragraph.

Some sites, such as LinkedIn, allow members to “recommend” current or former co-workers. Business Name forbids employees from making recommendations regarding other former or current employees for reasons of business liability. All communication of this type should be referred to [the Information Security Officer / the Network Administrator / the President / Human Resources / Management / Owner] for verification.

**OR**
Some sites, such as LinkedIn, allow members to “recommend” current or former co-workers. Business Name forbids employees from making formal recommendations regarding other former or current employees for reasons of business liability. All communication of this type should be referred to [the Information Security Officer / the Network Administrator / the President / Human Resources / Management / Owner] for verification. Informal “endorsements” can be made as long as the following language accompanies the post: “For a more formal reference on employee name, please contact [the Information Security Officer / the Network Administrator / the President / Human Resources / Management / Owner] via e-mail at e-mail address.

* Financial Information: Any online communication regarding Business Name’s financial data is strictly forbidden except through mechanisms managed internally by Business Name communications or marketing groups.
* Sensitive Matters: Any online communication regarding proprietary information such as layoffs, strategic decisions, or other announcements deemed inappropriate for uncoordinated public exchange is forbidden.

Reporting of Noncompliance: If any employee becomes aware of social networking activity that is distasteful or fails the good judgment test, please immediately contact the [the Information Security Officer / the Network Administrator / the President / Human Resources / Management / Owner]. You may do so anonymously.

Your Liability: To be clear, you are liable and accountable for anything you post in social media about the business or the business of [your industry here] in general, and you could be judged by your coworkers, supervisor, and the business for what you post in social media.

Limitation of Liability: You agree that Business Name shall not be liable, under any circumstances, for any errors, omissions, loss or damages claimed or incurred due to any social media communications by you.

Disclaimer:This policy intends to manage technology and information risk, and does not intend to infringe on employees’ Section 7 rights under the National Labor Relations Act (NLRA), and will not be applied in that manner. Specifically, any “concerted activities” performed on social media sites are not governed by this policy. For example, any discussions about the terms and conditions of your employment at [Business Name] as protected by the NLRA are not intended to be affected by this policy.

## **Webmail**

Webmail is a version of e-mail that uses your normal web-browser [Google Chrome, Internet Explorer, Mozilla Firefox] as the interface. You get to your webmail by going to a website outside of the organization's own mail servers. Many individuals have their own personal webmail accounts. Examples of webmail include Hotmail, Yahoo Mail, Gmail, etc. Business Name [does][does not] allow the use of webmail for personal accounts. (We recommend prohibiting them. If you do allow webmail consider adding: Personal accounts should not be used for business communications without express permission from the [Network Administrator / IT Manager / Owner].)

## **Chat Rooms**

The use of public messaging systems or chat rooms, such as those available on MSN, Yahoo, or Facebook, for the exchange of confidential information is prohibited. If you DO need to access a chat room in the course of your business for the exchange of non-confidential information with outside vendors, please notify the [Network Administrator / IT Manager / Owner].

## **E-mail Use**

The use of Business Name’s e-mail for personal communication is allowed on a limited basis. The transferring of excessively large files or large numbers of messages through Business Name’s servers is forbidden unless authorized and necessary. The receiving and forwarding of jokes, e-cards or possibly offensive material is not allowed. This material would have the business’ name attached to it and can put the business at a liability risk. Participation in “chain-letters”, spamming of any form, or any illegal activity may be grounds for immediate dismissal. For the purpose of this policy, spam is defined as ANY unsolicited mailing to individuals, either known or unknown, with the intent to sell a product, promote a service or site, or bring gain in any way to the sender or sender’s affiliations, which has not been authorized by [Senior Management / Owner].

## **Secure E-mail**

This next section only applies to businesses that are using a Secure Messaging system (a system that automatically encrypts sensitive information in email). If you transmit sensitive information using email very often (more than once per week), you should consider such as system.

Business Name uses Name of Software for secure e-mail. You ARE allowed to send sensitive information in e-mail if you utilize the secure e-mail package that Business Name has procured.

Note: If your secure messaging system has any user control considerations related to all users, such as sending announcement messages, consider documenting those in this policy. For example:

Our system encrypts e-mails and stores them on a server that sends a message to your intended recipient asking them to click on a link and log in to retrieve the message. This causes several of our customers to become frustrated if we do not properly help them remember passwords. Meanwhile, it does increase the likelihood of a successful phishing attack if we do not communicate carefully. Thus, this policy requires users to announce secure messages. This can be done verbally, or via e-mailed announcement messages with the following language:

Hello,

You will be receiving an e-mail from me, asking you to click on a link. It is legitimate.

<add information that specifically proves you are who you say you are.>

Please confirm when you have successfully downloaded the document!

Thanks,

<Your Name>

This is an out-of-band announcement of a secure message.

-----------------------------------------------------------------------------------------------------------------

NOTE: IT IS A BEST PRACTICE TO SEND AN OUT-OF-BAND E-MAIL ANNOUNCING DELIVERY OF A SECURE MESSAGE THAT USES A WEB PORTAL, TO PREVENT RECIPIENTS FROM BECOMING VULNERABLE TO A PHISHING ATTACK.

-----------------------------------------------------------------------------------------------------------------

Please do not open messages from me that are not announced!

## **E-mail Distribution Lists**

Business Name allows mass e-mailing for distribution lists only. This includes the following distribution lists:

* List here.

## **E-mail Signature Use**

All employees are required to use an appropriate and approved e-mail signature for all e-mails sent from Business Name’s domain. As such, every user of Business Name’s e-mail system must have included in their e-mail signature the following statement:

NOTICE: The information contained in this email is confidential and intended solely for the intended recipient. Any use, distribution, transmittal or retransmittal of information contained in this email by persons who are not intended recipients may be a violation of law and is strictly prohibited. If you are not the intended recipient, please contact the sender and delete all copies.

As e-mail is not a secure medium, non-public information (e.g. social security numbers, account numbers, etc.) is not to be sent via e-mail.

Business Name complies with all provisions of the CAN-SPAM ACT of 2003. If you have received this e-mail and wish to opt-out of future commercial e-mails, please fill out the form located at: state URL of opt-out form.

##

## **E-mail Auto-Reply Use**

Employees are prohibited from using the “auto-reply” feature available on our e-mail client.

 OR

The use of our e-mail client’s “auto-reply” feature is restricted to departments directly involved in customer service or on a case-by-case basis, with approval being granted by [Managemen**t** / Owner]. However, employees that are allowed to use the “auto-reply” feature are limited in what information can and cannot be revealed on the reply. The following restrictions apply:

* DO keep messages simple. State that you are out of the office, but don’t state your reason for being gone.
* DO get permission before divulging an alternate contact’s information.
* DO be careful about what you state about your job title (the higher up the ladder, the more attackers attempt to gather and use information).
* DON’T be specific about the dates you will be away from the office.
* DON’T divulge an associate’s e-mail address (this is more fuel for their fire). Give a phone number of someone that can help them in your absence instead.
* DON’T divulge personal information in your auto-reply message (home phone, cell phone, etc.).

## **E-mail Privacy**

While e-mail is private and secure within our firewall, this is a privilege and not a right. Any information transferred through Business Name’s resources can be intercepted and used for public record in the event of the suspicion of illegal activity or suspicion of activity to undermine Business Name or its customers. However, if it is deemed necessary to intercept and screen an individual’s e-mail, that individual will be informed once the investigation is completed and any extraneous information will be kept private.

Because of the nature of e-mail, it is impossible to guarantee that e-mail will not be read by another individual, not to mention that it could be inadvertently forwarded to a system postmaster, as well as the fact that your e-mail may be viewed in the event that you leave the organization.  Because of this, expect NO privacy in the use of your e-mail.

## **Portable Devices**

Note: There are two parts to this policy. The first, which should be in this policy regardless of your current posture on mobile devices, governs all users. The second part governs the subset of users who are issued mobile devices or authorized to use their own devices.

Part One:

Business Name recognizes the changing nature of portable devices and wants our employees to benefit from mobile technology while at the same time protecting themselves and the business from the risks associated with portability. Unless otherwise approved to do so (see below), no employee is allowed to use a portable device for business purposes. If not approved according to the policy defined below, you may not use your own device or a device owned by the business. The only exception to this is in the event of an emergency where the safety of business employees, customers, or the community is involved.

Part Two: If you have a stand-alone procedure governing portable devices, you may want to still refer to it in this policy, using the following language as a starting point:

The organization has a separate procedure governing mobile devices called the Portable Devices Security Procedure. If you are approved to use a portable device you will be given a copy of this procedure. This document addresses how devices such as laptops, tablet PCs, or smart phones are to be used. If you are issued a mobile device, or if you are approved to store data on your own mobile device, you must review this procedure and sign the signature page. See [your Supervisor / the IT Manager / the Network Administrator / the Information Security Officer / the President] if you do not have this procedure.

Or, if you do NOT have a stand-alone policy, consider the following:

If you are issued a laptop, personal digital assistant (such as a palm pilot), cell phone, or any other portable device, the device is considered to be the property of Business Name, and you must follow all policies when using the device. You are expected to return the device in good working condition upon request and without notice.

If confidential information resides on a portable device that has been issued to you, you must have a [Network Administrator / IT Manager / Owner] train you on how to secure that device.

A laptop issued to you is not meant as a replacement for your home computer. Personal data, if saved to the laptop, could be lost. You are expected to follow policies regarding storing data to ensure effective backup of your data. As part of ongoing preventative maintenance procedures and/or troubleshooting operations, Business Name could, at any time and without notice, reinstall a standardized configuration on your laptop. Any unauthorized software that has been installed, or data that is stored improperly, will be erased during this process.

You are responsible for the security of the laptop. Theft or loss could be a serious breach of customer confidentiality. [All laptops should be physically secured to the User’s desktop while at the office.] Do not leave the laptop anywhere but inside your home or your office. Do not loan your laptop to anybody. Allow no one but yourself and appropriate companystaff to use your laptop. DO NOT LOSE YOUR PORTABLE DEVICE.  In the event you lose a portable device, inform the [Network Administrator / IT Manager / Owner] immediately.

As a general policy, you are prohibited from transferring nonpublic customer information off of the network.  Do NOT put company data upon your own personal computer equipment without the permission of the [Network Administrator / IT Manager / Owner].  Doing so will require that you comply with security policies not listed in this acceptable use policy.

Unless your job description specifically provides for it, you are not allowed to use USB drives (otherwise known as pen drives, thumb drives, flash drives, etc.). In addition, unless your job description specifically provides for it, do not copy nonpublic customer information onto USB drives without the permission and help from the [Network Administrator / IT Manager / Owner].

Unless your job description specifically provides for it, you are also not allowed to use other temporary storage media (such as floppy drives, CDs, zip drives, or any other portable rewritable media). In addition, do not copy nonpublic customer information onto temporary storage media.  If you need to move data from one system to another, do so with the assistance of the [Network Administrator / IT Manager / Owner].

Unless specifically authorized to do so by the Information Security Officer / Network Administrator / President / Owner], Business Name prohibits connecting any other portable device to your workstation or anywhere on the network. This includes iPods or other media players, cell phones, webcams, or any future technology that has data storage capabilities or potential security implications.

If you are issuing portable devices or authorizing employees to use their own portable device, we strongly encourage you to adopt a stand-alone document rather than making users who are not issued/authorized wade through the details of portable device risk management in their Acceptable Use Policy.

## **Cell Phone Use**

Safety must come before all other concerns. It is the policy of Business Name that regardless Users should refrain from using a cell phone to conduct company business or to make/receive business-related calls while driving a vehicle. Regardless of the circumstances, including road conditions, slow or stopped traffic, etc., users are to pull off to the side of the road and safely stop their vehicle before placing or accepting a business call.

In addition, the use of a cell phone to discuss business with a customer or to discuss a customer’s interests over a cell phone may also create privacy issues, since cell phones are not secure. Also be mindful when using a cell phone, Users should not be discussing customer information in an area where the information can be overheard. Business related calls include (but are not limited to) making or receiving calls with business, customer, associates, management, checking voice mail, leaving a message for an associate, conversing with a customer, etc. Employees are not to send broadcast messages with any device issued by the business.

Employees that are issued a cell phone should have no expectation of privacy pertaining to anything sent or received via that device. This would include voice mail messages, text messages, etc.

## **Facsimiles**

The following guidelines should apply to all faxes sent from Business Name or any remote site used by employees:

1. Management authorization is required prior to the fax transmission of confidential information that falls outside of the employee’s normal job functions. Employees are responsible to ensure non-public information is shared with others on a “need to know basis”. When possible, non-public information should be de-identified prior to transmission.
2. Cover sheets should be used to facilitate delivery of document(s) to the intended receiver. The fax cover sheet should include the following items: recipient’s name, sender name and telephone number, date and time, description of the document, number of pages, and name, phone and fax number of the recipient.
3. The fax cover sheet must include the following confidentiality statement:

“This message is intended only for the use of the individual to whom, or entity to which, it is addressed and may contain information that is privileged, confidential, or exempt from disclosure under applicable law.

If the reader of this message is not the intended recipient or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is prohibited. If you have received this communication in error, please notify us immediately by telephone.”

1. Take reasonable steps to ensure the fax is sent to the appropriate destination. Pre-program and test destination numbers whenever possible to eliminate errors in transmission from misdialing. Confirm with recipients the correct fax number. Regularly confirm that programming is correct by checking confirmation sheets for accuracy.
2. When possible, the sender should schedule to send a confidential fax to the recipient at a time when it can be immediately retrieved.
3. Should you become aware that a fax with confidential information was sent to an incorrect recipient, contact the recipient and ask that the material be returned or destroyed.

## **Data Labeling**

*The following section is overkill for most organizations, large and small. But the purpose of data labeling should still be understood. Very often we can accidentally leak confidential data because we don’t realize it is confidential. While this should not be the case for Nonpublic Information (NPI), Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI),**and other regulated information, it is often the case for information that small businesses want kept confidential such as Owner Names, Vendors and Suppliers, etc. If we don’t tell our employees to keep owner names confidential, they may hand this information out to anybody that asks.*

All documents are to be labeled as per the Data Ownership Policy. Specified classifications are used to gauge information value or sensitivity. Designed classifications include: Critical, Confidential, Internal Use, and Unrestricted/Public. Employees are to use care in handling information based on these classifications.

## **Copy Machine Policy**

The copy machine[s] in our office [is] [are] intended for professional use only.

## **Telephone Policy**

Long distance calls for personal reasons are prohibited unless there is an emergency need.

## **Mandatory Vacations**

The following vacation policy should be implemented as a detective control. It may ALREADY be addressed in the Personnel Manual.

All employees are required to take vacations in one- or two-week increments. During their absence, another individual will perform that job and a discovery audit may take place to ensure that no irregular or illegal acts have been committed by the employee.

## **Background Checks**

The following background check policy should be implemented as a detective control. It may already be addressed in the Personnel Manual.

The business conducts ongoing background tests for many current employees on a random basis. Continued employment is contingent upon successful completion of an ongoing background check with considerations made for extenuating circumstances. In order to avoid embarrassing situations, employees are [required / strongly encouraged] to inform their supervisor and/or human resources in the event that something negative happens which could affect the results of a random background check.

## **Subsequent Criminal Convictions**

The following criminal conviction policy should be implemented as a detective control. It may already be addressed in the Personnel Manual.

In the event that an employee subject to this policy receives a criminal conviction after successful completion of the initial background check, that employee [should / must] inform the [Human Resources Department / Owner**]** in order to determine whether or not the conviction is relevant to his/her job under this policy. Employees who fail to notify the [Human Resources Department / Owner**]** about a “subsequent criminal conviction” that proves to be relevant to their job may be terminated for cause.

## **Termination**

Upon termination of employment, you must surrender all property and information owned by Business Name as per this policy. All provisions of this policy apply to and remain in force in the event of termination until such surrender is made. Furthermore, this policy survives the terminated relationship.

## **Security Awareness Training and Comprehension Testing**

All employees are required to attend annual Security Awareness Training as provided by [the Information Security Officer / the Network Administrator / the President / an approved Security Consultancy vendor] and based on this Acceptable Use Policy. Upon completion of the training, employees are required to take an AUP Comprehension Test and pass the test with a score of 100%. Completed tests will be stored in the employees’ personnel files.

## **Policy Violation Reporting**

Discuss your procedure for reporting suspicious activity, offensive materials, or other policy violations. Include who, what, when, where and how.

## **[Network Administrator / IT Manager / Owner]s**

For the purposes of this policy, existing [Network Administrator / IT Manager / Owner]s include:

* List all [Network Administrator / IT Manager / Owner]s

## **Concluding Sections**

*The following sections may or may not apply to your institution, depending upon your own policy/procedure development protocols. However, we do strongly urge you to include the distribution list, policy owner, and policy reviewers sections for your convenience and to ensure appropriate review and training. Please remove this section.*

## **Reporting to the Owners**

The [Information Security Officer / Network Administrator / President / Internal Auditor] will report to the Owners on an annual basis that all policies listed above have been reviewed for completion, enforcement, and training. Specifically, this report will indicate that all policies listed above have been updated. The report will list deficiencies related to enforcement of the policies, as well as indicate the level of training provided to members of the various teams affected by the policies.

The Owners will also receive summary reports of examinations, audits, and other assessments of the risk inherent in information security as they are required.

## **Noncompliance**

Violation of these policies may result in disciplinary action which may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Business Name’s information resources access privileges, and civil and/or criminal prosecution.

## **Storage of Policies, Procedures and Standards**

The [Information Security Officer / Network Administrator / President / Owner] is responsible for maintaining current copies of all information security related policies and procedures. These will be stored [state method and location] and an electronic copy will be stored off-site [state location]. The electronic copy will be updated annually (in December) as well as on an as-needed basis any time there is a major revision of a particular policy or procedure.

## **Distribution List**

The following positions will receive this policy and any changes to this policy:

* All employees

## **Policy Owner**

* Title Here

## **Policy Reviewers**

* Owners
* List others here

## **Revision History**

Note: This next section is optional, used to keep track of when you’ve updated policies and procedures. Know that using this will make it very clear to an Auditor when you skipped a revision cycle.

The following revisions were made to this document:

• 02/11/11: Document created.

• 02/23/12 John Doe [Information Security Officer / Network Administrator / President / Owner]

## **Declaration**

I have received a copy of the Acceptable Use Policy from Business Name. I understand that, as an employee of Business Name, I am to adhere to the standards as described within the Policy. I also understand that any violation of this Policy can lead to disciplinary action, up to and including dismissal.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Network Administrator / IT Manager / Human Resources Director / Owner] Date