Corporate Ethics & Securities Policies

Maple Technologies®
A Limited Liability Company

...building technology Solutions to grow your business...

ASPIRE®
Information Systems

500 Craig Road, 2nd Floor, Manalapan, NJ 07726 | Tel: (732) 863-5523 | www.maple-tech.com

V.2016.01

1. Maple Technologies' purpose for this ethics policy is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every Maple Technologies employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

   Maple Technologies is committed to protecting employees, partners, customers, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When Maple Technologies addresses issues proactively and uses correct judgment, it will help set us apart from competitors

   Maple Technologies will not tolerate any wrongdoing or impropriety at anytime. Maple Technologies will take the appropriate measures act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

2. **Purpose**
   Our purpose for authoring a publication on ethics is to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct.

3. **Scope**
   This policy applies to employees, contractors, consultants, temporaries, and other workers at Maple Technologies, including all personnel affiliated with third parties.

4. **Policy**

4.1. Executive Commitment to Ethics

4.1.1. Executive Officers within Maple Technologies must set a prime example. In any business practice, honesty and integrity must be top priority for executives.

4.1.2. Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.

4.1.3. Executives must disclose any conflict of interests regarding their position within Maple Technologies.

4.2. Employee Commitment to Ethics

4.2.1. Maple Technologies employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of

unethical or compromising practices.

4.2.2. Every employee needs to apply effort and intelligence in maintaining ethics value.

4.2.3. Employees must disclose any conflict of interests with regard to their position within Maple Technologies.

4.2.4. Employees will help Maple Technologies to increase customer and vendor satisfaction by providing quality products and timely response to inquiries.

4.3. Company Awareness

4.3.1. Promotion of ethical conduct with interpersonal communications of employees will be rewarded.

4.3.2. Maple Technologies will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

4.4. Maintaining Ethical Practices

4.4.1. Maple Technologies will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs to consistently maintain an ethical stance and support ethical behavior.

4.4.2. Employees at Maple Technologies should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

4.4.3. Maple Technologies has established a best practices disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Maple Technologies without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and/or video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Maple Technologies Confidential information (e.g., Maple Technologies Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Corporate Information Security.

2.0 Scope

All Maple Technologies information is categorized into two main classifications:

- Maple Technologies Public
- Maple Technologies Confidential

Maple Technologies Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Maple Technologies.

Maple Technologies Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in Maple Technologies Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of Maple Technologies Confidential information is "Maple Technologies Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation, which has been entrusted to Maple Technologies by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and customer information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Maple Technologies' network to support our operations.

Maple Technologies personnel are encouraged to use common sense judgment in securing Maple Technologies Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager.

3.0 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Maple Technologies Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the Maple Technologies Confidential information in question.

3.1 **Minimal Sensitivity:** General corporate information; some personnel and technical information; Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Maple Technologies Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "Maple Technologies Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, Maple Technologies information is presumed to be "Maple Technologies Confidential" unless expressly determined to be Maple Technologies Public information by a Maple Technologies employee with authority to do so.

Access:

Maple Technologies employees, contractors, people with a business need to know.

Distribution within Maple Technologies:

Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of Maple Technologies internal mail:

U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it be sent to only approved recipients.

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on Maple Technologies premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.2 **More Sensitive:** Business, financial, technical, and most personnel information.

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "Maple Technologies Confidential" or "Maple Technologies Proprietary", wish to label the information "Maple Technologies Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: Maple Technologies employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution within Maple Technologies: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of Maple Technologies internal mail: Sent via U.S. mail or approved private carriers.

Electronic distribution: No restrictions to approved recipients within Maple Technologies, but should be encrypted or sent via a private link to approved recipients outside of Maple Technologies premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In specially marked disposal bins on Maple Technologies premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.3 **Most Sensitive:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Maple Technologies Confidential information is very sensitive, you may should label the information "Maple Technologies Internal: Registered and Restricted", "Maple Technologies Eyes Only", "Maple Technologies Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Maple Technologies Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (Maple Technologies employees and non-employees) designated with approved access and signed non-disclosure agreements.

Distribution within Maple Technologies: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of Maple Technologies internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restrictions to approved recipients within Maple Technologies, but it is highly recommended that all information be strongly encrypted.

Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on Maple Technologies premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms and Definitions

Appropriate measures

To minimize risk to Maple Technologies from an outside business connection, Maple Technologies computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Maple Technologies corporate information, the amount of information at risk is minimized.

Configuration of Maple Technologies-to-other business connections

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required

Do not leave in interoffice mail slot; call the mailroom for special pick-up of mail.

Approved Electronic File Transmission Methods

Includes supported FTP clients and Web browsers.

Envelops Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team.

Approved Encrypted email and files

Techniques include the use of AES and PGP. AES encryption is available via many different public domain packages on all platforms. PGP use within Maple Technologies is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources

Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge

To reliably erase, expunge or sanitize data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Maple Technologies.

Encryption

Secure Maple Technologies Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication

One Time Password Authentication on Internet connections is accomplished by using a one-time password token to connect to Maple Technologies 's internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that Maple Technologies has control over its entire distance. For example, all Maple Technologies networks are connected via a private link. A computer with modem connected via a standard landline (not cell phone) to another computer has established a private link. ISDN lines to employee's homes is a private link. Maple Technologies also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies, which Maple Technologies has established private links include all

announced acquisitions and some short-term temporary links.

6.0 Revision History

03-01-2007, 03-12-2016 General Revisions to Document

1.0 Purpose

To empower Corporate Information Security to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

2.0 Scope

Risk assessments can be conducted on any entity within Maple Technologies or any outside entity that has signed a *Third Party Agreement* with Maple Technologies. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3.0 Policy

The execution, development and implementation of remediation programs is the joint responsibility of Corporate Information Security and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Corporate Information Security Risk Assessment Team in the development of a remediation plan.

4.0 Risk Assessment Process

For additional information, go to the Risk Assessment Process.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms	Definitions
Entity	Any business unit, department, group, or third party, internal or external to Maple Technologies, responsible for maintaining Maple Technologies assets.
Risk	Those factors that could affect confidentiality, availability, and integrity of Maple Technologies 's key information assets and systems. Corporate Information Security is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

7.0 Revision History

03-01-2007 General Revisions to Document

1.0 Purpose

To establish Corporate Information Security responsibilities regarding corporate acquisitions, and define the minimum-security requirements of a Corporate Information Security acquisition assessment.

2.0 Scope

This policy applies to all companies acquired by Maple Technologies and pertains to all systems, networks, laboratories, test equipment, hardware, software and firmware, owned and/or operated by the acquired company.

3.0 Policy

I. General

Acquisition assessments are conducted to ensure that a company being acquired by Maple Technologies does not pose a security risk to corporate networks, internal systems, and/or confidential/sensitive information. Corporate Information Security will provide personnel to serve as active members of the acquisition team throughout the acquisition process. The Corporate Information Security role is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work with the acquisitions team to implement solutions for any identified security risks, prior to allowing connectivity to Maple Technologies 's networks. Below are the minimum requirements that the acquired company must meet before being connected to the Maple Technologies network.

II. Requirements

A. Hosts

- All hosts (servers, desktops, laptops) will be replaced or re-imaged with a Maple Technologies standard image.
- Business critical production servers that cannot be replaced or re-imaged must be audited and a waiver granted by Corporate Information Security.
- All PC based hosts will require Maple Technologies approved virus protection before the network connection.

B. Networks

1. All network devices will be replaced or re-imaged with a Maple Technologies standard image.
2. Wireless network access points will be configured to the Maple Technologies standard.

C. Internet

1. All Internet connections will be terminated.
2. When justified by business requirements, air-gapped Internet connections require Corporate Information Security review and approval.

D. Remote Access

1. All remote access connections will be terminated.
2. Maple Technologies will provide remote access to the production network.

E. Labs

1. Lab equipment must be physically separated and secured from non-lab areas.

2. The lab network must be separated from the corporate production network with a firewall between the two networks.
3. Any direct network connections (including analog lines, ISDN lines, T1, etc.) to external customers, partners, etc., must be reviewed and approved by the Lab Security Group (LabSec).
4. All acquired labs must meet with LabSec lab policy, or be granted a waiver by LabSec. A server that is critic
5. In the event the acquired networks and computer systems being connected to the corporate network fail to meet these requirements, the Maple Technologies Chief Technology Officer (CTO) must acknowledge and approve of the risk to Maple Technologies' networks.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	Definitions
	Business Critical Production Server: A Server that is critical to the continued business operations of the acquired Company.

6.0 Revision History

03-01-2007 General Revisions to Document

Corporate Information Security Acceptable Use Policy

Section 5

1.0 Overview

Corporate Information Security's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Maple Technologies' established culture of openness, trust and integrity. Corporate Information Security is committed to protecting Maple Technologies employees, customers, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet / Intranet / Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Maple Technologies. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Maple Technologies employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Maple Technologies. These rules are in place to protect the employee and Maple Technologies. Inappropriate use exposes Maple Technologies to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Maple Technologies, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Maple Technologies.

4.0 Policy

4.1 General Use and Ownership

- While Maple Technologies' network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Maple Technologies. Because of the need to protect Maple Technologies' network, management cannot guarantee the confidentiality of information stored on any network device belonging to Maple Technologies.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet / Intranet / Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- Corporate Information Security recommends that any information that

users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Corporate Information Security's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to Corporate Information Security's Awareness Initiative.

- For security and network maintenance purposes, authorized individuals within Maple Technologies may monitor equipment, systems and network traffic at any time, per Corporate Information Security's Audit Policy.
- Maple Technologies reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

- The user interface for information contained on Internet / Intranet / Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed at least monthly; user level passwords should be changed at least every 90 days.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Windows users) when the host will be unattended.
- Use encryption of information in compliance with Corporate Information Security's Acceptable Encryption Use policy.
- Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips”.
- Postings by employees from a Maple Technologies email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Maple Technologies, unless posting is in the course of business duties.
- All hosts used by the employee that are connected to the Maple Technologies Internet / Intranet / Extranet, whether owned by the employee or Maple Technologies, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Maple Technologies authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Maple Technologies -owned resources.

The lists below are by no means exhaustive, but an attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Maple Technologies.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Maple Technologies or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Maple Technologies computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Maple Technologies account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods,

packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited unless prior notification to Corporate Information Security is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet / Intranet / Extranet.
- Providing information about, or lists of, Maple Technologies employees to parties outside Maple Technologies.

Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Maple Technologies 's networks of other Internet / Intranet / Extranet service providers on behalf of, or to advertise, any service hosted by Maple Technologies or connected via Maple Technologies 's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History

03-01-2007, 10-12-2016 General Revisions to Document

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Maple Technologies' entire corporate network. As such, all Maple Technologies employees (including contractors and vendors with access to Maple Technologies systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Maple Technologies facilities, has access to the Maple Technologies network, or stores any non-public Maple Technologies information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a monthly basis.
- All production system-level passwords must be part of the Corporate Information Security administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at Maple Technologies. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Maple Technologies", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for Maple Technologies accounts as for other non-Maple Technologies access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Maple Technologies access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Maple Technologies passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Maple Technologies information.

Here is a list of "don’ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others

- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Corporate Information Security Department.

Do not use the "Remember Password" feature of applications.

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system or electronic devices without encryption.

Change passwords at least once every 90 days (except system-level passwords which must be changed monthly).

If an account or password is suspected to have been compromised, report the incident to Corporate Information Security and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by Corporate Information Security or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards
Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users
Access to the Maple Technologies Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases
Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"
All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms	Definitions
	Application Administration Account: Any account that is for the administration of an application (e.g., SQL database administrator, ISSU administrator).

7.0 Revision History

03-01-2007, 10-12-2016 General Revisions to Document

1.0 Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Maple Technologies 's networks.

Computer programs running on Maple Technologies' networks often require the use of one of the many internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

2.0 Scope

This policy applies to all software that will access a Maple Technologies, multi-user production database.

3.0 Policy

3.1 General

In order to maintain the security of Maple Technologies 's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

3.2 Specific Requirements

3.2.1. Storage of Data Base User Names and Passwords

- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be word readable.
- Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials may not reside in the documents tree of a web server.
- Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database must adhere to the *Password Policy*.

3.2.2. Retrieval of Database User Names and Passwords

o If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the

memory containing the user name and password must be released or cleared.
o The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

o For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

3. Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the *Password Policy*.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
Computer language	A language used to generate programs.
Credentials	Something you know (e.g., a password or pass phrase), and/or something that identifies you (e.g., a user name, a fingerprint, voiceprint, retina print). Something you know and something that identifies you are presented for authentication.
Entitlement	The level of privilege that has been authenticated and authorized. The privileges level at which to access resources.
Executing body	The series of computer instructions that the computer executes to run a program.
Hash	An algorithmically generated number that identifies a datum or its location.
LDAP	Lightweight Directory Access Protocol, a set of protocols for accessing information directories.

Module	A collection of computer language instructions grouped together either logically or physically. A module may also be called a package or a class, depending upon which computer language is used.
Name space	A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.
Production	Software that is being used for a purpose other than when software is being implemented or tested.

6.0 Revision History

03-01-2007 General Revisions to Document

1.0 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

2.0 Scope

This policy applies to all Maple Technologies employees and affiliates.

3.0 Policy

Proven, standard algorithms such as AES, Blowfish, RSA, RC5, RC6 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Maple Technologies 's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Corporate Information Security. Be aware that the U.S. Government restricts the export of encryption technologies. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys is used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

6.0 Revision History

03-01-2007, 10-12-2016 General Revisions to Document

1.0 Purpose
This policy establishes information security requirements for Maple Technologies' labs to ensure that Maple Technologies' confidential information and technologies are not compromised, and that production services and other Maple Technologies interests are protected from lab activities.

2.0 Scope
This policy applies to all internally connected labs, Maple Technologies employees and third parties who access Maple Technologies' labs. All existing and future equipment, which fall under the scope of this policy, must be configured according to the referenced documents. DMZ Labs and stand-alone, air-gapped labs are exempt from this policy. DMZ labs must comply with the *DMZ Lab Security Policy*.

3.0 Policy

3.1 Ownership Responsibilities
1. Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with Corporate Information Security and the Corporate Enterprise Management Team. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.

2. Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard Maple Technologies from security vulnerabilities.

3. Lab managers are responsible for the lab's compliance with all Maple Technologies security policies. The following are particularly important:

> *Password Policy for networking devices and hosts, Wireless Security Policy, Anti-Virus Policy, and physical security*.

4. The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.

5. The Network Support Organization must maintain a firewall device between the corporate production network and all lab equipment.

6. The Network Support Organization and/or Corporate Information Security reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.

7. The Network Support Organization must record all lab IP addresses, which are routed

within Maple Technologies networks, in an Enterprise Address Management database along with current contact information for that lab.

8. Any lab that wants to add an external connection must provide a diagram and documentation to Corporate Information Security with business justification, the equipment, and the IP address space information. Corporate Information Security will review for security concerns and must approve before such connections are implemented.

9. All user passwords must comply with Maple Technologies' *Password Policy*. In addition, individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, Windows, etc) must be changed quarterly (once every 3 months). For any lab device that contains Maple Technologies proprietary information, group account passwords must be changed within three (3) days following a change in-group membership.
10. No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a Corporate Enterprise organization.

11. Corporate Information Security will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.2 General Configuration Requirements
1. All traffic between the corporate production and the lab network must go through a Network Support Organization maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.

2. Original firewall configurations and any changes thereto must be reviewed and approved by Corporate Information Security. Corporate Information Security may require security improvements as needed.

3. Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-Maple Technologies networks. These activities must be restricted within the lab.

4. Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.
5. Corporate Information Security reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.

6. Lab owned gateway devices are required to comply with all Maple Technologies product security advisories and must authenticate against the Corporate Authentication servers.

7. The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with Maple Technologies' Password *Policy*. The password

will only be provided to those who are authorized to administer the lab network.

8. In labs where non-Maple Technologies personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no Maple Technologies confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network only if authenticated against the Corporate Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by Corporate Information Security.

9. Infrastructure devices (e.g. IP Phones) needing corporate network connectivity must adhere to the *Open Areas Policy.*

10. All lab external connection requests must be reviewed and approved by Corporate Information Security. Analog or ISDN lines must be configured to only accept trusted call numbers. Strong passwords must be used for authentication.

11. All labs networks with external connections must not be connected to Maple Technologies corporate production network or any other internal network directly or via a wireless connection, or via any other form of computing equipment. A waiver from Corporate Information Security is required where air-gapping is not possible (e.g., Partner Connections to third party networks).

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Internal — A lab that is within Maple Technologies' corporate firewall and connected to Maple Technologies' corporate production network.

Network Support Organization - Any Corporate Information Security approved Maple Technologies support organization that manages the networking of non-lab networks.

Lab Manager — The individual responsible for all lab activities and personnel

Lab — A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.

External Connections (also known as DMZ) — External connections include (but not limited to) third-party data network-to-network, analog and ISDN data lines, or any other Telco data lines.

Lab Owned Gateway Device — A lab owned gateway device is the lab device that connects the lab network to the rest of Maple Technologies network. All traffic between the lab and the corporate production network must pass through the lab owned gateway device unless approved by Corporate Information Security.

Telco	A Telco is the equivalent to a service provider. Telcos offer network connectivity, e.g., T1, T3, OC3, OC12 or DSL. Telcos are sometimes referred to as "baby bells", although Sprint and AT&T are also considered Telcos. Telco interfaces include BRI, or Basic Rate Interface - a structure commonly used for ISDN service, and PRI, Primary Rate Interface - a structure for voice/dial-up service.
Traffic	Mass volume of unauthorized and/or unsolicited network Spamming/Flooding traffic.
Firewall	A device that controls access between networks. It can be a PIX, a router with access control lists or similar security devices approved by Corporate Information Security.
Extranet	Connections between third parties that require access to connections non-public Maple Technologies resources, as defined in Corporate Information Security's Extranet policy (link).
DMZ (De-Militarized Zone)	This describes network that exists outside of primary corporate firewalls, but are still under Maple Technologies administrative control.

6.0 Revision History

03-01-2007 General Revisions to Document

Guidelines on Anti-Virus Process

Section 10

Recommended processes to prevent virus problems:

1. Always run the corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
2. NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
3. Delete spam, chain, and other junk email without forwarding, in accordance with Maple Technologies' *Acceptable Use Policy*.
4. Never download files from unknown or suspicious sources.
5. Avoid direct disk sharing with read/write access unless there is an absolute business requirement to do so.
6. Always scan a storage device (e.g. flash drive, external hard disk, CD, etc.) from an unknown source for viruses before using it.
7. Back-up critical data and system configurations on a regular basis and store the data in a safe place.
8. If lab-testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
9. New viruses are discovered almost every day. Periodically check the *Lab Anti-Virus Policy* and this Recommended Processes list for updates.

Revision History

03-01-2007, 10-12-2016 General Revisions to Document

1.0 Purpose
The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Maple Technologies. Effective implementation of this policy will minimize unauthorized access to Maple Technologies proprietary information and technology.

2.0 Scope
This policy applies to server equipment owned and/or operated by Maple Technologies, and to servers registered under any Maple Technologies -owned internal network domain.

This policy is specifically for equipment on the internal Maple Technologies network. For secure configuration of equipment external to Maple Technologies on the DMZ, refer to the *Internet DMZ Equipment Policy*.

3.0 Policy

3.1 Ownership and Responsibilities
An operational group that is responsible for system administration must own all internal servers deployed at Maple Technologies. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Corporate Information Security. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Corporate Information Security.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines
- Operating System configuration should be in accordance with approved Corporate Information Security guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should

be avoided. Do not use a trust relationship when some other method of communication will do.

- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using TLS, SSL, SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - All security related logs will be kept online for a minimum of 1 week.
  - Daily incremental tape backups will be retained for at least 1 month.
  - Weekly full tape backups of logs will be retained for at least 1 month.
  - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to Corporate Information Security, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within Maple Technologies.
- The internal audit group or Corporate Information Security, in accordance with the Audit Policy, will manage audits. Corporate Information Security will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
DMZ	De-militarized Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal Maple Technologies Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History	03-01-2007, 10-12-2016 General Revisions to Document

1.0 Purpose
To establish requirements, which must be met by all computers, connected to Maple Technologies lab networks to ensure effective virus detection and prevention.

2.0 Scope
This policy applies to all Maple Technologies lab computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers, and any PC based lab equipment such as traffic generators.

3.0 Policy
All Maple Technologies PC-based lab computers must have Maple Technologies' standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Lab Admins / Lab Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into Maple Technologies' networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

Refer to Maple Technologies' *Anti-Virus Recommended Processes* to help prevent virus problems.

Noted exceptions: Machines with operating systems other than those based on Microsoft products are excepted at the current time.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History
03-01-2007 General Revisions to Document.

1.0 Purpose

This policy establishes information security requirements for all networks and equipment deployed in Maple Technologies' labs located on the "De-Militarized Zone" (DMZ). Adherence to these requirements will minimize the potential risk to Maple Technologies from the damage to public image caused by unauthorized use of Maple Technologies resources, and the loss of sensitive/company confidential data and intellectual property.

2.0 Scope

Maple Technologies Lab networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located outside Maple Technologies' corporate Internet firewalls are considered part of the DMZ Labs and are subject to this policy. This includes DMZ Labs in primary Internet Service Provider (ISP) locations and remote locations. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents. This policy does not apply to labs residing inside Maple Technologies' corporate Internet firewalls. Standards for these labs are defined in the *Internal Lab Security Policy*

3.0 Policy

3.1. Ownership and Responsibilities

- All new DMZ Labs must present a business justification with sign-off at the business unit Senior Officer level. Corporate Information Security must keep the business justifications on file.
- Lab owning organizations are responsible for assigning lab managers, point of contact (POC) and back up POC for each lab. The lab owners must maintain up to date POC information with Corporate Information Security. Lab managers or their backup must be available around-the-clock for emergencies.
- Changes to the connectivity and/or purpose of existing DMZ Labs and establishment of new DMZ Labs must be requested through a Maple Technologies Network Support Organization and approved by Corporate Information Security.
- A Maple Technologies Network Support Organization must maintain all ISP connections.
- A Network Support Organization must maintain a firewall device between the DMZ Lab(s) and the Internet.
- The Network Support Organization and Corporate Information Security reserve the right to interrupt lab connections if a security concern exists.
- The DMZ Lab will provide and maintain network devices deployed in the DMZ Lab up to the Network Support Organization point of demarcation.
- The Network Support Organization must record all DMZ Lab address spaces and current contact information.
- The DMZ Lab Managers are ultimately responsible for their DMZ Labs complying with this policy.
- Immediate access to equipment and system logs must be granted to members of Corporate Information Security and the Network Support

Organization upon request, in accordance with the *Audit Policy*

- Individual lab accounts must be deleted within three (3) days when access is no longer authorized. Group account passwords must comply with the *Password Policy* and must be changed within three (3) days from a change in the group membership.
- Corporate Information Security will address non-compliance waiver requests on a case-by-case basis.

3.2. General Configuration Requirements

1. Production resources must not depend upon resources on the DMZ Lab networks.
2. DMZ Labs must not be connected to Maple Technologies 's corporate internal networks, either directly or via a wireless connection.
3. DMZ Labs should be in a physically separate room from any internal networks. If this is not possible, the equipment must be in a locked rack with limited access. In addition, the Lab Manager must maintain a list of who has access to the equipment.
4. Lab Managers are responsible for complying with the following related policies:
    - *Password Policy*
    - *Wireless Communications Policy*
    - *Lab Anti-Virus Policy*
5. The Network Support Organization maintained firewall devices must be configured in accordance with least-access principles and the DMZ Lab business needs. Corporate Information Security will maintain all firewall filters.
6. The firewall device must be the only access point between the DMZ Lab and the rest of Maple Technologies' networks and/or the Internet. Any form of cross-connection, which bypasses the firewall device, is strictly prohibited.
7. Original firewall configurations and any changes thereto must be reviewed and approved by Corporate Information Security (including both general configurations and rule sets). Corporate Information Security may require additional security measures as needed.
8. Traffic from DMZ Labs to the Maple Technologies' internal network, including VPN access, falls under the *Remote Access Policy*
9. All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.
10. Operating systems of all hosts internal to the DMZ Lab running Internet Services must be configured to the secure host installation and configuration standards. [Add URL link to site where your internal configuration standards are kept].
11. Current applicable security patches/hot-fixes for any applications that are Internet services must be applied. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
12. All applicable security patches/hot-fixes recommended by the vendor must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.

13. Services and applications not serving business requirements must be disabled.
14. Maple Technologies Confidential information is prohibited on equipment in labs where non-Maple Technologies personnel have physical access (e.g., training labs), in accordance with the *Information Sensitivity Classification Policy*
15. Remote administration must be performed over secure channels (e.g., encrypted network connections using TLS, SSL, SSH or IPSEC) or console access independent from the DMZ networks.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
Access Control List (ACL)	Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
DMZ	Networking that exists outside of Maple Technologies primary corporate firewalls, but is still under Maple Technologies administrative control.
Network Support Organization	Any Corporate Information Security-approved support organization that manages the networking of non-lab networks.
Least Access Principle	Access to services, hosts, and networks is restricted unless otherwise permitted.
Internet Services	Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc.
Network Support Organization	The point at which the networking responsibility transfers from a Point of Demarcation Network Support Organization to the DMZ Lab. Usually a router or firewall.
Lab Manager	The individual responsible for all lab activities and personnel.
Lab	A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.
Firewall	A device that controls access between networks., such as a PIX, a router with access control lists, or a similar security device approved by Corporate Information Security.

Internally Connected Lab

A lab within Maple Technologies' corporate firewall and connected to the corporate production network.

6.0 Revision History

03-01-2007, 10-12-2016 General Revisions to Document

1.0 Purpose
The purpose of this policy is to define standards to be met by all equipment owned and/or operated by Maple Technologies located outside Maple Technologies' corporate Internet firewalls. These standards are designed to minimize the potential exposure to Maple Technologies from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of Maple Technologies resources.

Devices that are Internet facing and outside the Maple Technologies firewall are considered part of the "de-militarized zone" (DMZ) and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside outside the corporate firewalls.

The policy defines the following standards:

1. Ownership responsibility
2. Secure configuration requirements
3. Operational requirements
4. Change control requirement

2.0 Scope
All equipment or devices deployed in a DMZ owned and/or operated by Maple Technologies (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by Maple Technologies, must follow this policy.

This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "Maple Technologies .com" domain or appears to be owned by Maple Technologies.

All new equipment, which falls under the scope of this policy, must be configured according to the referenced configuration documents, unless a waiver is obtained from Corporate Information Security. All existing and future equipment deployed on Maple Technologies 's un-trusted networks must comply with this policy.

3.0 Policy

3.1. Ownership and Responsibilities
Equipment and applications within the scope of this policy must be administered by support groups approved by Corporate Information Security for the DMZ system, application, and/or network management.

Support groups will be responsible for the following:

- Equipment must be documented in the corporate wide enterprise management system. At a minimum, the following information is required:
  - Host contacts and location.
  - Hardware and operating system/version.
  - Main functions and applications.
  - Password groups for privileged passwords.
- Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).

- Password groups must be maintained in accordance with the corporate wide password management system / process.
- Immediate access to equipment and system logs must be granted to members of Corporate Information Security upon demand, per the *Audit Policy*.
- Changes to existing equipment and deployment of new equipment must follow and corporate governess or change management processes / procedures.

To verify compliance with this policy, Corporate Information Security will periodically audit DMZ equipment per the *Audit Policy*.

3.2. General Configuration Policy

All equipment must comply with the following configuration policy:

- Corporate Information Security as part of the pre-deployment review phase must approve hardware, operating systems, services and applications.
- Operating system configuration must be done according to the secure host and router installation and configuration standards.
- All patches/hot-fixes recommended by the equipment vendor and Corporate Information Security must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
- Services and applications not serving business requirements must be disabled.
- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by Corporate Information Security.
- Access control lists must restrict services and applications not for general access.
- Insecure services or protocols (as determined by Corporate Information Security) must be replaced with more secure equivalents whenever such exist.
- Remote administration must be performed over secure channels (e.g., encrypted network connections using TLS, SSL, SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords (DES/SofToken) must be used for all access levels.
- All host content updates must occur over secure channels.
- Security-related events must be logged and audit trails saved to Corporate Information Security-approved logs. Security-related events include (but are not limited to) the following:
    - User login failures.
    - Failure to obtain privileged access.
    - Access policy violations.
- Corporate Information Security will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.3. New Installations and Change Management Procedures

All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- New installations must be done via the *DMZ Equipment Deployment Process*.
- Configuration changes must follow the Corporate Change Management (CM) Procedures.
- Corporate Information Security must be invited to perform system/application audits prior to the deployment of new services.
- Corporate Information Security must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

3.4. Equipment Outsourced to External Service Providers

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

5.0 Definitions

Terms	Definitions
DMZ	Any un-trusted network connected to, but separated from, Maple Technologies 's corporate network by a firewall, used for external (Internet/partner, etc.) access from within Maple Technologies , or to provide information to external parties. Only DMZ networks connecting to the Internet fall under the scope of this policy.
Secure Channel	Out-of-band console management or channels using strong encryption according to the *Acceptable Encryption Policy*. Non-encrypted channels must use strong user authentication (one-time passwords).
Un-Trusted Network	Any network firewalled off from the corporate network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet etc.), or anything else identified as a potential threat to those resources.

6.0 Revision History

03-01-2007, 10-12-2016 General Revisions to Document

1.0 Purpose
This document describes the policy under which third party organizations connect to Maple Technologies networks for the purpose of transacting business related to Maple Technologies.

2.0 Scope
Connections between third parties that require access to non-public Maple Technologies resources fall under this policy, regardless of whether a telco circuit (such as frame relay or ISDN) or VPN technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for Maple Technologies or to the Public Switched Telephone Network does NOT fall under this policy.

3.0 Policy

3.1 Pre-Requisites

3.1.1 Security Review
All new extranet connectivity will go through a security review with the Information Security department (Corporate Information Security). The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

3.1.2 Third Party Connection Agreement
All new connection requests between third parties and Maple Technologies require that the third party and Maple Technologies representatives agree to and sign the *Third Party Agreement*. This agreement must be signed by an authorized officer of the Sponsoring Organization as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the relevant extranet group. Documents pertaining to connections into Maple Technologies labs are to be kept on file with Corporate Information Security.

3.1.3 Business Case
All production extranet connections must be accompanied by a valid business justification, in writing, that is approved by a project manager in the extranet group. Corporate Information Security must approve lab connections. Typically this function is handled as part of the *Third Party Agreement*.

3.1.4 Point Of Contact
The Sponsoring Organization must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the Sponsoring Organization, and is responsible for those portions of this policy and the *Third Party Agreement* that pertain to it. In the event that the POC changes, the relevant extranet Organization must be informed promptly.

3.2 Establishing Connectivity
Sponsoring Organizations within Maple Technologies that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage Corporate Information Security to address security issues inherent in the project. If the proposed connection is to terminate within a lab at Maple Technologies, the Sponsoring Organization must engage

Corporate Information Security. The Sponsoring Organization must provide full and complete information as to the nature of the proposed access to the extranet group and Corporate Information Security, as requested.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will Maple Technologies rely upon the third party to protect Maple Technologies 's network or resources.

3.3 Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The Sponsoring Organization is responsible for notifying the extranet management group and/or Corporate Information Security when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

3.4 Terminating Access

When access is no longer required, the Sponsoring Organization within Maple Technologies must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. The extranet and lab security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct Maple Technologies business, will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct Maple Technologies business necessitates a modification of existing permissions, or termination of connectivity, Corporate Information Security and/or the extranet team will notify the POC or the Sponsoring Organization of the change prior to taking any action.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
Circuit	For the purposes of this policy, circuit refers to the method of network access, whether it's through traditional ISDN, Frame Relay etc., or via VPN/Encryption technologies.
Sponsoring Organization	The Maple Technologies organization who requested that the third party have access into Maple Technologies.
Third Party	A business that is not a formal or subsidiary part of Maple Technologies.

6.0 Revision History

03-01-2007 General Revisions to Document

Virtual Private Network (VPN) Policy

Section 16

1.0 Purpose

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Maple Technologies corporate network.

2.0 Scope

This policy applies to all Maple Technologies employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Maple Technologies network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

3.0 Policy

Approved Maple Technologies employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

Additionally,

- It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Maple Technologies internal networks.
- VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
- Dual (split) tunneling is NOT permitted; only one network connection is allowed.
- VPN gateways will be set up and managed by Maple Technologies network operational groups.
- All computers connected to Maple Technologies internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
- VPN users will be automatically disconnected from Maple Technologies 's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- The VPN concentrator is limited to an absolute connection time of 24 hours.
- Users of computers that are not Maple Technologies -owned equipment must configure the equipment to comply with Maple Technologies 's VPN and Network policies.
- Only Corporate Information Security-approved VPN clients may be used.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Maple Technologies 's network, and

as such are subject to the same rules and regulations that apply to Maple Technologies -owned equipment, i.e., their machines must be configured to comply with Corporate Information Security's Security Policies.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
IPSec Concentrator	A device in which VPN connections are terminated.

6.0 Revision History

03-01-2007 General Revisions to Document

1.0 Purpose

The purpose of this policy is to define standards for connecting to Maple Technologies 's network from any host. These standards are designed to minimize the potential exposure to Maple Technologies from damages which may result from unauthorized use of Maple Technologies resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Maple Technologies internal systems, etc.

2.0 Scope

This policy applies to all Maple Technologies employees, contractors, vendors and agents with a Maple Technologies -owned or personally-owned computer or workstation used to connect to the Maple Technologies network. This policy applies to remote access connections used to do work on behalf of Maple Technologies, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

- It is the responsibility of Maple Technologies employees, contractors, vendors and agents with remote access privileges to Maple Technologies 's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Maple Technologies.
- General access to the Internet for recreational use by immediate household members through the Maple Technologies Network on personal computers is permitted for employees that have flat-rate services. The Maple Technologies employee is responsible to ensure the family member does not violate any Maple Technologies policies, does not perform illegal activities, and does not use the access for outside business interests. The Maple Technologies employee bears responsibility for the consequences should the access be misused.
- Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Maple Technologies 's network:
    - *Acceptable Encryption Policy*
    - *Virtual Private Network (VPN) Policy*
    - *Wireless Communications Policy*
    - *Acceptable Use Policy*
- For additional information regarding Maple Technologies 's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements

- Secure remote access must be strictly controlled. Control will be enforced via

one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

- At no time should any Maple Technologies employee provide their login or email password to anyone, not even family members.
- Maple Technologies employees and contractors with remote access privileges must ensure that their Maple Technologies -owned or personal computer or workstation, which is remotely connected to Maple Technologies 's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- Maple Technologies employees and contractors with remote access privileges to Maple Technologies 's corporate network must not use non-Maple Technologies email accounts (i.e., Gmail, Yahoo, AOL), or other external resources to conduct Maple Technologies business, thereby ensuring that official business is never confused with personal business.
- Routers for dedicated ISDN lines configured for access to the Maple Technologies network must meet minimum authentication requirements of CHAP.
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
- Frame Relay must meet minimum authentication requirements of DLCI standards.
- Remote Access Services must approve non-standard hardware configurations, and Corporate Information Security must approve security configurations for access to hardware.
- All hosts that are connected to Maple Technologies internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
- Personal equipment that is used to connect to Maple Technologies' networks must meet the requirements of Maple Technologies -owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the Maple Technologies production network must obtain prior approval from Remote Access Services and Corporate Information Security.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a Maple Technologies -provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Maple Technologies and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Remote Access	Any access to Maple Technologies 's corporate network through a non-Maple

	Technologies controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-Maple Technologies network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Maple Technologies 's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

03-01-2007 General Revisions to Document

1.0 Purpose

This document explains Maple Technologies analog and ISDN line acceptable use and approval policies and procedures. This policy covers two distinct uses of analog/ISDN lines: lines that are to be connected for the sole purpose of fax sending and receiving, and lines that are to be connected to computers.

2.0 Scope

This policy covers only those lines that are to be connected to a point inside Maple Technologies building and testing sites. It does not pertain to ISDN/phone lines that are connected into employee homes, PBX desktop phones, and those lines used by Telecom for emergency and non-corporate information purposes.

3.0 Policy

3.1 Scenarios & Business Impact

There are two important scenarios that involve analog line misuse, which we attempt to guard against through this policy. The first is an outside attacker who calls a set of analog line numbers in the hope of connecting to a computer that has a modem attached to it. If the modem answers (and most computers today are configured out-of-the-box to auto-answer) from inside Maple Technologies premises, then there is the possibility of breaching Maple Technologies 's internal network through that computer, unmonitored. At the very least, information that is held on that computer alone can be compromised. This potentially results in the substantial loss of corporate information. (Maple Technologies does not employ analog or ISDN technologies).

The second scenario is the threat of anyone with physical access into a Maple Technologies facility being able to use a modem-equipped laptop or desktop computer. In this case, the intruder would be able to connect to the trusted networking of Maple Technologies through the computer's Ethernet connection, and then call out to an unmonitored site using the modem, with the ability to siphon Maple Technologies information to an unknown location. This could also potentially result in the substantial loss of vital information.

Specific procedures for addressing the security risks inherent in each of these scenarios follow.

3.2 Facsimile Machines

As a rule, the following applies to requests for fax and analog lines:

- Fax lines are to be approved for departmental use only.
- No fax lines will be installed for personal use.
- No analog lines will be placed in a personal cubicle.
- The fax machine must be placed in a centralized administrative area designated for departmental use, and away from other computer equipment.
- A computer, which is capable of making a fax connection, is not to be allowed to use an analog line for this purpose.

Waivers for the above policy on analog-as-fax lines will be delivered on a case-by-case basis after reviewing the business need with respect

to the level of sensitivity and security posture of the request.

Use of an analog/ISDN fax line is conditional upon the requester's full compliance with the requirements listed below. These requirements are the responsibility of the authorized user to enforce at all times:

- The fax line is used solely as specified in the request.
- Only persons authorized to use the line have access to it.
- When not in use, the line is to be physically disconnected from the computer.
- When in use, the computer is to be physically disconnected from Maple Technologies 's internal network.
- The line will be used solely for Maple Technologies business, and not for personal reasons.
- All downloaded material, prior to being introduced into Maple Technologies systems and networks, must have been scanned by an approved anti-virus utility (e.g., Symantec Antivirus Client) which has been kept current through regular updates.

3.3 Computer-to-Analog Line Connections

The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within Maple Technologies will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to Maple Technologies, and active penetrations have been launched against such lines by hackers. Waivers to the policy above will be granted on a case by case basis. Replacement lines, such as those requested because of a move, fall under the category of "new" lines. They will also be considered on a case-by-case basis.

3.4 Requesting an Analog/ISDN Line

Once approved by a manager, the individual requesting an analog/ISDN line must provide the following information to Telecom:

- a clearly detailed business case of why other secure connections available at Maple Technologies cannot be used,
- the business purpose for which the analog line is to be used,
- the software and hardware to be connected to the line and used across the line,
- and to what external connections the requester is seeking access.

The business case must answer, at a minimum, the following questions:

- What business needs to be conducted over the line?
- Why is a Maple Technologies - equipped desktop computer with Internet capability unable to accomplish the same tasks as the proposed analog line?
- Why is Maple Technologies 's current dial-out access pool unable to accomplish the same tasks as an analog line?

In addition, the requester must be prepared to answer the following supplemental questions related to the security profile of the request:

- Will the machines that are using the analog lines be physically disconnected from Maple Technologies 's internal network?
- Where will the analog line be placed? A cubicle or lab?

- Is dial-in from outside of Maple Technologies needed?
- How many lines are being requested, and how many people will use the line?
- How often will the line be used? Once a week, 2 hours per day...?
- What is the earliest date the line can be terminated from service?
- The line must be terminated as soon as it is no longer in use.
- What other means will be used to secure the line from unauthorized use?
- Is this a replacement line from an old location? What was the purpose of the original line?
- What types of protocols will be run over the line?
- Will a Maple Technologies -authorized anti-virus scanner be installed on the machine(s) using the analog lines?
- The requester should use the Analog/ISDN Line Request Form to address these issues and submit a request.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

03-01-2007 General Revisions to Document

1.0 Purpose
The purpose of this policy is to protect Maple Technologies' electronic information from being inadvertently compromised by authorized personnel using a dial-in connection.

2.0 Scope
The scope of this policy is to define appropriate dial-in access and its use by authorized personnel.

3.0 Policy
Maple Technologies does not currently employ any dial-in connectivity features for employees or clients. However, in the event such features become required at a future time, Maple Technologies employees and authorized third parties (customers, vendors, etc.) can use dial-in connections to gain access to the corporate network. Dial-in access should be strictly controlled, using one-time password authentication.

It is the responsibility of employees with dial-in access privileges to ensure a dial-in connection to Maple Technologies is not used by non-employees to gain access to company information system resources. An employee who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and Maple Technologies are literal extensions of Maple Technologies 's corporate network, and that they provide a potential path to the company's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect Maple Technologies 's assets.

Analog and non-GSM digital cellular phones cannot be used to connect to Maple Technologies 's corporate network, as their signals can be readily scanned and/or hijacked by unauthorized individuals. Only GSM standard digital cellular phones are considered secure enough for connection to Maple Technologies 's network. For additional information on wireless access to the Maple Technologies network, consult the *Wireless Communications Policy*.

Note: Dial-in accounts are considered 'as needed' accounts. Account activity is monitored, and if a dial-in account is not used for a period of six months the account will expire and no longer function. If dial-in access is subsequently required, the individual must request a new account as described above.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History
03-01-2007 General Revisions to Document

1.0 Purpose
This policy prohibits access to Maple Technologies networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Corporate Information Security are approved for connectivity to Maple Technologies 's networks.

2.0 Scope
This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Maple Technologies 's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Maple Technologies ’s networks do not fall under the purview of this policy.

3.0 Policy

3.1 Register Access Points and Cards
All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by Corporate Information Security. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with Corporate Information Security

3.2 Approved Technology
All wireless LAN access must use corporate-approved vendor products and security configurations.

3.3 VPN Encryption and Authentication
All computers with wireless LAN devices must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point-to-point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

3.4 Setting the SSID
The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	Definitions
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

6.0 Revision History

07-03-2003, Section 3.4 Added

07-06-2003, expanded to support CDI Initiative

03-01-2007 General Revisions to Document

Email Retention Policy

Section 21

1.0 Purpose

The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees should familiarize themselves with the email retention topic areas that follow this introduction.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Corporate Information Security.

2.0 Scope

This email retention policy is secondary to Maple Technologies policy on Freedom of Information and Business Record Keeping. Any email that contains information in the scope of the Business Record Keeping policy should be treated in that manner. All Maple Technologies email information is categorized into four main classifications with retention guidelines:

- Administrative Correspondence (4 years)
- Fiscal Correspondence (4 years)
- General Correspondence (1 year)
- Ephemeral Correspondence (Retain until read, destroy)

3.0 Policy

3.1 Administrative Correspondence

Maple Technologies Administrative Correspondence includes, though is not limited to clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All email with the information sensitivity label Management Only shall be treated as Administrative Correspondence. To ensure Administrative Correspondence is retained, a mailbox admin@Maple-Tech.com has been created, if you copy (cc) this address when you send email, retention will be administered by the Corporate Information Security Department.

3.2 Fiscal Correspondence

Maple Technologies Fiscal Correspondence is all information related to revenue and expense for the company. To ensure Fiscal Correspondence is retained, a mailbox fiscal@Maple-Tech.com has been created, if you copy (cc) this address when you send email, retention will be administered by the Corporate Information Security Department.

3.3 General Correspondence

Maple Technologies General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for email retention of General Correspondence.

3.4 Ephemeral Correspondence
Maple Technologies Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports.

3.5 Instant Messenger Correspondence
Maple Technologies Instant Messenger General Correspondence may be saved with logging function of Instant Messenger, or copied into a file and saved. Instant Messenger conversations that are Administrative or Fiscal in nature should be copied into an email message and sent to the appropriate email retention address.

3.6 Encrypted Communications
Maple Technologies encrypted communications should be stored in a manner consistent with Maple Technologies Information Sensitivity Policy, but in general, information should be stored in a decrypted format.

3.7 Recovering Deleted Email via Backup Media
Maple Technologies maintains backup tapes from the email server and once a quarter a set of tapes is taken out of the rotation and they are moved offsite. No effort will be made to remove email from the offsite backup tapes.

- **Enforcement**
  Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

- **Definitions - Terms and Definitions**

Approved Electronic Mail Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files
Techniques include the use of AES and PGP. AES encryption is available via many different public domain packages on all platforms. PGP use within Maple Technologies is done via a license. Please contact the appropriate support organization if you require a license.

Individual Access Controls Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers.

Insecure Internet Links
Insecure Internet Links are all network links that originate from a locale or travel over

lines that are not totally under the control of Maple Technologies.

Encryption Secure Maple Technologies Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

- **Revision History**

07-28-2004 Added discussion of backup media.
03-01-2007 General Revisions to Document
10-12-2016 General Revisions to Document

Automatically Forwarded Email Policy

Section 22

1.0 Purpose

To prevent the unauthorized and/or inadvertent disclosure of sensitive company information.

2.0 Scope

This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of Maple Technologies.

3.0 Policy

Employees must exercise utmost caution when sending any email from inside Maple Technologies to an outside network. Unless approved by an employee's manager and Corporate Information Security, Maple Technologies email will not be automatically forwarded to an external destination. Sensitive information, as defined in the *Information Sensitivity Policy*, will not be forwarded via any means, unless that email is critical to business and is encrypted in accordance with the *Acceptable Encryption Policy*.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
Email	The electronic transmission of information through a mail protocol such as SMTP. Microsoft Outlook uses SMTP.
Forwarded email	Email resent from internal networking to an outside point.
Sensitive information	Information is considered sensitive if it can be damaging to Maple Technologies or its customers' dollar value, reputation, or market standing.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

6.0 Revision History

03-01-2007 General Revisions to Document

Audit Vulnerability Scan Policy

Section 23

1.0 Purpose

The purpose of this agreement is to set forth our agreement regarding network security scanning offered by the Corporate Information Security to the Maple Technologies. Corporate Information Security shall utilize Symantec Antivirus Client to perform electronic scans of Client's networks and/or firewalls or on any system at Maple Technologies.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents ensure conformance to Maple Technologies security policies
- Monitor user or system activity where appropriate.

2.0 Scope

This policy covers all computer and communication devices owned or operated by Maple Technologies. This policy also covers any computer and communications device that are present on Maple Technologies premises, but which may not be owned or operated by Maple Technologies. The Corporate Information Security will not perform Denial of Service activities.

3.0 Policy

When requested, and for the purpose of performing an audit, consent to access needed will be provided to members of Corporate Information Security. Maple Technologies hereby provides its consent to allow Corporate Information Security to access its networks and/or firewalls to the extent necessary to allow Corporate Information Security to perform the scans authorized in this agreement. Maple Technologies shall provide protocols, addressing information, and network connections sufficient for Corporate Information Security to utilize the software to perform network scanning.

This access may include:

7.0 User level and/or system level access to any computing or communications device

8.0 Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on Maple Technologies equipment or premises

9.0 Access to work areas (labs, offices, cubicles, storage areas, etc.)

10.0 Access to interactively monitor and log traffic on Maple Technologies networks.

3.1 Network Control.

If Client does not control their network and/or Internet service is provided via a second or third party, these parties are required to approve scanning in writing, if scanning is to occur outside of the Maple Technologies LAN. By signing this agreement, all involved parties acknowledge that they authorize Corporate Information Security to use their service networks as a gateway to conduct any of these tests during the dates and times specified.

3.2 Service Degradation and/or Interruption.

Network performance and/or availability may be affected by the network scanning. Maple Technologies releases Corporate Information Security of any and all liability for damages that may arise from network availability restrictions

caused by the network scanning, unless such damages are the result Corporate Information Security's gross negligence or intentional misconduct.

3.3 Client Point of Contact During the Scanning Period. Maple Technologies shall identify in writing a person to be available if the result Corporate Information Security Scanning Team has questions regarding data discovered or requires assistance.

3.4 Scanning period. Maple Technologies and Corporate Information Security Scanning Team shall identify in writing the allowable dates for the scan to take place.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

09-29-2003**,** updated to include National Association of State Auditors, Comptrollers, and Treasurers; the National Association of Local Government Auditors; the U.S. General Accounting Office; and U.S. Inspectors General Legal and Reporting Considerations.
03-01-2007 General Revisions to Document

1.0 Overview

This document defines the minimum-security criteria that an Application Service Provider (ASP) must meet in order to be considered for use by Maple Technologies. As part of the ASP selection process, the ASP Vendor must demonstrate compliance with the Standards listed below by responding in writing to EVERY statement and question in the six categories. Corporate Information Security will closely review the vendor responses, and will suggest remediation measures in any areas that fall short of the minimum-security criteria. Corporate Information Security approval of any given ASP resides largely on the vendor's response to this document.

These Standards are subject to additions and changes without warning by Corporate Information Security.

2.0 Scope

This document can be provided to ASPs that are either being considered for use by Maple Technologies, or have already been selected for use.

3.0 Responding to These Standards

Corporate Information Security is looking for explicitly detailed, technical responses to the following statements and questions. ASPs should format their responses directly beneath the Standards (both questions and requirements) listed below. In addition, please include any security whitepapers, technical documents, or policies that you may have.

Answers to each Guideline should be specific and avoid generalities, e.g.:

Examples:

Unacceptable: "We have hardened our hosts against attack."

Acceptable: "We have applied all security patches for Windows 7 as of 12/01/2009 to our servers. Our Administrator is tasked with keeping up-to-date on current vulnerabilities that may affect our environment, and our policy is to apply new patches during our maintenance period (2300hrs, Saturday) every week. Critical updates are implemented within 24 hours. A complete list of applied patches is available to Maple Technologies."

Unacceptable: "We use encryption."

Acceptable: "All communications between our site and Maple Technologies will be protected by IPSec ESP Tunnel mode using 168-bit TripleDES encryption, SHA-1 authentication. We exchange authentication material via either out-of-band shared secret, or PKI certificates."

4.0 Standards

4.1 General Security

- Maple Technologies reserves the right to periodically audit the Maple Technologies application infrastructure to ensure compliance with the ASP Policy and these Standards. Non-intrusive network audits (basic portscans, etc.) may be done randomly, without prior notice. More intrusive network and physical audits may be conducted on site with 24 hours notice.

- The ASP must provide a proposed architecture document that includes a full network diagram of the Maple Technologies Application Environment, illustrating the relationship between the Environment and any other relevant networks, with a full data flowchart that detail where Maple Technologies data resides, the applications that manipulate it, and the security thereof.

- The ASP must be able to immediately disable all or part of the functionality of the application should a security issue be identified.

4.2 Physical Security

- The equipment hosting the application for Maple Technologies must be located in a physically secure facility, which requires secured access at a minimum.

- The infrastructure (hosts, network equipment, etc.) hosting the Maple Technologies application must be located in a locked cage-type environment.

- Maple Technologies shall have final say on who is authorized to enter any locked physical environment, as well as access the Maple Technologies Application Infrastructure.

- The ASP must disclose who amongst their personnel will have access to the environment hosting the application for Maple Technologies.

- Maple Technologies 's Corporate Asset Protection team requires that the ASP disclose their ASP background check procedures and results prior to Corporate Information Security granting approval for use of an ASP.

4.3 Network Security

- The network hosting the application must be air-gapped from any other network or customer that the ASP may have. This means the Maple Technologies application environment must use separate hosts, and separate infrastructure.

- How will data go between Maple Technologies and the ASP? Keep in mind the following two things:

    - If Maple Technologies will be connecting to the ASP via a private circuit (such as frame relay, etc.), then that circuit must terminate on the Maple Technologies extranet, and the operation of that circuit will

come under the procedures and policies that govern the Maple Technologies Partner Network Management Group.

- If, on the other hand, the data between Maple Technologies and the ASP will go over a public network such as the Internet, the ASP must deploy appropriate firewalling technology, and the traffic between Maple Technologies and the ASP must be protected and authenticated by cryptographic technology (See Cryptography below).

4.4 Host Security

- The ASP must disclose how and to what extent the hosts (Unix, NT, etc.) comprising the Maple Technologies application infrastructure have been hardened against attack. If the ASP has hardening documentation for the CAI, provide that as well.

- The ASP must provide a listing of current patches on hosts, including host OS patches, web servers, databases, and any other material application.

- Information on how and when security patches will be applied must be provided. How does the ASP keep up on security vulnerabilities, and what is the policy for applying security patches?

- The ASP must disclose their processes for monitoring the integrity and availability of those hosts.

- The ASP must provide information on their password policy for the Maple Technologies application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.

- Maple Technologies cannot provide internal usernames/passwords for account generation, as the company is not comfortable with internal passwords being in the hands of third parties. With that restriction, how will the ASP authenticate users? (e.g., LDAP, Netegrity, Client certificates.)

- The ASP must provide information on the account generation, maintenance and termination process, for both maintenance as well as user accounts. Include information as to how an account is created, how account information is transmitted back to the user, and how accounts are terminated when no longer needed.

4.5 Web Security

- At Maple Technologies 's discretion, the ASP may be required to disclose the specific configuration files for any web servers and associated support functions (such as search engines or databases).

- Please disclose whether, and where, the application uses Java, Javascript, ActiveX,

PHP or ASP (active server page) technology.

- What language is the application back-end written in? (C, Perl, Python, VBScript, etc.)

- Please describe the ASP process for doing security Quality Assurance testing for the application. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.

- Has the ASP done web code review, including CGI, Java, etc, for the explicit purposes of finding and remediating security vulnerabilities? If so, who did the review, what were the results, and what remediation activity has taken place? If not, when is such an activity planned?

4.6 Cryptography

- The Maple Technologies application infrastructure cannot utilize any "homegrown" cryptography – any symmetric, asymmetric or hashing algorithm utilized by the Maple Technologies application infrastructure must utilize algorithms that have been published and evaluated by the general cryptographic community.

- Encryption algorithms must be of sufficient strength to equate to 168-bit TripleDES.

- Preferred hashing function is SHA-3.

- Connections to the ASP utilizing the Internet must be protected using any of the following cryptographic technologies: TLS, SSL, IPSec, SSH/SCP, PGP.

- If the Maple Technologies application infrastructure requires PKI, please contact Maple Technologies Information Security Group for additional guidance.

5.0 Revision History

03-01-2007, 10-12-2016 General Revisions to Document

EMPLOYEE ACKNOWLEDGEMENT

As an employee of Maple Technologies, I have been provided with a complete copy of The Corporate Ethics Policy and Security Policies and Protocols for Maple Technologies. I hereby acknowledge receipt of same and further acknowledge that I have read and agree to abide by and adhere to these policies.

Signed and Acknowledged:

_____

Employee Name:
Date Signed:

EMPLOYEE NONDISCLOSURE AGREEMENT

FOR GOOD CONSIDERATION, and in consideration of being employed by Maple Technologies, the undersigned employee hereby agrees and acknowledges:

1. That during the course of my employ there may be disclosed to me certain trade secrets of the Company; said trade secrets consisting but not necessarily limited to:

- a) Technical information: Methods, processes, formulae, compositions, systems, techniques, inventions, machines, computer programs and research projects.

  b) Business information: Customer lists, pricing data, sources of supply, financial data and marketing, production, or merchandising systems or plans.

2. I agree that I shall not during, or at any time after the termination of my employment with the Company, use for myself or others, or disclose or divulge to others including future employees, any trade secrets, confidential information, or any other proprietary data of the Company in violation of this agreement.

3. That upon the termination of my employment from the Company:

- a) I shall return to the Company all documents and property of the Company, including but not necessarily limited to: drawings, blueprints, reports, manuals, correspondence, customer lists, computer programs, computers, hardware and all other materials and all copies thereof relating in any way to the Company's business, or in any way obtained by me during the course of employ. I further agree that I shall not retain copies, notes or abstracts of the foregoing.

  b) The Company may notify any future or prospective employer or third party of the existence of this agreement, and shall be entitled to full injunctive relief for any breach.

  c) This agreement shall be binding upon me and my personal representatives and successors in interest, and shall inure to the benefit of the Company, its successors and assigns.

Signed and dated:

_____ _____

For Company: Employee Name: