IT Security Policy

For Pix Transmission Ltd. Internal Circulation Only

Information Security Policy

01. Overview

The purpose of this document is to outline the strategies and managing processes behind implementing a Successful Security Policy.
The Information Security Policy addresses Confidentiality, Integrity & Availability of PIX Transmissions Ltd's Information resources, where the main objective will be to provide staff members with a better, if not much improved understanding of the issues stated in a security policy.

02. Scope

This document is intended to provide clear directives as to the usage of Information Technology resources & serve as reference for all related IT engagements.

03. Introduction

Information security has come to play an extremely vital role in today's fast moving, but invariably technically fragile business environment. Consequently, secured communications are needed in order for both companies and customers to benefit from the advancements that the Internet is empowering us with.
The importance of this fact needs to be clearly highlighted so that adequate measures will be implemented, not only enhancing the company's daily business procedures and transactions, but also to ensure that the much needed security measures are implemented with an acceptable level of security competency.
The possibility of having your company's data exposed to a malicious attacker is constantly increasing nowadays due to the high number of "security novice" staff also having access to sensitive, and sometimes even secret business information.

04. Why Have a Security Policy

As building a good security policy provides the foundations for the successful implementation of IT projects in the future, this is without a doubt the first measure that must be taken to reduce the risk of unacceptable use of any of the company's information resources.
The first step towards enhancing a company's security is the introduction of a precise yet enforceable security policy, informing staff on the various aspects of their responsibilities, general use of company resources and explaining how sensitive information must be handled. The policy will also describe in detail the meaning of acceptable use, as well as listing prohibited activities.
The development (and the proper implementation) of a security policy is highly beneficial as it will not only turn all of staff into participants in the company's effort to secure its communications but also help reduce the risk of a potential security breach through "human-factor" mistakes.
These are usually issues such as revealing information to unknown (or unauthorized sources), the insecure or improper use of the Internet and many other dangerous activities.
Additionally the building process of a security policy will also help define a company's critical assets, the ways they must be protected and will also serve as a centralized document, as far as protecting Information Security Assets is concerned.

05. What Is a Security Policy?

The security policy is basically a plan, outlining what the company's critical assets are, and how they must (and can) be protected. Its main purpose is to provide staff with a brief overview of the "acceptable use" of any of the Information Assets, as well as to explain what is deemed as allowable and what is not, thus engaging them in securing the company's critical systems.
The document acts as a "must read" source of information for everyone using in any way systems and resources defined as potential targets. A good and well developed security policy should address some of these following elements:
- How sensitive information must be handled

- How to properly maintain your ID(s) and password(s), as well as any other accounting data
- How to respond to a potential security incident, intrusion attempt, etc.
- How to use workstations and Internet connectivity in a secure manner
- How to properly use the corporate e-mail system

Basically, the main reasons behind the creation of a security policy is to set a company's information security foundations, to explain to staff how they are responsible for the protection of the information resources, and highlight the importance of having secured communications while doing business online.

06. Security Policy Violation

In order to realize the importance of a security policy, employees need to be aware and fully understand the consequences of violating the policy, thereby exposing critical systems to a malicious attacker, or causing unintended damage to other companies worldwide. Violations should be handled accordingly; those who in one way or the other violate the security policy should be made aware that they may face being put through a "trial period", which involves also the limited use of some of the company information assets until they can show they are able to act in a secure manner while using the corporate systems. They should also be aware that in some (severe) cases they also may risk being fired or even prosecuted as the Information Technology Act of India.

Appropriate action needs to be taken in every violation case in accordance with corporate policy, with the focus on reiterating the security basics. In case of lapse of Security, there will most likely be a successful penetration, either due to human error, or misunderstanding the policy.

07. Revising the Security Policy

The Security Policy will be revised from time to time based on corporate directives as well as Industry Best practices & prevalent Information technology laws, as well as to ensure its effectiveness by closely reviewing several critical factors for its lasting success.

08. Reporting of Security Incidents:

Employees are advised to log a call with IT helpdesk (IT.Support@Pixtrans.com) or call at 07104-669123 to report Information Security Incidents.

Employees may also contact the Head of Information Technology to gain clarification or to report Information Security breach incidents at the below mentions contact details.

Information Sensitivity Policy

1. 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 PIX Transmissions Ltd 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 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 PIX Transmissions Ltd Confidential information (e.g., PIX Transmissions Ltd 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 Information Security Manager.

2. Scope

All PIX Transmissions Ltd information is categorized into two main classifications:

· PIX Transmissions Ltd Public

· PIX Transmissions Ltd Confidential

PIX Transmissions Ltd 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 PIX Transmissions Ltd.

PIX Transmissions Ltd 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 PIX Transmissions Ltd 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 PIX Transmissions Ltd Confidential information is "PIX Transmissions Ltd Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to PIX Transmissions Ltd 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 supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into PIX Transmissions Ltd's network to support our operations.

PIX Transmissions Ltd personnel are encouraged to use common sense judgment in securing PIX Transmissions Ltd 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. Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as PIX Transmissions Ltd Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the PIX Transmissions Ltd 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" PIX Transmissions Ltd Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "PIX Transmissions Ltd Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, PIX Transmissions Ltd information is presumed to be "PIX Transmissions Ltd Confidential" unless expressly determined to be PIX Transmissions Ltd Public information by a PIX Transmissions Ltd employee with authority to do so.

Access: PIX Transmissions Ltd employees, contractors, people with a business need to know.
Distribution within PIX Transmissions Ltd: Standard interoffice mail approved electronic mail and electronic file transmission methods.
Distribution outside of PIX Transmissions Ltd internal mail: International 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 PIX Transmissions Ltd 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 "PIX Transmissions Ltd Confidential" or "PIX Transmissions Ltd Proprietary", wish to label the information "PIX Transmissions Ltd 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: PIX Transmissions Ltd employees and non-employees with signed non-disclosure agreements who have a business need to know.
Distribution within PIX Transmissions Ltd: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of PIX Transmissions Ltd internal mail: Sent via 3rd party mail or approved private carriers.
Electronic distribution: No restrictions to approved recipients within PIX Transmissions Ltd, but should be encrypted or sent via a private link to approved recipients outside of PIX Transmissions Ltd premises.
Storage: Individual access controls are highly recommended for electronic information.
Disposal/Destruction: In specially marked disposal bins on PIX Transmissions Ltd 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 PIX Transmissions Ltd Confidential information is very sensitive, you may should label the

information "PIX Transmissions Ltd Internal: Registered and Restricted", "PIX Transmissions Ltd Eyes Only", "PIX Transmissions Ltd Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of PIX Transmissions Ltd 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 (PIX Transmissions Ltd employees and non-employees) designated with approved access and signed non-disclosure agreements.
Distribution within PIX Transmissions Ltd: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution outside of PIX Transmissions Ltd internal mail: Delivered direct; signature required; approved private carriers.
Electronic distribution: No restrictions to approved recipients within PIX Transmissions Ltd, 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 PIX Transmissions Ltd 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. Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions
Terms and Definitions
Appropriate measures
To minimize risk to PIX Transmissions Ltd from an outside business connection. PIX Transmissions Ltd computer use by competitors
and unauthorized personnel must be restricted so that, in the event of an attempt to access PIX Transmissions Ltd corporate information, the amount of information at risk is minimized.

Configuration of PIX Transmissions Ltd-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 mail room for special pick-up of mail.

Approved Electronic File Transmission Methods
Includes supported FTP clients and Web browsers.

Envelopes 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. These include, but are not necessarily limited to, Currently Postmaster 8 with Web access is the deployed email system. 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 SSL encryption is available via many different public domain packages on all platforms

SSL use within PIX Transmissions Ltd 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 or expunge data on a PC you must use inbuilt or a separate program to overwrite data, supplied as a part of PIX Transmissions IT approved software. Otherwise, the email client software's normal erasure routine keeps the data intact until overwritten.

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 Laptops & 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 PIX Transmissions Ltd.

Encryption
Secure PIX Transmissions Ltd 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 system network configuration to connect to PIX Transmissions Ltd's internal network over the Internet. Contact IT support 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 PIX Transmissions Ltd has control over its entire distance. For example, all PIX Transmissions Ltd networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to sites, offices or employee's homes is a private link. PIX Transmissions Ltd also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which PIX Transmissions Ltd has established private links include all announced acquisitions and some short-term temporary links

Information Technology Ethics Policy

1. Overview

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

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

PIX Transmissions Ltd will not tolerate any wrongdoing or impropriety at anytime. PIX Transmissions Ltd 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 IT 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 PIX Transmissions Ltd, including all personnel affiliated with third parties.

4. Policy

4.1. Executive Commitment to Ethics

4.1.1. 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 regard their position within PIX Transmissions Ltd.

4.2. Employee Commitment to Ethics

4.2.1. PIX Transmissions Ltd 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 regard their position within PIX Transmissions Ltd.

4.2.4. Employees will help PIX Transmissions Ltd to increase customer and vendor satisfaction by providing quality product s and timely response to inquiries.

4.3. Company Awareness

4.3.1. Promotion of ethical conduct within interpersonal communications of employees will be adequately appraised.

4.3.2. PIX Transmissions Ltd will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

4.4. Maintaining Ethical Practices

4.4.1. PIX Transmissions Ltd will reinforce the importance of the integrity message and the tone.

4.4.2. Every employee, manager, Head of Department needs consistently maintain an ethical stance and support ethical behavior.

4.4.3. Employees at PIX Transmissions Ltd should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.
4.4.4. PIX Transmissions Ltd has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

4.5. **Unethical Behavior**

4.5.1. PIX Transmissions Ltd will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.
4.5.2. PIX Transmissions Ltd will not tolerate harassment or discrimination.
4.5.3. Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.
4.5.4. PIX Transmissions Ltd will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.
4.5.5. PIX Transmissions Ltd employees will not use corporate assets or business relationships for personal use or gain.

5. Enforcement

5.1. Any infractions of this code of ethics will not be tolerated and PIX Transmissions Ltd will act quickly in correcting the issue if the ethical code is broken.
5.2. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Information Security Acceptable Use Policy

1.0 Overview

Information Security's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to PIX Transmissions Ltd's established culture of openness, trust and integrity. Information Security is committed to protecting PIX Transmissions Ltd's employees, 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 PIX Transmissions Ltd. 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 PIX Transmissions Ltd 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 PIX Transmissions Ltd. These rules are in place to protect the employee and PIX Transmissions Ltd. Inappropriate use exposes PIX Transmissions Ltd 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 PIX Transmissions Ltd,
including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by PIX Transmissions Ltd.

4.0 Policy

4.1 General Use and Ownership

1. While PIX Transmissions Ltd's 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 PIX Transmissions Ltd. Because of the need to protect PIX Transmissions Ltd's network, management cannot guarantee the confidentiality of information stored on any network device belonging to PIX Transmissions Ltd.
2. 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.
3. Information Security recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Information Security's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to Information Security's Awareness Initiative.
4. For security and network maintenance purposes, authorized individuals within PIX Transmissions Ltd may monitor equipment, systems and network traffic at any time, per Information Security's Audit Policy.
5. PIX Transmissions Ltd reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. 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 Corporate 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.
2. 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 quarterly; user level passwords should be changed every six months.
3. 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.
4. Use encryption of information in compliance with Information Security's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Security Tips" posted on the Information Security portal at http://192.168.40.21/pix_int/index.htm

6. Postings by employees from a PIX Transmissions Ltd email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of PIX Transmissions Ltd, unless posting is in the course of business duties.

7. All hosts used by the employee that are connected to the PIX Transmissions Ltd Internet/Intranet/Extranet, whether owned by the employee or PIX Transmissions Ltd, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
8. 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 PIX Transmissions Ltd authorized to engage in any activity that is illegal under local, state, central or international law while utilizing PIX Transmissions Ltd-owned resources.
The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. 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 PIX Transmissions Ltd.
2. 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 PIX Transmissions Ltd or the end user does not have an active license is strictly prohibited.
3. 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.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. 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.
6. Using a PIX Transmissions Ltd 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.
7. Making fraudulent offers of products, items, or services originating from any PIX Transmissions Ltd account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. 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.
10. Port scanning or security scanning is expressly prohibited unless prior notification to Information Security is made.
11. 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.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. 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.
15. Providing information about, or lists of, PIX Transmissions Ltd employees to parties outside PIX Transmissions Ltd.

Email and Communications Activities
1. 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).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. 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.
5. Creating or forwarding "chain letters"or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within PIX Transmissions Ltd's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by PIX Transmissions
Ltd or connected via PIX Transmissions Ltd's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.4. Blogging on Intranet Portal
1. Blogging by employees on Intranet Portal, whether using PIX Transmissions Ltd’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of PIX Transmissions Ltd’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate PIX Transmissions Ltd’s policy, is not detrimental to PIX Transmissions Ltd’s best interests, and does not interfere with an employee's regular work duties. Blogging from PIX Transmissions Ltd’s systems is also subject to monitoring.
2. PIX Transmissions Ltd’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by Information Security policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of PIX Transmissions Ltd and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by PIX Transmissions Ltd’s Non-Discrimination and Anti-Harassment policy.

4. Employees may also not attribute personal statements, opinions or beliefs to PIX Transmissions Ltd when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of PIX Transmissions Ltd. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, PIX Transmissions Ltd's trademarks, logos and any other PIX Transmissions Ltd intellectual property may also not be used in connection with any blogging activity

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**
Blogging:	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Spam:	Unauthorized and/or unsolicited electronic mass mailings.

Risk Assessment Policy

1.0 Purpose
To empower 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 PIX Transmissions Ltd or any outside entity that has signed a *Third Party Agreement* with PIX Transmissions Ltd. 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 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 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 PIX Transmissions Ltd, responsible for maintaining PIX Transmissions Ltd assets.
Risk:	Those factors that could affect confidentiality, availability, and integrity of PIX Transmissions Ltd's key information assets and systems. 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.

Audit Vulnerability Scan Policy

1.0 Purpose
The purpose of this agreement is to set forth our agreement regarding network security scanning offered by the Vulnerability Auditing Party to the PIX Transmissions Ltd. Vulnerability Auditing Party shall utilize PIX Transmissions IT Approved Software to perform electronic scans of Client's networks and/or firewalls or on any system at PIX Transmissions Ltd.
Audits may be conducted to:
· Ensure integrity, confidentiality and availability of information and resources
· Investigate possible security incidents ensure conformance to PIX Transmissions Ltd security policies
· Monitor user or system activity where appropriate.

2.0 Scope
This policy covers all computer and communication devices owned or operated by PIX Transmissions Ltd. This policy also covers any computer and communications device that are present on PIX Transmissions Ltd premises, but which may not be owned or operated by PIX Transmissions Ltd. The Vulnerability Auditing Party 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 Vulnerability Auditing Party. PIX Transmissions Ltd hereby provides its consent to allow of Vulnerability Auditing Party to access its networks and/or firewalls to the extent necessary to allow the Audit Party to perform the scans authorized in this agreement. PIX Transmissions Ltd shall provide protocols, addressing information, and network connections sufficient for Vulnerability Auditing Party to utilize the software to perform network scanning.

This access may include:
· User level and/or system level access to any computing or communications device
· Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on PIX Transmissions Ltd equipment or premises
· Access to work areas (labs, offices, cubicles, storage areas, etc.)
· Access to interactively monitor and log traffic on PIX Transmissions Ltd 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 PIX Transmissions ltd's LAN. By signing this agreement, all involved parties acknowledge that they authorize of Vulnerability Auditing Party to use their service networks as a gateway for the conduct 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. PIX Transmissions Ltd releases Vulnerability Auditing Party 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 Vulnerability Auditing Party's gross negligence or intentional misconduct.

3.3 Client Point of Contact during the Scanning Period. PIX Transmissions Ltd shall identify in writing a person to be available if the resulting Vulnerability Auditing Party Scanning Team has questions regarding data discovered or requires assistance.

3.4 Scanning period. PIX Transmissions Ltd and Vulnerability Auditing Party 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

Internet Use Policy

1.0 Purpose
The purpose of this policy is to define standards for systems that monitor and limit web use from any host within PIX Transmissions Ltd's network. These standards are designed to ensure employees use the Internet in a safe and responsible manner, and ensure that employee web use can be monitored or researched during an incident.

2.0 Scope
This policy applies to all PIX Transmissions Ltd employees & Partners with a PIX Transmissions Ltd owned or personally-owned computer or workstation connected to the PIX Transmissions td network. This policy applies to all end user initiated communications between PIX Transmissions Ltd's network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

3.0 Policy
All internet access inside PIX Transmissions Ltd network & systems should be strictly for PIX Transmissions Ltd business purposes only. Internet access is categorized for different user segments as per their Business needs. Internet Webmail except PIX Transmissions mail is blocked for all users. Exception groups are defined as per Business need. Provision of the privileged Internet access is purely on the discretion of PIX Transmissions Ltd senior management & can be reverted without notification.

3.1 Web Site Monitoring
The Information Technology Department shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 14 days.

3.2 Access to Web Site Monitoring Reports
General trending and activity reports will be made available to any employee as needed upon request to the Information Technology Department. IT & Security Team members may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the IT & Security Team upon written or email request to Information Security Head from Head of Departments from other teams.

3.3 Internet Use Filtering System
The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for PIX Transmissions Ltd's corporate environment. The following protocols and categories of websites would be blocked for all user groups:
· Adult/Sexually Explicit Material
· Advertisements & Pop-Ups
· Chat and Instant Messaging
· Gambling
· Hacking
· Illegal Drugs
· Intimate Apparel and Swimwear
· Peer to Peer File Sharing
· Personals and Dating
· Social Network Services
· SPAM, Phishing and Fraud
· Spyware
· Tasteless and Offensive Content
· Violence, Intolerance and Hate

Web Based Internet Email except PIX Transmissions webmail blocked for all users. Exception groups defined as per Business need.

3.4 Internet Use Filtering Rule Changes

The Information Technology Department shall periodically review and recommend changes to web and protocol filtering rules. Information Security Head would review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in Internet Access forms.

3.5 Internet Use Filtering Exceptions

If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the Information Technology help desk. An IT employee will review the request and un-block the site if it is miscategorized. Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to the IT Help desk. Requesting Employee will present all approved exception requests to Information Technology in writing or by email. Information Technology will unblock that site or category for that associate only. Information Technology will track approved exceptions and report on them upon request.

4.0 Enforcement

The designated IT Security Officer will periodically review Internet use monitoring and filtering systems and processes to ensure they are in compliance with this policy. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Internet Filtering – Using technology that monitors each instance of communication between devices on the corporate network and the Internet and blocks traffic that matches specific rules.
User ID – User Name or other identifier used when an associate logs into the corporate network.
IP Address – Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.
SMTP – Simple Mail Transfer Protocol. The Internet Protocol that facilitates the exchange of mail messages between Internet mail servers.
Peer to Peer File Sharing – Services or protocols such as Bit Torrent and Kazaa that allow Internet connected hosts to make files available to or download files from other hosts.
Social Networking Services – Internet sites such as Orkut that allow users to post content, chat, and interact in online communities.
SPAM – Unsolicited Internet Email. SPAM sites are websites link to from unsolicited Internet mail messages.
Phishing – attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.
Hacking – Sites that provide content about breaking or subverting computer security controls.

Software Installation Policy

1.0 Overview
Allowing employees to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered in an audit and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on company equipment.

2.0 Purpose
To minimize the risk of loss of program functionality, the exposure of sensitive information contained within PIX Transmissions Ltd computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

3.0 Scope
This policy covers all computers, servers, Laptops, PDAs, smart phones, and other computing devices owned by PIX Transmissions Ltd.

4.0 Policy
Employees may not install software on PIX Transmissions Ltd computing devices operated within the PIX Transmissions Ltd network.
Software requests must first be approved by the requester's manager and then be made to the Information Technology department or Help Desk in writing or via email. Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need. The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

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
DLL: Dynamically Linked Library. A shared program module used by one or more programs, often installed as part of a program installation. If the current version of a DLL is overwritten by a newer or older version; existing programs that relied upon the original version may cease to function or may not function reliably.
Malware: A wide variety of programs created with the explicit intention of performing malicious acts on systems they run on, such as stealing information, hijacking functionality, and attacking other systems.
PDA: Personal Digital Assistant. A portable, hand held computing device capable of running software programs. It may connect to host computers or to wired or wireless networks.
Smartphone: A cellular phone with qualities of a computer or PDA. It is capable of running software programs and connecting to computer networks.

Server Security Policy

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 PIX Transmissions Ltd. Effective implementation of this policy will minimize unauthorized access to PIX Transmissions Ltd proprietary information and technology.

2.0 Scope
This policy applies to server equipment owned and/or operated by PIX Transmissions Ltd, and to servers registered under any PIX Transmissions Ltd-owned internal network domain.
This policy is specifically for equipment on the internal PIX Transmissions Ltd network. For secure configuration of equipment external to PIX Transmissions Ltd on the DMZ, refer to the *Internet DMZ Equipment Policy*.

3.0 Policy
This Policy is applicable to all PIX Transmissions Ltd Server systems or low end systems used as Servers. This policy is applicable irrespective of the Hardware, Software, and Operating system platform used for deploying the Servers.

3.1 Ownership and Responsibilities
All internal servers deployed at PIX Transmissions Ltd must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by 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 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 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 appropriate access-control methods.
· 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/admin account 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 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 2 weeks.
· Monthly full backups will be retained for a minimum of 1 month.

· Security-related events will be reported to 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 PIX Transmissions Ltd.
· Audits will be managed by the internal audit group or Information Security, in accordance with the *Audit Policy*. 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 PIX Transmissions Ltd Server. Desktop/laptop machines and Lab equipment are also relevant to the scope of this policy if used as Servers.

Workstation Security Policy

1.0 Purpose
The purpose of this policy is to provide guidance for workstation security for PIX Transmissions Ltd workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the PIX Transmissions Limited Security Policy is met.

2.0 Scope
This policy applies to all PIX Transmissions Ltd employees, contractors, workforce members and Business Partners with a PIX Transmissions Ltd-owned or personal-workstation connected to the PIX Transmissions Ltd network.

3.0 Policy
Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of information and that access to sensitive information is restricted to authorized users.

3.1 Workforce members using workstations shall consider the sensitivity of the information, including protected information that may be accessed and minimize the possibility of unauthorized access.
3.2 PIX Transmissions Ltd will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.
3.3 Appropriate measures include:
· Restricting physical access to workstations to only authorized personnel.
· Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
· Complying with all applicable PIX Transmissions Ltd password policies and procedures.
· Ensuring workstations are used for authorized business purposes only.
· Never installing unauthorized software on workstations.
· Storing all sensitive information on network servers
· Keeping food and drink away from workstations in order to avoid accidental spills.
· Securing laptops that contain sensitivity information by using cable locks or locking laptops up in drawers or cabinets.
· Complying with the Anti-Virus policy
· Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
· Ensuring workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents
· Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
· If wireless network access is used, ensure access is secure by following the Wireless Access 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
Workstations include: laptops, desktops, PDAs, computer based equipment containing or accessing company information and authorized home workstations accessing the PIX Transmissions Ltd network.
Workforce members include: employees, volunteers, trainees, and other persons under the direct control of PIX Transmissions Ltd

Antivirus & Server Malware Protection Policy

1.0 Overview:
PIX Transmissions Ltd IT Team is entrusted with the responsibility to provide professional management of employee systems (clients) & servers as outlined in IT Policies. Inherent in this responsibility is an obligation to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover.

2.0 Purpose:
The purpose of this policy is to outline which server systems are required to have anti-virus and/or anti-spyware applications.

3.0 Scope:
This policy applies to all servers & clients that PIX Transmissions Ltd is responsible to manage. This explicitly includes any system for which PIX Transmissions Ltd has a contractual obligation to administer. This also includes all server systems setup for internal use by PIX Transmissions Ltd, regardless of whether PIX Transmissions Ltd retains administrative obligation or not.

4.0 Policy:
PIX Transmissions Ltd operations staff will adhere to this policy to determine which servers & clients will have antivirus and/or anti-spyware applications installed on them and to deploy such applications as appropriate.

4.1 ANTI-VIRUS
All servers & clients MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:
· The system connects to PIX Transmissions Ltd IT network.
· Non-administrative users have remote access capability
· The system is a file server
· NBT/Microsoft Share access is open to this server from systems used by non-administrative users
· HTTP/FTP access is open from the Internet
· Other “risky” protocols/applications are available to this system from the Internet at the discretion of the PIX Transmissions Ltd Information Security Officer.
All servers SHOULD Mandatorily have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:
· Outbound web access is available from the system
· Password used to stop AV services must be change in regular intervals

4.2 MAIL SERVER & MAIL CLIENT ANTI-VIRUS
If the target system is a mail server/client it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if the Central anti-virus Server application still scans inbound emails while the backup is being performed.

4.3 ANTI-SPYWARE
All servers & clients MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:
· ANY inbound/outbound access is permitted to the Internet
· Any system where non-technical or non-administrative users have remote access to the system.
· Any system where non-technical or non-administrative users have the ability to install software on their own.

4.4 NOTABLE EXCEPTIONS

An exception to the above standards will generally be granted with minimal resistance and documentation if one of the following notable conditions apply to this system:

· The system is not on PIX Transmissions Ltd IT wired or wireless network.

· The system is used on dedicated Quarantined VLAN.

· The system is a consultant or visitor laptop connected temporarily to PIX Transmissions network Quarantined VLAN.

4.5 Enforcement:

The responsibility for implementing this policy belongs to all operational staff at PIX Transmissions Ltd. Responsibility for ensuring that new and existing systems remain in compliance with this policy resides with the PIX Transmissions Ltd Security Officer. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.6 Definitions:

TERM DEFINITION

Server: For purposes of this policy, a server is any computer system residing in the physically secured data center owned and operated by PIX Transmissions Ltd. In addition, this includes any system running an operating system specifically intended for server usage as defined by the PIX Transmissions Ltd IT/IS Manager that has access to internal secure networks. This includes, but is not limited to, Microsoft Servers and all permutations, any Linux/Unix based operating systems that external users are expected to regularly connect to and VMS.etc.

Malware: Software designed to infiltrate or damage a computer system without the owner's informed consent. It is a blend of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Spyware: Broad category of software designed to intercept or take partial control of a computer's opera tion without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

Anti-virus Software: Consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).

Guidelines on Anti-Virus Process

Recommended processes to prevent virus problems:

· Always use the corporate standard, supported anti-virus software.

· Download and run the current version; download and install anti-virus software updates as they become available.

· 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.

· Delete spam, chain, and other junk email without forwarding, in with PIX Transmissions Ltd's *Acceptable Use Policy*.

· Never download files from unknown or suspicious sources.

· Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

· Always scan removable devices from an unknown source for viruses before using it.

· Back-up critical data and system configurations on a regular basis and store the data in a safe place.

· If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, and 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.

· New viruses are discovered almost every day. Periodically check the *Lab Anti-Virus Policy* and this Recommended Processes list for updates.

Password Policy

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 PIX Transmissions Ltd's entire corporate network. As such, all PIX Transmissions Ltd employees (including contractors and Business Partners with access to PIX Transmissions Ltd 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 PIX Transmissions Ltd facility, has access to the PIX Transmissions Ltd network, or stores any non-public PIX Transmissions Ltd information.

4.0 Policy
4.1 General
· All system-level passwords (e.g., root, enable, Windows admin, application administration accounts, etc.) must be changed on regular basis.
· All production system-level passwords must adhere to Information Security Password Best Practices.
· All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at regular intervals the recommended change interval is every 6 month.
· User accounts that have system-level privileges granted through group memberships 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 for network management, 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 PIX Transmissions Ltd. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, Email 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 "PIX Transmissions Ltd", "thane", "Jkgroup" 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 and is a passphrase (Ohmy1stubbedmyt0e).
· 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 PIX Transmissions Ltd accounts as for other non-PIX Transmissions Ltd access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various PIX Transmissions Ltd 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 Windows account and a third party account.
Do not share PIX Transmissions Ltd passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential PIX Transmissions Ltd information.
Here is a list of "I's":
· 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 senior or subordinate, unless approved by the Information Security Head.
· 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 the IT Security Head.
Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, and Netscape Messenger).
Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
Change passwords at least once every six months (except system-level passwords which must be changed quarterly).
The recommended change interval is every 1 month.
If an account or password is suspected to have been compromised, report the incident to Information Security and change all passwords.
Password cracking or guessing may be performed on a periodic or random basis by Information Security or its delegates with formal user approval. 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 strong security frameworks like 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 PIX Transmissions Ltd 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.

4.3 Enforcement

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

4.4 Definitions

Terms Definitions

Application Administration Account Any account that is for the administration of an application .

Database Password Policy

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 PIX Transmissions Ltd's networks. Computer programs running on PIX Transmissions Ltd's 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 PIX Transmissions Ltd, multi-user production database.

3.0 Policy

3.1 General

In order to maintain the security of PIX Transmissions Ltd'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 be adequately encrypted & not be openly 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, 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. Technical Retrieval of Database User Names and Passwords

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

3. 2.3 Access to Database User Names and Passwords

· Every program or every collection of programs implementing a single business function must have unique database credentials. Credentials may be mapped between programs. 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.

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

3.4 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.

Removable Media Policy

1.0 Overview
Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations leading to legal implications.

2.0 Purpose
To minimize the risk of loss or exposure of sensitive information maintained by PIX Transmissions Ltd and to reduce the risk of acquiring malware infections on computers operated by PIX Transmissions Ltd.

3.0 Scope
This policy covers all computers and servers operating in PIX Transmissions Ltd.

4.0 Policy
PIX Transmissions Ltd staff may only use PIX Transmissions Ltd removable media in their work computers. PIX Transmissions Ltd removable media may not be connected to or used in computers that are not owned or leased by the PIX Transmissions Ltd without explicit permission of the PIX Transmissions Ltd information technology & security staff. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies.
When Sensitive information is stored on removable media; it must be encrypted in accordance with the PIX Transmissions Ltd Acceptable Encryption Policy.
Exceptions to this policy may be requested on a case-by-case basis on formal approval & verification from the Information Security Head.

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

*Removable Media***:**	Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and any commercial music and software disks not provided by PIX Transmissions Ltd.
Encryption:	*A* procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.
Sensitive Information:	Information which, if made available to unauthorized persons, may adversely affect PIX Transmissions Ltd, its programs, or participants served by its programs. Examples include, but are not limited to, personal identifiers and , financial information.
Malware:	Software of malicious intent/impact such as viruses, worms, and Spyware.

Email Use Policy

1.0 Purpose
To comply with safe, secured & appropriate usage of PIX Transmissions Ltd email systems & prevent tarnishing the public image of PIX Transmissions Ltd when email goes out from PIX Transmissions Ltd as general public will tend to view that message as an official policy statement from the PIX Transmissions Ltd.

2.0 Scope
This policy covers appropriate use of any email sent from a PIX Transmissions Ltd email address and applies to all employees, Business Partners, operating on behalf of PIX Transmissions Ltd.

3.0 Policy
Currently Postmaster Ver 8 & MS Outlook with Web Access over SSL as email clients are used at PIX Transmissions Ltd. Adequate mailbox sizes have been allocated to users based on their Business needs & on existing Server space. Webmail will be issue on request with the approval of E-Mail & IT Security Admin.

3.1 Prohibited Use. The PIX Transmissions Ltd email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any PIX Transmissions Ltd employee should report the matter to their supervisor immediately. E-Mail sending more than 4 Mb attachments
will not be allow, the attachment size will differ as per the designation.

3.2 Personal Use.
Using any amount of PIX Transmissions Ltd Internet & resources for personal emails is not acceptable. Sending chain letters or joke emails from a PIX Transmissions Ltd email account is prohibited. Virus warnings or other malware warnings and mass mailings from PIX Transmissions Ltd shall be approved by PIX Transmissions Ltd Head of Information Security before sending.
These restrictions also apply to the forwarding of mail received by a PIX Transmissions Ltd employee.

3.3 Monitoring
PIX Transmissions Ltd employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. PIX Transmissions Ltd may monitor messages without prior notice. PIX Transmissions Ltd is not obliged to monitor email messages.

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**
Email:	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Forwarded email:	Email resent from an internal network to an outside point.
Chain email or letter:	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information:	Information is considered sensitive if it can be damaging to PIX Transmissions Ltd or its customers' reputation or market standing.
Virus warning:	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Unauthorized Disclosure:	The intentional or unintentional revealing of restricted information to people, both Inside and outside PIX Transmissions Ltd, who do not have a need to know that information.

Email Retention Policy

1. 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 IT Helpdesk.
Questions about these guidelines should be addressed to Information Security Head.

2. Scope

This email retention policy is secondary to PIX Transmissions Ltd *Email Use Policy*. Any email that contains information in the scope of the Business Record Keeping policy should be treated in that manner. All PIX Transmissions Ltd email information is categorized into four main classifications with retention guidelines:
Business Correspondence Administrative Correspondence
Fiscal Correspondence
Ephemeral Correspondence

3. Policy

Currently Hosted Email Solution & MS Outlook with Web Access over SSL as email clients are used at PIX Transmissions Ltd. Adequate mailbox sizes have been allocated to users based on their Business needs & on existing Server space.

3.1 Business Correspondence

PIX Transmissions Ltd Business 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. To ensure Business Correspondence is retained, personal folders on individual user systems can be configured.
Daily Backup of emails on the mail Server is done. Critical Users laptops & desktops are backed up through DLO agent's backups. IT team can provide assistance in configuring the Personal Folders.

3.2 Administrative Correspondence

PIX Transmissions Ltd Administrative Correspondence includes, though is not limited to clarification of established company policy, corporate directives, Human resource intimations like holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. To ensure Administrative Correspondence is retained, personal folders on individual user systems can be configured. Daily Backup of emails on the mail Server is done. Critical Users laptops & desktops are backed up timely IT team can provide assistance in configuring the Personal Folders.

3.3 Fiscal Correspondence

PIX Transmissions Ltd Fiscal Correspondence is all information related to revenue and expense for the company. To ensure Fiscal Correspondence is retained to ensure Fiscal Correspondence is retained, personal folders on individual user systems can be configured.
Daily Backup of emails on the mail Server is done. Critical Users laptops & desktops are backed up IT team can provide assistance in configuring the Personal Folders.

3.4 Ephemeral Correspondence

PIX Transmissions Ltd Ephemeral Correspondence is by far the largest category and includes personal email, daily requests for recommendations or review, email related to updates and status reports.
To ensure Ephemeral Correspondence is retained, personal folders on individual user systems can be configured.

Daily Backup of emails on the mail Server is done. Critical Users laptops & desktops are backed up. IT team can provide assistance in configuring the Personal Folders.

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

3.7 Recovering Deleted Email via Backup Media
PIX Transmissions Ltd maintains backup on Storage boxes & Hard disk of the email server from which Email archival can be done.

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

5. 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, Hosted Email Solution with Outlook 2007 clients & Web Access.

Approved Encrypted email and files
Techniques include the use of SSL, 3DES, DES and PGP.SSL & PGP use within PIX Transmissions Ltd is done via a license. Please contact the appropriate support organization if you require a license.
Approved Instant Messenger
The Skype Client is the only IM that is approved for use on PIX Transmissions Ltd computers.
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 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 PIX Transmissions Ltd.
Encryption Secure PIX Transmissions Ltd 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.

Automatically Forwarded Email Policy

1.0 Purpose
To prevent the unauthorized or inadvertent disclosure of sensitive company information over email systems.

2.0 Scope
This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, Business Partners, operating on behalf of PIX Transmissions Ltd.

3.0 Policy
Employees must exercise utmost caution when sending any email from inside PIX Transmissions Ltd to an outside network.
Unless approved by Information Security Head, PIX Transmissions Ltd 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*. Email forwarding within the organization can be done with approval of Process owner.

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. Programs such as Eudora and Microsoft Outlook use SMTP.
Forwarded email:	Email resent from internal networking to an outside point.
Sensitive information:	Information is considered sensitive if it can be damaging to PIX Transmissions Ltd 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.

Network Policy

1.0 Purpose:
To ensure that a secure method of network connectivity within PIX Transmissions Ltd and all third parties and to provide a formalized method for the request, approval and tracking of such connections.

2.0 Scope:
Data network connections to PIX Transmissions Ltd can create potential security exposures if not administered and managed correctly and consistently. These exposures may include non-approved methods of connection to the PIX Transmissions Ltd network, the inability to shut down access in the event of a security breach, and exposure to hacking attempts. Therefore, all external company data network connections will be via the approved Providers Network. This policy applies to all new Third Party Network Connection requests and any existing Third Party Network Connections. When existing Third Party Network Connections do not meet all of the guidelines and requirements outlined in this document, they will be re-engineered as needed.

3.0 Definitions:
A "Network Connection" is defined as one of the connectivity options listed in Section B. below. “Third Parties” is defined as PIX Transmissions Ltd, Business Partners, and the like.

A. Third-Party Connection Requests and Approvals
All requests for Third Party connections must be made using the appropriate method based on the support organization. The required information is outlined in the **Third Party Connection Request – Information Requirements Document** All information requested on this form must be completed prior to approval and sign off. It is Company’s responsibility to ensure that Company has provided all of the necessary information and that such information is correct.

All Third Party connection requests must have a Head IT Infrastructure signature for approval. In some cases approval may be given at a lower level with pre-authorization from the Head IT Infrastructure. Also, all Third Parties requesting a Network Connection must complete and sign a PIX Transmissions Ltd Non-Disclosure Agreement.

As a part of the request and approval process, the technical and administrative contact within Company’s organization or someone at a higher level within Company will be required to read and sign the "Third Party Connection Agreement” and any additional documents, such as the PIX Transmissions Ltd Non-Disclosure Agreement.

B. Connectivity Options
The following five connectivity options are the standard methods of providing a Third Party Network Connection.vAnything that deviates from these standard methods would not be entertained.

1) Leased line (e.g. T1) - Leased lines for Third Parties will be terminated on the Partners network.
2) ISDN/FR - Dial leased lines will terminate on a Third Party only router located on the IT Partners network. Authentication for these connections must be as stated in Section E. below.
3) Encrypted Tunnel - Encrypted tunnels should be terminated on the Partners Network whenever possible. In certain circumstances, it may be required to terminate an encrypted tunnel on the dirty subnet, in which case the normal PIX Transmissions Ltd perimeter security measures will control access to internal devices.
4) Telnet access from Internet - Telnet access from the Internet will be provided by first telneting to the Third Party gateway machine, where the connection will be authenticated per Section E. below. Once the connection is authenticated, telnet sessions to internal hosts will be limited to those services needed by using the authorization capabilities of PIX Transmissions Ltd Secure.
5) Remote Dial-up via PPP/SLIP - Remote dial-up via PPP/SLIP will be provided by a separate Third Party modem pool. The connection will be authenticated per Section E. below

C. Third Party (Partner) Access Points
When possible, Third Party (Partner) Access Points (PAPs should be established in locations such that the cost of the access is minimized. Each PAP should consist of at least one router with VPN, leased line, Broadband and/or ISDN capability.

D. Services Provided
In general, services provided over Third Party Network Connections should be limited only to those services needed, and only to those devices (hosts, routers, etc.) needed. **Blanket access will not be provided for anyone.**
The default policy position is to deny all access and then only allow those specific services that are needed and approved by PIX Transmissions Ltd pursuant to the established procedure.

In no case shall a Third Party Network Connection to PIX Transmissions Ltd be used as the Internet connection for the Third Party.
The standard set of allowable services are listed below:

File Exchange via ftp – Where possible, file exchange via ftp should take place on the existing PIX Transmissions Ltd ftp servers .IT supported Third Party connections have additional FTP services provided by a server in on the Partners Network.

Electronic Mail Exchange – Business-related email exchange between PIX Transmissions Ltd and Third Parties may be conducted over the Network Connection as needed. Mail from Third Party sites to non-PIX Transmissions Ltd addresses will not be allowed over the Network Connection.

Telnet Access – Telnet access will be provided to specific PIX Transmissions Ltd hosts, as needed. Employees from Third Parties will only be given accounts on the specific PIX Transmissions Ltd hosts that are needed. Where possible, router ACLs and static routes will be used to limit the paths of access to other internal PIX Transmissions Ltd hosts and devices.
NOTE: Domain accounts and Directory Services are not to be established for employees of Third Parties who have accounts on PIX Transmissions Ltd hosts.

Web Resource Access – Access to internal web resources will be provided on an as-needed basis. Access will be provided by mirroring the appropriate web resources to a web server that resides on the Partners Network. Access to PIX Transmissions Ltd's public web resources will be accomplished via the normal Internet access for the Third Party.

Access to Source Code Repositories This access will be decided on case by case basis with formal approvals.

Print Services – Print services can be provided to PIX Transmissions Ltd IT-supported Third Party connections by via two print spoolers on the PIX Transmissions Ltd Partners Network. PIX Transmissions Ltd-owned printers that boot off the print spoolers will be located on the PIX Transmissions Ltd –extended network at the Third Party sites.

Database Access – This will be decided on a case by case basis with formal approvals.

ERP Access – This will be decided on a case by case basis with formal approvals.

Windows File Exchange – File exchange will be provided by Windows file servers located on the PIX Transmissions Ltd
Partners Network. Each Third Party needing Windows File exchange will be provided with a separate folder that is only accessible to that Party and the necessary people at PIX Transmissions Ltd.

E. Authentication for Third Party Network Connections

Third Party Network Connections made via remote dial-up using PPP/SLIP or standard telnet over the Internet will be authenticated using the Partners Authentication databases, SSL VPN or Token Access System. A separate server will be established specifically for Third Parties. Reports showing who has access will be generated monthly and sent to the PIX Transmissions Ltd Information Security team for each Third Party for verification and review.
Telnet connection made via the Internet must be initiated to a separate which authenticates to the Partners Authentication database and Token Access System mentioned above.
ISDN connections will be authenticated via the Partners PIX Transmissions Ltd Secure database, which is separate from the PIX Transmissions Ltd ISDN authentication database.

F. PIX Transmissions Ltd Equipment at Third Party Sites
In many cases it may be necessary to have PIX Transmissions Ltd-owned and maintained equipment at a Third Party site. All such equipment will be documented on the Third Party Connection Request – Information Requirements Document.
Access to network devices such as routers and switches will only be provided to PIX Transmissions Ltd support personnel.
All PIX Transmissions Ltd-Owned Equipment located at Third Party sites must be used only for business purposes. Any misuse of access or tampering with PIX Transmissions Ltd-provided hardware or software, except as authorized in writing by PIX Transmissions Ltd, may, in PIX Transmissions Ltd's sole discretion, result in termination of the connection agreement with the Third Party. If PIX Transmissions Ltd equipment is loaned to a Third Party, the Third Party will be required to sign an
appropriate PIX Transmissions Ltd Equipment Loan Agreement, if one is required

G. Protection of Company Private Information and Resources
The PIX Transmissions Ltd network support group responsible for the installation and configuration of a specific Third Party Connection must ensure that all possible measures have been taken to protect the integrity and privacy of PIX Transmissions Ltd confidential information. At no time should PIX Transmissions Ltd rely on access/authorization control mechanisms at the Third Party's site to protect or prohibit access to PIX Transmissions Ltd confidential information. Security of Third Party Connections will be achieved by implementing "Access Control Lists" on the Partner Gateway routers to which the Third Party sites are connected. The ACLs will restrict access to pre-defined hosts within the internal PIX Transmissions Ltd network. The ACLs will be determined by the appropriate support organization.
A set of default ACLs may be established as a baseline.
Enable-level access to PIX Transmissions Ltd-owned/maintained routers on Third Party premise will only be provided to the appropriate support organization. All other business personnel (i.e. Partner Site local technical support personnel) will have restricted access/read-only access to the routers at stheir site and will not be allowed to make configuration changes.
PIX Transmissions Ltd shall not have any responsibility for ensuring the protection of Third Party information. The Third Party shall be entirely responsible for providing the appropriate security measures to ensure protection of their private internal network and information.

H. Audit and Review of Third Party Network Connections
All aspects of Third Party Network Connections - up to, but not including Company's firewall, will be monitored by the appropriate PIX Transmissions Ltd network support group. Where possible, automated tools will be used to accomplish the auditing tasks. Monthly reports should be generated on the Partners Authentication database showing the specific login entries and the appropriate PIX Transmissions Ltd POC. Each PIX Transmissions Ltd Partner POC will receive a copy of the monthly reports showing all of the accounts pertaining to his/her area. Copies of the reports will also be mailed to the department directors. Nightly audits will be performed on all PIX Transmissions Ltd-owned/maintained Third Party outer/network device configurations and the output will be mailed to the appropriate PIX Transmissions Ltd network support group. Any unauthorized changes will be investigated immediately.

All Third Party Network Connections will be reviewed on a quarterly basis and information regarding specific Third Party Network Connection will be updated as necessary. Obsolete Third Party Network Connections will be terminated.

I. PIX Transmissions Ltd Corporate IT Information Security Organization
PIX Transmissions Ltd Corporate IT Information Security has the responsibility for maintaining related policies and standards. Corporate IT Information Security will also provide advice and assistance regarding judgment calls, and will facilitate information gathering in order to make a correct decision. Coordination of confidentiality and nondisclosure agreements with all third parties is also the responsibility of PIX Transmissions Ltd Corporate IT Information Security.

J. PIX Transmissions Ltd Enterprise Network Services
The Enterprise Network Services Partners Group is responsible for all global firewall design, configuration and engineering required for support of the Global Partners Network.

Router Security Policy

1.0 Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of PIX Transmissions Ltd.

2.0 Scope

All routers and switches connected to PIX Transmissions Ltd production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the *Internet DMZ*
Equipment Policy.

3.0 Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers must use suitable authentication mechanisms like TACACS+ for all user authentications.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:

    a. IP directed broadcasts
    b. Incoming packets at the router sourced with invalid addresses.
    c. TCP small services
    d. UDP small services
    e. All source routing
    f. All web services running on router

4. Use corporate standardized SNMP community strings.
5. Access rules are to be added as business needs arise.
6. The router must be included in the corporate enterprise management system with a designated point of contact.
7. Each router must have the following statement posted in clear view:
   "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."
8. Telnet may never be used across any network to manage a router, unless there is a secure tunnel

   protecting the entire communication path. SSH is the preferred management protocol.

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

Production Network:	The "production network" is the network used in the daily business of PIX Transmissions Ltd. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to PIX Transmissions Ltd employees or impact their ability to do work.
Lab Network:	A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to PIX Transmissions Ltd nor affect the production network.

Remote Access Policy

1.0 Purpose

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

2.0 Scope

This policy applies to all PIX Transmissions Ltd employees, contractors, Business Partners with a PIX Transmissions Ltd-owned or personally-owned computer or workstation used to connect to the PIX Transmissions Ltd network. This policy applies to remote access connections used to do work on behalf of PIX Transmissions Ltd, 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

1. It is the responsibility of PIX Transmissions Ltd employees, contractors, Business Partners with remote access privileges to PIX Transmissions Ltd's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to PIX Transmissions Ltd.
2. General access to the Internet for recreational use by immediate household members through the PIX Transmissions Ltd Network on personal computers is permitted for employees that have flat-rate services. The PIX Transmissions Ltd employee is responsible to ensure the family member does not violate any PIX Transmissions Ltd policies, does not perform illegal activities, and does not use the access for outside business interests. The PIX Transmissions Ltd employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of PIX Transmissions Ltd's network:
    a. Acceptable Encryption Policy
    b. Virtual Private Network (VPN) Policy
    c. Wireless Communications Policy
    d. Acceptable Use Policy
4. For additional information regarding PIX Transmissions Ltd's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., request call should be logged to IT Helpdesk.

3.2 Requirements

1. 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 passphrase see the Password Policy.
2. At no time should any PIX Transmissions Ltd employee provide their login or email password to anyone, not even family members.
3. PIX Transmissions Ltd employees and contractors with remote access privileges must ensure that their PIX Transmissions Ltd-owned or personal computer or workstation, which is remotely connected to PIX Transmissions Ltd'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.
4. PIX Transmissions Ltd employees and contractors with remote access privileges to PIX Transmissions Ltd's corporate network must not use non-PIX Transmissions Ltd email

accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct PIX Transmissions Ltd business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the PIX Transmissions Ltd network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI (Data Link Connection Identifier) standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and Information Security must approve security configurations for access to hardware.
9. All hosts that are connected to PIX Transmissions Ltd 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*.
10. Personal equipment that is used to connect to PIX Transmissions Ltd's networks must meet the requirements of PIX Transmissions Ltd-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the PIX Transmissions Ltd production network must obtain prior approval from It Infrastructure and Information Security Head.

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 Internet service provider (ISP). Being on a PIX Transmissions Ltd provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into PIX Transmissions Ltd 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 64 Kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access: Any access to PIX Transmissions Ltd's corporate network through a non-PIX Transmissions Ltd controlled network, device, or medium.

Split-tunneling: Simultaneous direct access to a non-PIX Transmissions Ltd network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into PIX Transmissions Ltd'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.

Mobile Computing Policy

1.0 Purpose:
The purpose of this policy is to establish an authorized method for controlling mobile computing and storage devices that contain or access information resources at the PIX Transmissions Ltd.

2.0 Background/History:
With advances in computer technology, mobile computing and storage devices have become useful tools to meet the business needs at the PIX Transmissions Ltd. These devices are especially susceptible to loss, theft, hacking, and the distribution of malicious software because they are easily portable and can be used anywhere. As mobile computing becomes more widely used, it is necessary to address security to protect information resources at the PIX Transmissions Ltd.

3.0 Persons Affected:
PIX Transmissions Ltd employees, consultants, Business Partners, contractors, students, and others who use mobile computing and storage devices on the network at the PIX Transmissions Ltd.

4.0 Policy:
It is the policy of the PIX Transmissions Ltd that mobile computing and storage devices containing or accessing the information resources at the PIX Transmissions Ltd must be approved prior to connecting to the information systems at the PIX Transmissions Ltd. This pertains to all devices connecting to the network at the PIX Transmissions Ltd, regardless of ownership. Mobile computing and storage devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or PIX Transmissions Ltd owned, that may connect to or access the information systems at the PIX Transmissions Ltd. A risk analysis for each new media type shall be conducted and documented prior to its use or connection to the network at the PIX Transmissions Ltd unless the media type has already been approved by the Desktop Standards Committee. The Desktop Standards Committee will maintain a list of approved mobile computing and storage devices.
Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorized access and introduction of malicious software to the network at the PIX Transmissions Ltd. These risks must be mitigated to acceptable levels. Portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive PIX Transmissions Ltd information must use encryption or equally strong measures to protect the data while it is being stored. Unless written approval has been obtained from the Data Resource Manager and Chief Information Security Officer, databases or portions thereof, which reside on the network at the PIX Transmissions Ltd, shall not be downloaded to mobile computing or storage devices.

Technical personnel and users, which include employees, consultants, Business Partners, contractors, and students, shall have knowledge of, sign, and adhere to the Computer Use and Information Security Policy Agreement
(PIX Transmissions Ltd). Compliance with the Remote Access Standards, the Mobile Media Standards, and other applicable policies, procedures, and standards is mandatory.

5.0 Procedures:
Minimum Requirements:
· To report lost or stolen mobile computing and storage devices, call the Enterprise Help Desk at 07104-669123.
· The PIX Transmissions Ltd IT Infrastructure Head shall approve all new mobile computing and storage devices that may connect to information systems at the PIX Transmissions Ltd.
· Any non-departmental owned device that may connect to the PIX Transmissions Ltd network must first be approved by technical personnel such as those from the PIX Transmissions Ltd Desktop Support.
· Submit requests for an exception to this policy to the Information Security Head.

6.0 Roles and Responsibilities:

Users of mobile computing and storage devices must diligently protect such devices from loss of equipment and disclosure of private information belonging to or maintained by the PIX Transmissions Ltd and they must annually complete the PIX Transmissions Ltd. Before connecting a mobile computing or storage device to the network at PIX Transmissions Ltd, users must ensure it is on the list of approved devices.

The **Enterprise Help Desk** must be notified immediately upon detection of a security incident, especially when a mobile device may have been lost or stolen.

The **IT Infrastructure Team** is responsible for the mobile device policy at the PIX Transmissions Ltd and shall conduct a risk analysis to document safeguards for each media type to be used on the network or on equipment owned by the PIX Transmissions Ltd.

The **Information Security Head** is responsible for developing procedures for implementing this policy. The Desktop Standards Committee will maintain a list of approved mobile computing and storage devices and will make the list available on the intranet.

6.0 Definitions:

CD: A *compact disc* (sometimes spelled *disk)* is a small, portable, round medium made of molded polymer (close in size to the floppy disc) for electronically recording, storing, and playing back audio, video, text, and other information in digital form.

DVD: The *digital versatile disc* stores much more than a CD and is used for playing back or recording movies. The audio quality on a DVD is comparable to that of current audio compact discs. A DVD can also be used as a backup media because of its large storage capacity.

Flash Drive: A plug-and-play portable storage device that uses flash memory and is lightweight enough to attach to a key chain. The computer automatically recognizes the removable drive when the device is plugged into its USB port. A flash drive is also known as a keychain drive, USB drive, or disk-on-key. A keychain drive, which looks very much like an ordinary highlighter marker pen, can be used in place of a floppy disk, Zip drive disk, or CD.

Handheld wireless device: A communication device small enough to be carried in the hand or pocket and is also known as a Personal Digital Assistant (PDA). Various brands are available, and each performs some similar or some distinct functions. It can provide access to other internet services, can be centrally managed via a server, and can be configured for use as a phone or pager. In addition, it can include software for transferring files and for maintaining a built-in address book and personal schedule.

Media Type: For the purpose of this policy, the term “media type” is interchangeable with “mobile device.” Not to be confused with media makes, models, or brands.

Media Type Model: Refers to the brand of media device such as Sony, Treo, or IBM.

Mobile Devices: Mobile media devices include, but are not limited to: PDAs, plug-ins, USB port devices, CDs, DVDs, flash drives, modems, handheld wireless devices, and any other existing or future media device.

Modems: A device that modulates and demodulates information so that two computers can communicate over a phone line, cable line, or wireless connection. The connection talks to the modem, which connects to another modem that in turn talks to the computer on its side of the connection. The two modems talk back and forth until the two computers have no further need of either modem’s translation services.

PDA: The *Personal Digital Assistant* is also known as a handheld. It is any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use, often for keeping schedule calendars and address book information handy.
Many people use the name of one of the popular PDA products as a generic term, such as Hewlett-Packard's Palmtop and 3Com's PalmPilot.

Plug-In: Programs that can easily be installed and used as part of your Web browser. A plug-in application is recognized automatically by the browser, and its function is integrated into the main

HTML file that is being presented. Among popular plug-ins is Adobe's Acrobat, a document presentation and navigation program that provides a view of documents just as they look in the print medium. There are hundreds of plug-in devices.

Wireless Networking Cards: Mobile device for wireless internet connectivity from a laptop. This card allows mobile users the ability to access a secured connection to the internet via a specified vendor.

Personal Communication Devices and Email Policy

1.0 Purpose
This document describes Information Security's requirements for Personal Communication Devices and Email for PIX Transmissions Ltd.

2.0 Scope
This policy applies to any use of Personal Communication Devices and PIX Transmissions Ltd Email issued by PIX Transmissions Ltd or used for PIX Transmissions Ltd business.

3.0 Policy
3.1 Issuing Policy
Personal Communication Devices (PCDs) will be issued only to PIX Transmissions Ltd personnel with duties that require them to be in immediate and frequent contact when they are away from their normal work locations. For the purpose of this policy, PCDs are defined to include handheld wireless devices, cellular telephones, laptop wireless cards and pagers. Effective distribution of the various technological devices must be limited to persons for whom the productivity gained is appropriate in relation to the costs incurred. Handheld wireless devices may be issued, for operational efficiency, to PIX Transmissions Ltd personnel who need to conduct immediate, critical PIX Transmissions Ltd business. These individuals generally are at the executive and management level. In addition to verbal contact, it is necessary that they have the capability to review and have documented responses to critical issues.

3.2 Bluetooth
Hands-free enabling devices, such as the Bluetooth, may be issued to authorized PIX Transmissions Ltd personnel who have received approval. Care must be taken to avoid being recorded when peering Bluetooth adapters; Bluetooth 2.0
Class 1 devices have a range of 330 feet.

3.3 Email
Email boxes may be issued to PIX Transmissions Ltd personnel who require a method for others to leave messages when they are not available. Email boxes must be protected by a PIN which must never be the same as the last four digits of the telephone number of the Email box.

3.4 Loss and Theft
Files containing confidential or sensitive data may not be stored in PCDs unless protected by approved encryption. Confidential or sensitive data shall never be stored on a personal PCD. Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the employee, as determined on a case-by-case basis. The cost of any item beyond the standard authorized equipment is also the responsibility of the employee. Lost or stolen equipment must immediately be reported.

3.5 Personal Use
PCDs and Email are issued for PIX Transmissions Ltd business. Personal use should be limited to minimal and incidental use.

3.6 PCD Safety
Conducting telephone calls or utilizing PCDs while driving can be a safety hazard. Drivers should use PCDs while parked or out of the vehicle. If employees must use a PCD while driving, PIX Transmissions Ltd requires the use of hands free enabling devices.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action that leads to being ineligible for continued use of PCDs. Extreme cases could lead to additional discipline, up to and including termination of employment.

5.0 Definitions

Term Definition

Bluetooth: Bluetooth is an industrial specification for wireless personal area networks (PANs), also known as IEEE 802.15.1. Bluetooth provides a way to connect and exchange information between devices such as personal digital assistants (PDAs), and mobile phones via a secure, globally unlicensed short-range radio frequency.
Source: Wikipedia

Confidential or sensitive data: All data that is not approved for public release shall be considered confidential or sensitive.

Virtual Private Network (VPN) Policy

1.0 Purpose
The purpose of this policy is to provide guidelines for Remote Access VPN, SSL, IPSec or L2TP Virtual Private Network (VPN) connections to the PIX Transmissions Ltd corporate network.

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

3.0 Policy
Approved PIX Transmissions Ltd employees and authorized third parties (customers, Business Partners, 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,
1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to PIX Transmissions Ltd internal networks.
2. 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.
3. 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.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by PIX Transmissions Ltd network operational groups.
6. All computers connected to PIX Transmissions Ltd internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard; this includes personal computers.
7. VPN users will be automatically disconnected from PIX Transmissions Ltd'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.
8. The VPN Firewall is limited to an absolute connection time of 24 hours.
9. Users of computers that are not PIX Transmissions Ltd-owned equipment must configure the equipment to comply with PIX Transmissions Ltd's VPN and Network policies.
10. Only Information Security-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of PIX Transmissions Ltd's network, and as such are subject to the same rules and regulations that apply to PIX Transmissions Ltd-owned equipment, i.e., their machines must be configured to comply with 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.

Extranet Policy

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

2.0 Scope
Connections between third parties that require access to non-public PIX Transmissions Ltd resources fall under this policy, regardless of whether a Telco circuit (such as Broadband, Leased line 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 PIX Transmissions Ltd 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 (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 PIX Transmissions Ltd require that the third party and PIX Transmissions Ltd representatives agree to and sign the *Third Party Agreement*. This agreement must be signed by the Head of Department 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 PIX Transmissions Ltd are to be kept on file with the IT Infrastructure Team.

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. Test or Lab connections must be approved by the IT Infrastructure Head. 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 PIX Transmissions Ltd 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 Information Security to address security issues inherent in the project. If the proposed connection is to terminate within a Test lab at PIX Transmissions Ltd, the Sponsoring Organization must engage the It Infrastructure Team. The Sponsoring Organization must provide full and complete information as to the nature of the proposed access to the extranet group and 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 PIX Transmissions Ltd rely upon the third party to protect PIX Transmissions Ltd'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 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 PIX Transmissions Ltd 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 PIX Transmissions Ltd 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 PIX Transmissions Ltd business necessitate a modification of existing permissions, or termination of connectivity, 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 PIX Transmissions Ltd organization who requested that the third party have access into PIX Transmissions Ltd.

Third Party: *A* business that is not a formal or subsidiary part of PIX Transmissions Ltd.

ISDN/Analog Line Security Policy

1.0 Purpose
This document explains PIX Transmissions ltd ISDN & analog 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 backup to WAN links, 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 PIX Transmissions ltd 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 ISDN/analog line misuse, which we attempt to guard against through this policy. The first is an outside attacker who calls a set of ISDN/analog line numbers in the hope of connecting to a computer that has a modem attached to it. If the modem answers from inside PIX Transmissions ltd premises, then there is the possibility of breaching PIX Transmissions ltd'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.
The second scenario is the threat of anyone with physical access into a PIX Transmissions ltd 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 PIX Transmissions ltd through the computer's Ethernet connection, and then call out to an unmonitored site using the modem, with the ability to siphon PIX Transmissions ltd 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 PIX Transmissions ltd's internal network.
· The line will be used solely for PIX Transmissions ltd business, and not for personal reasons.
· All downloaded material, prior to being introduced into PIX Transmissions ltd systems and networks, must have been scanned by an approved anti-virus utility which has been kept current through regular updates.

3.3 Computers-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 PIX Transmissions ltd will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to PIX Transmissions ltd, 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 ISDN/Analog Line
Once approved by a manager, the individual requesting an analog/ISDN line must provide the following information to Telecom dept:
· a clearly detailed business case of why other secure connections available at PIX Transmissions ltd cannot be used,
· the business purpose for which the ISDN/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 PIX Transmissions ltd-equipped desktop computer with Internet capability unable to accomplish the same tasks as the proposed ISDN/analog line?
· Why is PIX Transmissions ltd's current dial-in/out VPN access pool unable to accomplish the same tasks as an ISDN/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 ISDN/analog lines be physically disconnected from PIX Transmissions ltd's internal network?
· Where will the ISDN/analog line be placed? A cubicle or lab?
· Is dial-in from outside of PIX Transmissions ltd 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 PIX Transmissions ltd-authorized anti-virus scanner be installed on the machine(s) using the analog lines?
· The requester should use the ISDN/Analog Line Request Form to address these issues and submit a request to Telecom dept.

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

Internet DMZ Equipment Policy

1.0 Purpose
The purpose of this policy is to define standards to be met by all equipment owned and/or operated by PIX Transmissions Ltd located outside PIX Transmissions Ltd's corporate Internet firewalls. These standards are designed to minimize the potential exposure to PIX Transmissions Ltd from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of PIX Transmissions Ltd resources.
Devices that are Internet facing and outside the PIX Transmissions Ltd 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:
· Ownership responsibility
· Secure configuration requirements
· Operational requirements
· Change control requirement

2.0 Scope
All equipment or devices deployed in a DMZ owned and/or operated by PIX Transmissions Ltd (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by PIX Transmissions Ltd, 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 "PIX Transmissions. In" domain or appears to be owned by PIX Transmissions Ltd. 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 Information Security. All existing and future equipment deployed on PIX Transmissions Ltd'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 Information Security for 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 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, 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:

- Hardware, operating systems, services and applications must be approved by Information Security as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration.
- All patches/hot-fixes recommended by the equipment vendor and 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/hot fixes.

· 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 Information Security.
· Services and applications not for general access must be restricted by access control lists.
· Insecure services or protocols (as determined by 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 SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords (SSL, 3DES/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 Information Security-approved logs. Security-related events include (but are not limited to) the following:
    o User login failures.
    o Failure to obtain privileged access.
    o Access policy violations.
· 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.
· Information Security must be invited to perform system/application audits prior to the deployment of new services.
· 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 (de-militarized zone) :	Any un-trusted network connected to, but separated from, PIX Transmissions Ltd's corporate network by a firewall, used for external (Internet/partner, etc.) access from within PIX Transmissions Ltd, 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.

Internal Lab (IT Test Environment) Security Policy

1.0 Purpose

This policy establishes information security requirements for PIX Transmissions Ltd IT Test /Development labs to ensure that PIX Transmissions Ltd confidential information and technologies are not compromised, and that production services and other PIX Transmissions Ltd interests are protected from Test Environment activities.

2.0 Scope

This policy applies to all internally connected labs, PIX Transmissions Ltd employees and third parties who access PIX Transmissions Ltd's 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. Test Environment owning organizations are responsible for assigning Test Environment managers, a point of contact (POC), and a back-up POC for each lab. Test Environment owners must maintain up-to-date POC information with Information Security and the Corporate Enterprise Management Team. Test Environment managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.
2. Test Environment managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Test Environment managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined Test Environment managers must do their best to safeguard PIX Transmissions Ltd from security vulnerabilities.
3. Test Environment managers are responsible for the lab's compliance with all PIX Transmissions Ltd 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 Test Environment Manager is responsible for controlling Test Environment access. Access to any given Test Environment will only be granted by the Test Environment 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 Test Environment have their access terminated.
5. The Network Support Organization must maintain a firewall device between the corporate production network and all Test Environment equipment.
6. The Network Support Organization and/or Information Security reserve the right to interrupt Test Environment connections that impact the corporate production network negatively or pose a security risk.
7. The Network Support Organization must record all Test Environment IP addresses, which are routed within PIX Transmissions Ltd networks, in Enterprise Address Management database along with current contact information for that lab.
8. Any Test Environment that wants to add an external connection must provide a diagram and documentation to Information Security with business justification, the equipment, and the IP address space information. Information Security will review for security concerns and must approve before such connections are implemented.
9. All user passwords must comply with PIX Transmissions Ltd's *Password Policy*. In addition, individual user accounts on any Test Environment device must be deleted when no longer authorized within three (3) days. Group account passwords on Test Environment computers (UNIX, windows, etc) must be changed quarterly (once every 3 months).
For any Test Environment device that contains PIX Transmissions Ltd proprietary information, group account passwords must be changed within three (3) days following a change in group membership.
10. No Test Environment 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 designated Teams..

11. 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 Test Environment network must go through a Network Support Organization maintained firewall. Test Environment network devices (including wireless) must not cross connect the Test Environment and production networks.
2. Original firewall configurations and any changes thereto must be reviewed and approved by Information Security. 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-PIX Transmissions Ltd networks. These activities must be restricted within the lab.
4. Traffic between production networks and Test Environment networks, as well as traffic between separate Test Environment 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 Test Environment confidential information at risk.
5. 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. Test Environment owned gateway devices are required to comply with all PIX Transmissions Ltd product security advisories and must authenticate against the Corporate Authentication servers.
7. The enable password for all Test Environment owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with PIX Transmissions Ltd's *Password Policy*. The password will only be provided to those who are authorized to administer the Test Environment network.
8. In labs where non-PIX Transmissions Ltd personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no PIX Transmissions Ltd 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 Information Security.
9. Infrastructure devices needing corporate network connectivity must adhere to the *Network Policy.*
10. All Test Environment external connection requests must be reviewed and approved by 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 PIX Transmissions Ltd 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 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 Test Environment that is within PIX Transmissions Ltd's corporate firewall and connected to PIX Transmissions Ltd's corporate production network
· *Network Support Organization* - Any Information Security approved PIX Transmissions Ltd support organization that manages the networking of non-Test Environment networks.
· *Test Environment Manager* - The individual responsible for all Test Environment activities and personnel
· *Test Environment*- A Test Environments 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.
· *Test Environment Owned Gateway Device* - A Test Environment owned gateway device is the Test

Environment device that connects the Test Environment network to the rest of PIX Transmissions Ltd network. All traffic between the Test Environment and the corporate production network must pass through the Test Environment owned gateway device unless approved by Information Security.

· *Telco* - A Telco is the equivalent to a service provider. Telco's offer network connectivity, e.g., T1, T3, OC3, OC12 or DSL. Telco's are sometimes referred to as "baby bells", although Sprint and AT&T are also considered Telco's. 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 PIX, a router with access control lists or similar security devices approved by Information Security.
· *Extranet* - Connections between third parties that require access to connections non-public PIX Transmissions Ltd
resources, as defined in Information Security's extranet policy (link).
· *DMZ (De-Militarized Zone)* - This describes network that exists outside of primary corporate firewalls, but are still under PIX Transmissions Ltd administrative control.

DMZ Lab Security Policy

1.0 Purpose

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

2.0 Scope

PIX Transmissions Ltd Lab networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located outside PIX Transmissions Ltd 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 PIX Transmissions Ltd's corporate Internet firewalls. Standards for these labs are defined in the *Internal Lab Security Policy*

3.0 Policy

3.1. Ownership and Responsibilities

1. All new DMZ Labs must present a business justification with sign-off at the business unit Head of Department level. IT Infrastructure Team must keep the business justifications on file.
2. 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 Information Security Lab managers or their backup must be available around-the-clock for emergencies.
3. Changes to the connectivity and/or purpose of existing DMZ Labs and establishment of new DMZ Labs must be requested through a PIX Transmissions Ltd Network Support Organization and approved by Information Security.
4. All ISP connections must be maintained by a PIX Transmissions Ltd Network Support Organization.
5. A Network Support Organization must maintain a firewall device between the DMZ Lab(s) and the Internet.
6. The Network Support Organization and Information Security reserve the right to interrupt lab connections if a security concern exists.
7. The DMZ Lab will provide and maintain network devices deployed in the DMZ Lab up to the Network Support Organization point of demarcation.
8. The Network Support Organization must record all DMZ Lab address spaces and current contact information.
9. The DMZ Lab Managers are ultimately responsible for their DMZ Labs complying with this policy.
10. Immediate access to equipment and system logs must be granted to members of Information Security and the Network Support Organization upon request, in accordance with the *Audit Policy*
11. 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.
12. 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 PIX Transmissions Ltd'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:

a. Password Policy
b. Wireless Communications Policy

5. The Network Support Organization maintained firewall devices must be configured in accordance with least-access principles and the DMZ Lab business needs. All firewall filters will be maintained by Information Security.
6. The firewall device must be the only access point between the DMZ Lab and the rest of PIX Transmissions Ltd's 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 Information Security (including both general configurations and rule sets). Information Security may require additional security measures as needed.
8. Traffic from DMZ Labs to the PIX Transmissions Ltd 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.
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/hot fixes.
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. PIX Transmissions Ltd Confidential information is prohibited on equipment in labs where non-PIX Transmissions Ltd 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 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 (de-militarized zone):*Networking that exists outside of PIX Transmissions Ltd primary corporate firewalls, but is still under PIX Transmissions Ltd administrative control.
Network Support Organization: Any 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 Point of Demarcation: The point at which the networking responsibility transfers from a 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 Information Security.
Internally Connected Lab: A lab within PIX Transmissions Ltd's corporate firewall and connected to the corporate production network.

Wireless Communication Policy

1 Overview
The purpose of this policy is to secure and protect the information assets owned by PIX Transmissions Ltd. PIX Transmissions Ltd provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. PIX Transmissions Ltd grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets. This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to PIX Transmissions Ltd network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to a PIX Transmissions Ltd network.

2 Scope
All employees & consultants at PIX Transmissions Ltd, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of PIX Transmissions Ltd must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a PIX Transmissions Ltd network or reside on a PIX Transmissions Ltd site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.
The Information Security Head is authorized to approve exceptions to this policy in advance.

3 Policy Statement

3.1 General Network Access Requirements
All wireless infrastructure devices that reside at a PIX Transmissions Ltd site and connect to a PIX Transmissions Ltd network, or provide access to information classified as PIX Transmissions Ltd Confidential, PIX Transmissions Ltd Highly Confidential, or PIX Transmissions Ltd Restricted must:

3.1.1 Abide by the standards specified in the Wireless Communication Standard.
3.1.2 Be installed, supported, and maintained by a approved support team.
3.1.3 Use PIX Transmissions Ltd approved authentication protocols and infrastructure.
3.1.4 Use PIX Transmissions Ltd approved encryption protocols.
3.1.5 Maintain a hardware address (MAC address) that can be registered and tracked.
3.1.6 Not interfere with wireless access deployments maintained by other support organizations.

3.2 Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to PIX Transmissions Ltd Confidential, PIX Transmissions Ltd Highly Confidential, or PIX Transmissions Ltd Restricted information must adhere to section 3.1. Lab and isolated wireless devices that do not provide general network connectivity to the PIX Transmissions Ltd network must:
3.2.1 Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the DMZ Lab Security Policy or the Internal Lab Security Policy.
3.2.2 Not interfere with wireless access deployments maintained by other support organizations.

3.3 SOHO Wireless Device Requirements
3.3.1 Wireless infrastructure devices that provide direct access to the PIX Transmissions Ltd corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.
3.3.2 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the PIX Transmissions Ltd corporate network. Access to the PIX Transmissions Ltd corporate network through this device must use standard remote access authentication.

4 Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with PIX Transmissions Ltd.

5 Definitions

Term	**Definition**
PIX Transmissions Ltd network:	A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to corporate services.
Corporate connectivity:	A connection that provides access to a PIX Transmissions Ltd network.
Enterprise Class Teleworker (ECT):	An end-to-end hardware VPN solution for teleworker access to the PIX Transmissions Ltd network.
Information assets:	Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organization.
MAC address:	The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network.

Wireless Communication Standard

1 Overview

The purpose of this standard is to secure and protect the information assets owned by PIX Transmissions Ltd. PIX Transmissions Ltd provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. PIX Transmissions Ltd grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets. This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a PIX Transmissions Ltd network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the Information Security Team are approved for connectivity to a PIX Transmissions Ltd network.

2 Scope

All employees, contractors, consultants, temporary and other workers at PIX Transmissions Ltd, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of PIX Transmissions Ltd must adhere to this standard. This standard applies to all wireless infrastructure devices that connect to a PIX Transmissions Ltd network or reside on a PIX Transmissions Ltd site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.
The PIX Transmissions Ltd Information Security Team must approve exceptions to this policy in advance.

3 Statement of Requirements

3.1 General Requirements

All wireless infrastructure devices that connect to a PIX Transmissions Ltd network or provide access to PIX Transmissions Ltd Confidential, PIX Transmissions Ltd Highly Confidential, or PIX Transmissions Ltd

Restricted information must:
3.1.1 Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
3.1.2 Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.

3.2 Lab and Isolated Wireless Device Requirements

3.2.1 Lab device Service Set Identifier (SSID) must be different from PIX Transmissions Ltd production device SSID.
3.2.2 Broadcast of lab device SSID must be disabled.

3.3 Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a PIX Transmissions Ltd network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

3.3.1 Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
3.3.2 When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
3.3.3 Disable broadcast of SSID
3.3.4 Change the default SSID name
3.3.5 Change the default login and password

4 References

In support of this standard, the following policies, guidelines, and resources are included:
Information Sensitivity Policy
Wireless Communication Policy

5 Enforcement

This standard is part of the Wireless Communication Policy and failure to conform to the standard is a violation of the policy. Any employee found to have violated the policy may be subject to disciplinary action, up to and including termination of employment. Any violation of the policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with PIX Transmissions Ltd.

6 Definitions

Term	**Definition**
AES:	Advanced Encryption System
PIX Transmissions Ltd network:	A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to corporate services.
Corporate connectivity:	A connection that provides access to a PIX Transmissions Ltd network.
EAP-FAST :	Extensible Authentication Protocol-Fast Authentication via Secure Tunneling authentication protocol for wireless networks.
EAP-TLS:	Extensible Authentication Protocol-Translation Layer Security, used to create a secured connection for 802.1X by pre-installing a digital certificate on the client computer.
Enterprise Class Teleworker (ECT) :	An end-to-end hardware VPN solution for teleworker access to the PIX Transmissions Ltd network.
Information assets:	Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organization.
PEAP :	Protected Extensible Authentication Protocol, a protocol used for transmitting authentication data, including passwords, over 802.11 wireless networks
Service Set Identifier (SSID):	A set of characters that give a unique name to a wireless local area network.
TKIP:	Temporal Key Integrity Protocol, an encryption key that's part of WPA.
WPA-PSK:	WiFi Protected Access pre-shared key

Acceptable Encryption Policy

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 Indian IT Law & regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the India.

2.0 Scope
This policy applies to all PIX Transmissions Ltd employees and affiliates.

3.0 Policy
Proven, standard algorithms such as SSL, AES, and 3DES, DES, Blowfish, RSA, RC5 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. PIX Transmissions Ltd'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 Information Security. Employees residing in countries other than the India 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 are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

Application Service Providers (ASP) Policy

1.0 Purpose
This document describes Information Security's requirements of Application Service Providers (ASPs) that engage with PIX Transmissions Ltd.

2.0 Scope
This policy applies to any use of Application Service Providers by PIX Transmissions Ltd, independent of where hosted.

3.0 Policy
3.1 Requirements of Project Sponsoring Organization
The ASP Sponsoring Organization must first establish that its project is an appropriate one for the ASP model, prior to engaging any additional infrastructure teams within PIX Transmissions Ltd or ASPs external to the company. The person/team wanting to use the ASP service must confirm that the ASP chosen to host the application or project complies with this policy. The Business Function to be outsourced must be evaluated against the following:
1. The requester must go through the ASP engagement process with the ASP Team to ensure affected parties are properly engaged.
2. In the event that PIX Transmissions Ltd data or applications are to be manipulated by, or hosted at, an ASP's service, the ASP sponsoring organization must have written, explicit permission from the data/application owners.
A copy of this permission must be provided to Information Security.
3. The information to be hosted by an ASP must fall under the "Minimal" or "More Sensitive" categories. Information that falls under the "Most Sensitive" category may not be outsourced to an ASP. Refer to the *Information Sensitivity Policy* for additional details.
4. If the ASP provides confidential information to PIX Transmissions Ltd, the ASP sponsoring organization is responsible for ensuring that any obligations of confidentiality are satisfied. This includes information contained in the ASP's application. PIX Transmissions Ltd's legal services department should be contacted for further guidance if questions about third-party data arise.
Projects that do not meet these criteria may not be deployed to an ASP.

3.2 Requirements of the Application Service Provider
Information Security has created an associated document, entitled *ASP Security Standards* that sets forth the minimum security requirements for ASPs. The ASP must demonstrate compliance with these Standards in order to be considered for use.
The ASP engagement process includes an Information Security evaluation of security requirements. The *ASP Security Standards* can be provided to ASPs that are either being considered for use by PIX Transmissions Ltd, or have already been selected for use.
Information Security may request that additional security measures be implemented in addition to the measures stated in the *ASP Security Standards* document, depending on the nature of the project. Information Security may change the requirements over time, and the ASP is expected to comply with these changes.
*ASPs that do not meet these requirements may not qualify for PIX Transmissions Ltd Systems projects***.**

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

Application Service Provider (ASP):	ASPs combine hosted software, hardware and networking technologies to offer a service-based application, as opposed to a

	PIX Transmissions Ltd owned and operated application. Common ASP offerings include enterprise resource planning (ERP), collaboration and sales force automation tools, but are not limited to these things.
ASP Sponsoring Organization:	The group within PIX Transmissions Ltd that wishes to utilize the services of an ASP.
Business Function:	The business need that a software application satisfies. Managed by an ASP that hosts an application on behalf of PIX Transmissions Ltd.

Application Service Providers Security Standards

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 PIX Transmissions Ltd. 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. Information Security will closely review the vendor responses, and will suggest remediation measures in any areas that fall short of the minimum security criteria. 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 Information Security.

2.0 Scope

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

3.0 Responding to These Standards

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:

Non Qualifying Answer: "We have hardened our hosts against attack."
Qualifying Answer: "We have applied all security patches for Windows 2012 as of 31-Mar-2016 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.
Critical updates are implemented within 24 hours. A complete list of applied patches is available to PIX TransmissionsLtd."
Non Qualifying Answer: "We use encryption."
Qualifying Answer: "All communications between our site and PIX Transmissions Ltd will be protected by IPSec ESP Tunnel mode using 168-bit Triple DES 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

1. PIX Transmissions Ltd reserves the right to periodically audit the PIX Transmissions Ltd application infrastructure to ensure compliance with the ASP Policy and these Standards. Non-intrusive network audits (basic port scans, etc.)
may be done randomly, without prior notice. More intrusive network and physical audits may be conducted on site with 24 hours notice.
2. The ASP must provide a proposed architecture document that includes a full network diagram of the PIX Transmissions Ltd Application Environment, illustrating the relationship between the Environment and any other relevant networks, with a full data flowchart that details where PIX Transmissions Ltd data resides, the applications that manipulate it, and the security thereof.
3. 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

1. The equipment hosting the application for PIX Transmissions Ltd must be located in a physically secure facility, which requires badge access at a minimum.
2. The infrastructure (hosts, network equipment, etc.) hosting the PIX Transmissions Ltd application must be located in a locked cage-type environment.

3. PIX Transmissions Ltd shall have final say on who is authorized to enter any locked physical environment, as well as access the PIX Transmissions Ltd Application Infrastructure.
4. The ASP must disclose who amongst their personnel will have access to the environment hosting the application for PIX Transmissions Ltd.
5. PIX Transmissions Ltd's Information Security Policy requires that the ASP disclose their ASP background check procedures and results prior to Information Security granting approval for use of an ASP.

4.3 Network Security

1. The network hosting the application must be air-gapped from any other network or customer that the ASP may have. This means the PIX Transmissions Ltd application environment must use separate hosts, and separate infrastructure.
2. Data flow between PIX Transmissions Ltd & ASP can be allowed following two things:
    a. If PIX Transmissions Ltd will be connecting to the ASP via a private circuit (such as frame relay, etc.), then that circuit must terminate on the PIX Transmissions Ltd extranet, and the operation of that circuit will come under the procedures and policies that govern the PIX Transmissions Ltd Partner Network Management Group.
    b. If, on the other hand, the data between PIX Transmissions Ltd and the ASP will go over a public network such as the Internet, appropriate firewalling technology must be deployed by the ASP, and the traffic between PIX Transmissions Ltd and the ASP must be protected and authenticated by cryptographic technology
    (See Cryptography below).

4.4 Host Security

1. The ASP must disclose how and to what extent the hosts (UNIX, Windows, etc.) comprising the PIX Transmissions Ltd application infrastructure have been hardened against attack. If the ASP has hardening documentation for the CAI, provide that as well.
2. The ASP must provide a listing of current patches on hosts, including host OS patches, web servers, databases, and any other material application.
3. 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?
4. The ASP must disclose their processes for monitoring the integrity and availability of those hosts.
5. The ASP must provide information on their password policy for the PIX Transmissions Ltd application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.
6. PIX Transmissions Ltd 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.)
7. 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

1. At PIX Transmissions Ltd'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).
2. Please disclose whether, and where, the application uses Java, Javascript, ActiveX, PHP or ASP,etc technology.
3. What language is the application back-end written in? (C, Perl, Python, VBScript, etc.)
4. 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.
5. 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

1. The PIX Transmissions Ltd application infrastructure cannot utilize any "homegrown" cryptography – any symmetric, asymmetric or hashing algorithm utilized by the PIX Transmissions Ltd application infrastructure must utilize algorithms that have been published and evaluated by the general cryptographic community.
2. Encryption algorithms must be of sufficient strength to equate to min 128 bit SSL or 168-bit Triple DES.
3. Preferred hashing functions are SHA-1 and MD-5.
4. Connections to the ASP utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, SSL, SSH/SCP, PGP.
5. If the PIX Transmissions Ltd application infrastructure requires PKI, please contact PIX Transmissions Ltd Information Security Group for additional guidance.

Acquisition Assessment Policy

1.0 Purpose
To establish Information Security responsibilities regarding corporate acquisitions, and define the minimum security requirements of an Information Security acquisition assessment.

2.0 Scope
This policy applies to all companies acquired by PIX Transmissions Ltd 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 PIX Transmissions Ltd does not pose a security risk to corporate networks, internal systems, and/or confidential/sensitive information. Information Security will provide personnel to serve as active members of the acquisition team throughout the acquisition process. The 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 PIX Transmissions Ltd's networks. Below are the minimum requirements that
the acquired company must meet before being connected to the PIX Transmissions Ltd network.

II. Requirements
A. Hosts

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

B. Networks

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

C. Internet

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

D. Remote Access

1. All remote access connections will be terminated.
2. Remote access to the production network will be provided by PIX Transmissions Ltd.

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 Lab Security policy, or be granted a waiver by LabSec.
5. In the event the acquired networks and computer systems being connected to the corporate network fail to meet these requirements, the PIX Transmissions Ltd Head of IT Security must acknowledge and report the risk to PIX Transmissions Ltd's Management.

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.

Backup/ Restore & retention policy

1.0 Purpose

The purpose of this policy is to define the process of data storage for the Protection and integrity of PIX Transmissions Ltd's primary servers regarding backup and recovery of the same information with specific retention period.

2.0 Background

It is statistical fact that computer systems fail; it is not a matter of why or how, but a matter of when. Several external factors, of which PIX Transmissions Ltd is not in control can cause occasional or severe problems to the servers; natural disasters such as flood, power cuts or lightning to man-made disasters such as trucks hitting a major power poll outside PIX Transmissions Ltd office and disturbing the power for a prolonged period of time. PIX Transmissions Ltd's most important assets is its ERP & Business Intelligence system, Emails, R&D schematics, drawings, specifications and processes, along with their patents and Proprietary trade secrets, which must be saved at all costs.

Loss of this information could cause severe downtime resulting in: lost production, delay of product, wasted time in recreation effort, deterioration in customer relationships, loss of market share and inevitably loss in income.

3.0 Scope

This policy pertains to all primary servers contained in PIX Transmissions Ltd main office. It includes all files related to the operating system, installed applications and data pertaining to those applications. Data retention period to be decide for Email/File server/ERP etc.

4.0 Policy

4.1 Statement

Backups of all primary servers are run during Day/Night, to make sure that all files are closed and available for backup. ERP Backup & file server backup is scheduled ones in a day & then move it to NAS Box. CRM/HRMS Backups are scheduled 8 times in a day & then move it to the NAS Box. Email archival is done on real time in to the email archival server. Laptop backups are done monthly, important desktops & industrial machine backup is scheduled monthly.

4.2 Responsibility

There are designated IT personnel responsible for setting backup schedules, monitoring & analysis of Backup & results.

The designated IT personnel are also responsible for data restores to misplaced data files at the individual request of the person that owns the original data files needing to be recovered.

The designated person is responsible for data retention as per the policy.

The person or persons responsible for this activity in the absence of the designated IT personnel will be an appointed member of the IT Staff at the request of the Head IT Infrastructure. The IT Head audits this policy on a Quarterly basis for compliance and make appropriate recommendations to the Head IT Infrastructure regarding such compliance issues as deemed necessary.

4.3 Actions

The daily, weekly, monthly and yearly backup done on appropriate media (Storage HDD, Storage Servers). & then moved to NAS Box permanently. Availability of sufficient Storage space must be ready. This is due to a combination of acceptable risks from PIX Transmissions Ltd senior management that have been determined either based on engineering, financial or individual department requirements.

No data will be recovered after it has aged more than 7 year time. PIX Transmissions Ltd senior management also realizes that there are time gaps where data might not be available due to rotation of series and / or no detail being available after the second yearly rotation to provide sufficient detail on a daily, weekly or monthly basis.

DATA BACKUP PROCEDURE

1.0 Purpose

The purpose of this Data Backup Procedure is to provide definition to PIX Transmissions Ltd's Data Backup Policy. All previous copies of this procedure are to be destroyed and printed copy is only for reference by the authorized person(s) performing the designated tasks.

2.0 Requirements to Perform Tasks

The only employees assigned the tasks of data backup / recovery of data contained on PIX Transmissions Ltd corporate servers are the IT Managers, IT Senior staff and IT Administration staff.

3.0 Prerequisites that are required for performing these tasks are:

1. Authorized physical access to IT server rooms,
2. Authorized access to Administrator account on all servers performing backups,
3. Authorized access to the Backup Software for all Server Systems.
4. Knowledge of backup software, schedules, media used and physical storage requirements,
5. Physical access and keys to fireproof cabinets and vaults utilized in physical storage of media.

4.0 Responsibilities

Backups of all primary servers are run during Day/Night, to make sure that all files are closed and available for backup. ERP Backup & file server backup is scheduled ones in a day & then move it to NAS Box. CRM/HRMS Backups are scheduled 8 times in a day & then move it to the NAS Box. Email archival is done on real time in to the email archival server. Laptop backups are done monthly, important desktops & industrial machine backup is scheduled monthly. Backups are to be complete prior to beginning of next business day.
The IT designated personnel are responsible for setting backup schedules, monitoring the success / failure of each system's previous nightly backup, rerunning the backup procedure if required and time permits between server checks and next available backup schedule.
The IT designated personnel are also responsible for data restores to misplaced data files at the individual request of the person that owns the original data files needing to be recovered.
The IT designated person is responsible for data retention as per the policy
This request will be in the form of an e-mail sent from the owner of the data wishing to be recovered sent to the IT Help Desk e-mail account for purposes of tracking and accountability. The person or persons responsible for this activity in the absence of the IT Manager will be an appointed member of the IT Staff at the request of the IT Manager.

5.0 Backup Process

Most of the backup jobs have been scheduled via automated Backup Software by the IT Manager to commence at Several timings during the Day/night on all servers. This allows adequate time for all employees to log off of their respective workstations so that all files located on the servers are closed and ready for backup. All jobs are setup in such a manner as to include all drives located on the server regardless of operating system or data volumes. All jobs are setup to include tape rewrite option, full backup (unless designated by IT Manager to provide incremental backup capability), the name of the server included in the tape label accordingly, default mediaset, verify after backup complete, compression set to Hardware (if available, otherwise software), backup open files set to yes.

6.0 Daily Backup Verification

Daily Backup verification is carried out for the Server systems of whose backup is scheduled.
Errors & exceptions are escalated to Head IT Infrastructure & appropriate remedial measures are taken.

7.0 Audit Verification

The IT Manager performs periodic data recovery tests on a monthly basis according to best practices to ensure efficiently of the backup mechanism.
The IT Security Team audits this policy on quarterly basis for compliance and makes appropriate Recommendations to the IT Manager regarding such compliance issues as deemed necessary.

8.0 Data Retention

The designated persons are responsible for data retention in following ways.

ERP	**Last 2 days on NAS box & 5 days on server.**
Email	**Last 7 years**
File server	**Last month**
CRM/HRMS	**Last 2 months**
Imp. Desktop Backup	**Last copy (monthly)**
Laptop backup	**last 2 copies (monthly)**
Final backup (Laptop)	**last copy of backup till the 7 years.**
Active Directory	**Daily (last 8 copies to be maintain)**
Cyberoam	**Monthly last 2 copies to be maintain)**

-- Annexure --

THIRD PARTY CONNECTION AGREEMENT

This Third Party Network Connection Agreement (the "Agreement") by and between PIX Transmissions Ltd, with principal offices at <Address>, <State>, ("PIX Transmissions Ltd") and _____, a _____ corporation, with principal offices at _____ ("Company"), is entered into as of the date last written below ("the Effective Date").

This Agreement consists of this signature page and the following attachments that are incorporated in this Agreement by this reference:

1. Attachment 1: Third Party Network Connection Agreement Terms and Conditions
2. Attachment 2 Network Connection Policy
3. Attachment 3: Third Party Connection Request - Information Requirements Document
4. Attachment 4: PIX Transmissions Ltd Non-Disclosure Agreement
5. Attachment 5: PIX Transmissions Ltd Equipment Loan Agreement

This Agreement is the complete agreement between the parties hereto concerning the subject matter of this Agreement and replaces any prior oral or written communications between the parties. There are no conditions, understandings, agreements, representations, or warranties, expressed or implied, which are not specified herein. This Agreement may only be modified by a written document executed by the parties hereto. Any disputes arising out of or in connection with this Agreement shall be governed by <Your Company's State> law without regard to choice of law provisions.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly executed. Each party warrants and represents that its respective signatories whose signatures appear below have been and are on the date of signature duly authorized to execute this Agreement.

_____ ("Company")	PIX Transmissions Ltd ("PIX Transmissions Ltd")
_____	_____
Authorized Signature	Authorized Signature
_____	_____
Name	Name
_____	_____
Date	Date

Attachment 1

THIRD PARTY CONNECTION AGREEMENT TERMS AND CONDITIONS

Object:

To ensure that a secure method of connectivity is provided between PIX Transmissions Ltd and Company and to provide guidelines for the use of network and computing resources associated with the Network Connection as defined below.

Definition: "Network Connection" means one of the PIX Transmissions Ltd connectivity options listed in Section B of the Network Connection Policy.

1. Right to Use Network Connection. Company may only use the Network Connection for business purposes as outlined by the **Third Party Connection Request - Information Requirements Document**.

2. PIX Transmissions Ltd-Owned Equipment.

2.1 PIX Transmissions Ltd may, in PIX Transmissions Ltd sole discretion, loan to Company certain equipment and/or software for use on Company premises (the PIX Transmissions Ltd-Owned Equipment) under the terms of the PIX Transmissions Ltd Equipment Loan Agreement set forth in Attachment 5. PIX Transmissions Ltd-Owned Equipment will only be configured for TCP/IP, and will be used solely by Company on Company's premises and for the purposes set forth in this Agreement.

2.2 Company may modify the configuration of the PIX Transmissions Ltd-Owned Equipment only after notification and approval in writing by authorized PIX Transmissions Ltd personnel.

2.3 Company will not change or delete any passwords set on PIX Transmissions Ltd-Owned Equipment without prior approval by authorized PIX Transmissions Ltd personnel. Promptly upon any such change, Company shall provide PIX Transmissions Ltd with such changed password.

3. Network Security.

3.1 Company will allow only Company employees approved in advance by PIX Transmissions Ltd ("Authorized Company Employees") to access the Network Connection or any PIX Transmissions Ltd-Owned Equipment. Company shall be solely responsible for ensuring that Authorized Company Employees are not security risks, and upon PIX Transmissions Ltd's request, Company will provide PIX Transmissions Ltd with any information reasonably necessary for PIX Transmissions Ltd to evaluate security issues relating to any Authorized Company Employee. Access to the Network Connection or any PIX Transmissions Ltd-Owned Equipment

3.2 Company will promptly notify PIX Transmissions Ltd whenever any Authorized Company Employee leaves Company's employ or no longer requires access to the Network Connection or PIX Transmissions Ltd-Owned Equipment.

3.3 Each party will be solely responsible for the selection, implementation, and maintenance of security procedures and policies that are sufficient to ensure that

(a) such party's use of the Network Connection (and Company's use of PIX Transmissions Ltd-Owned Equipment) is secure and is used only for authorized purposes, and

(b) such party's business records and data are protected against improper access, use, loss alteration or destruction.

4. Notifications. Company shall notify PIX Transmissions Ltd in writing promptly upon a change in the user base for the work performed over the Network Connection or whenever in Company's opinion a change in the connection and/or functional requirements of the Network Connection is necessary.

5. Payment of Costs. Each party will be responsible for all costs incurred by that party under this Agreement, including, without limitation, costs for phone charges, telecommunications equipment and personnel for maintaining the Network Connection.

6. DISCLAIMER OF WARRANTIES. NEITHER PARTY MAKES ANY WARRANTIES, EXPRESSED OR IMPLIED, CONCERNING ANY SUBJECT MATTER OF THIS AGREEMENT, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

7. LIMITATION OF LIABILITY. EXCEPT WITH RESPECT TO A PARTY'S CONFIDENTIALITY OBLIGATIONS UNDER THIS AGREEMENT, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, BUSINESS OR PROFITS) ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, ANY DAMAGES RESULTING FROM ANY DELAY, OMISSION OR ERROR IN THE ELECTRONIC TRANSMISSION OR RECEIPT OF DATA PURSUANT TO THIS AGREEMENT, WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, AND WHETHER OR NOT A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

8. Confidentiality. The parties acknowledge that by reason of their relationship to each other hereunder, each will have access to certain information and materials concerning the others technology and products that is confidential and of substantial value to that party, which value would be impaired if such information were disclosed to third parties ("Confidential Information"). Should such Confidential Information be orally or visually disclosed, the disclosing party shall summarize the information in writing as confidential within thirty (30) days of disclosure.
Each party agrees that it will not use in any way for its own account, except as rovided herein, nor disclose to any third party, any such Confidential Information revealed to it by the other party. Each party will take every reasonable precaution to protect the confidentiality of such Confidential Information. Upon request by the receiving party, the disclosing party shall advise whether or not it considers any particular information or materials to be Confidential Information. The receiving party acknowledges that unauthorized use or disclosure thereof could cause the disclosing party irreparable harm that could not be compensated by monetary damages. Accordingly each party agrees that the other will be entitled to seek injunctive and preliminary relief to remedy any actual or threatened unauthorized use or disclosure of such other party's Confidential Information.

The receiving party's obligation of confidentiality shall not apply to information that:

(a) is already known to the receiving party or is publicly available at the time of disclosure;

(b) is disclosed to the receiving party by a third party who is not in breach of an obligation of confidentiality to the party to this agreement which is claiming a proprietary right in such information; or

(c) becomes publicly available after disclosure through no fault of the receiving party.

9. Term, Termination and Survival. This Agreement will remain in effect until terminated by either party. Either party may terminate this agreement for convenience by providing not less than thirty (30) days prior written notice, which notice will specify the effective date of termination. Either party may also terminate this Agreement immediately upon the other party's breach of this Agreement. Sections 5, 6, 7, 8, 10.1 and 10.2 shall survive any termination of this Agreement.

10. MISCELLANEOUS.

10.1 Severability. If for any reason a court of competent jurisdiction finds any provision or portion of this Agreement to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remainder of this Agreement will continue in full force and effect.

10.2 Waiver. The failure of any party to enforce any of the provisions of this Agreement will not be construed to be a waiver of the right of such party thereafter to enforce such provisions.

10.3 Assignment. Neither party may assign this Agreement, in whole or in part, without the other party's prior written consent. Any attempt to assign this Agreement, without such consent, will be null and of no effect. Subject to the foregoing, this Agreement is for the benefit of and will be binding upon the parties' respective successors and permitted assigns.

10.4 Force Majeure. Neither party will be liable for any failure to perform its obligations in connection with any Transaction or any Document if such failure results from any act of God or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic or communications failure) which prevents such party from transmitting or receiving any Documents.

Attachment2
NETWORK CONNECTION POLICY

1.0 Purpose:

To ensure that a secure method of network connectivity within PIX Transmissions Ltd and all third parties and to provide a formalized method for the request, approval and tracking of such connections.

2.0 Scope:

Data network connections to PIX Transmissions Ltd can create potential security exposures if not administered and managed correctly and consistently. These exposures may include non-approved methods of connection to the PIX Transmissions Ltd network, the inability to shut down access in the event of a security breach, and exposure to hacking attempts. Therefore, all external company data network connections will be via the approved Providers Network.

This policy applies to all new Third Party Network Connection requests and any existing Third Party Network Connections. When existing Third Party Network Connections do not meet all of the guidelines and requirements outlined in this document, they will be re-engineered as needed.

3.0 Definitions:
A "Network Connection" is defined as one of the connectivity options listed in Section B. below. “Third Parties” is defined as PIX Transmissions Ltd Partners, Business Partners, and the like.

A. Third-Party Connection Requests and Approvals
All requests for Third Party connections must be made using the appropriate method based on the support organization. The required information is outlined in the **Third Party Connection Request - Information Requirements Document** All information requested on this form must be completed prior to approval and sign off.

It is Company’s responsibility to ensure that Company has provided all of the necessary information and that such information is correct.

All Third Party connection requests must have a Head IT Infrastructure signature for approval. In some cases approval may be given at a lower level with pre-authorization from the Head IT Infrastructure. Also, all Third Parties requesting a Network Connection must complete and sign a PIX Transmissions Ltd Non-Disclosure Agreement.
As a part of the request and approval process, the technical and administrative contact within Company’s organization or someone at a higher level within Company will be required to read and sign the "Third Party Connection Agreement” and any additional documents, such as the PIX Transmissions Ltd Non-Disclosure Agreement.

B. Connectivity Options
The following five connectivity options are the standard methods of providing a Third Party Network Connection. Anything that deviates from these standard methods would not be entertained.

1) Leased line (e.g. T1) - Leased lines for Third Parties will be terminated on the Partners network.

2) ISDN/FR - Dial leased lines will terminate on a Third Party only router located on the IT Partners network. Authentication for these connections must be as stated in Section E. below.

3) Encrypted Tunnel - Encrypted tunnels should be terminated on the Partners Network whenever possible. In certain circumstances, it may be required to terminate an encrypted tunnel on the dirty subnet, in which case the normal PIX Transmissions Ltd perimeter security measures will control access to internal devices.

4) Telnet access from Internet - Telnet access from the Internet will be provided by first telneting to the Third Party gateway machine, where the connection will be authenticated per Section E. below. Once the connection is authenticated, telnet sessions to internal hosts will be limited to those services needed by using the authorization capabilities of PIX Transmissions Ltd Secure.

5) Remote Dial-up via PPP/SLIP - Remote dial-up via PPP/SLIP will be provided by a separate Third Party modem pool. The connection will be authenticated per Section E. below

C. Third Party (Partner) Access Points
When possible, Third Party (Partner) Access Points (PAPs should be established in locations such that the cost of the access is minimized. Each PAP should consist of at least one router with VPN, leased line, Broadband and/or ISDN capability.

D. Services Provided
In general, services provided over Third Party Network Connections should be limited only to those services needed, and only to those devices (hosts, routers, etc.) needed. **Blanket access will not be provided for anyone.** The default policy position is to deny all access and then only allow those specific services that are needed and approved by PIX Transmissions Ltd pursuant to the established procedure.
In no case shall a Third Party Network Connection to PIX Transmissions Ltd be used as the Internet connection for the Third Party.
The standard set of allowable services are listed below:

File Exchange via ftp – Where possible, file exchange via ftp should take place on the existing PIX Transmissions Ltd ftp servers .IT supported Third Party connections have additional FTP services provided by a server in on the Partners Network.

Electronic Mail Exchange – Business-related email exchange between PIX Transmissions Ltd and Third Parties may be conducted over the Network Connection as needed. Mail from Third Party sites to non-PIX Transmissions Ltd addresses will not be allowed over the Network Connection.

Telnet Access – Telnet access will be provided to specific PIX Transmissions Ltd hosts, as needed. Employees from Third Parties will only be given accounts on the specific PIX Transmissions Ltd hosts that are needed. Where possible, router ACLs and static routes will be used to limit the paths of access to other internal PIX Transmissions Ltd hosts and devices.

NOTE: Domain accounts and Directory Services are not to be established for employees of Third Parties who have accounts on PIX Transmissions Ltd hosts.

Web Resource Access – Access to internal web resources will be provided on an as-needed basis. Access will be provided by mirroring the appropriate web resources to a web server that resides on the Partners Network. Access to PIX Transmissions Ltd's public web resources will be accomplished via the normal Internet access for the Third Party.

Access to Source Code Repositories This access will be decided on case by case basis with formal approvals.

Print Services – Print services can be provided to PIX Transmissions Ltd IT-supported Third Party connections by via two print spoolers on the PIX Transmissions Ltd Partners Network. PIX Transmissions Ltd-owned printers that boot off the print spoolers will be located on the PIX Transmissions Ltd –extended network at the Third Party sites.

Database Access – This will be decided on a case by case basis with formal approvals.

ERP Access – This will be decided on a case by case basis with formal approvals.

Windows File Exchange – File exchange will be provided by Windows file servers located on the PIX Transmissions Ltd Partners Network. Each Third Party needing Windows File exchange will be provided with a separate folder that is only accessible to that Party and the necessary people at PIX Transmissions Ltd.

E . Authentication for Third Party Network Connections

Third Party Network Connections made via remote dial-up using PPP/SLIP or standard telnet over the Internet will be authenticated using the Partners Authentication databases, SSL VPN or Token Access System. A separate server will be established specifically for Third Parties. Reports showing who has access will be generated monthly and sent to the PIX Transmissions Ltd Information Security team for each Third Party for verification and review.

Telnet connection made via the Internet must be initiated to a separate which authenticates to the Partners Authentication database and Token Access System mentioned above.

ISDN connections will be authenticated via the Partners PIX Transmissions Ltd Secure database, which is separate from the PIX Transmissions Ltd ISDN authentication database.

F. PIX Transmissions Ltd Equipment at Third Party Sites

In many cases it may be necessary to have PIX Transmissions Ltd-owned and maintained equipment at a Third Party site. All such equipment will be documented on the Third Party Connection Request – Information Requirements Document.

Access to network devices such as routers and switches will only be provided to PIX Transmissions Ltd support personnel.

All PIX Transmissions Ltd-Owned Equipment located at Third Party sites must be used only for business purposes. Any misuse of access or tampering with PIX Transmissions Ltd-provided hardware or software, except as authorized in writing by PIX Transmissions Ltd, may, in PIX Transmissions Ltd's sole discretion, result in termination of the connection agreement with the Third Party. If PIX Transmissions Ltd equipment is loaned to a Third Party, the Third Party will be required to sign an appropriate PIX Transmissions Ltd Equipment Loan Agreement, if one is required

G. Protection of Company Private Information and Resources

The PIX Transmissions Ltd network support group responsible for the installation and configuration of a specific Third Party Connection must ensure that all possible measures have been taken to protect the integrity and privacy of PIX Transmissions Ltd confidential information.

At no time should PIX Transmissions Ltd rely on access/authorization control mechanisms at the Third Party's site to protect or prohibit access to PIX Transmissions Ltd confidential information.

Security of Third Party Connections will be achieved by implementing "Access Control Lists" on the Partner Gateway routers to which the Third Party sites are connected. The ACLs will restrict access to pre-defined hosts within the internal PIX Transmissions Ltd network. The ACLs will be determined by the appropriate support organization.

A set of default ACLs may be established as a baseline.

Enable-level access to PIX Transmissions Ltd-owned/maintained routers on Third Party premise will only be provided to the appropriate support organization. All other business personnel (i.e. Partner Site local technical support personnel) will have restricted access/read-only access to the routers at their site and will not be allowed to make configuration changes.

PIX Transmissions Ltd shall not have any responsibility for ensuring the protection of Third Party information. The Third Party shall be entirely responsible for providing the appropriate security measures to ensure protection of their private internal network and information.

H. Audit and Review of Third Party Network Connections
All aspects of Third Party Network Connections - up to, but not including Company's firewall, will be monitored by the appropriate PIX Transmissions Ltd network support group. Where possible, automated tools will be used to accomplish the auditing tasks.

Monthly reports should be generated on the Partners Authentication database showing the specific login entries and the appropriate PIX Transmissions Ltd POC. Each PIX Transmissions Ltd Partner POC will receive a copy of the monthly reports showing all of the accounts pertaining to his/her area. Copies of the reports will also be mailed to the department directors.

Nightly audits will be performed on all PIX Transmissions Ltd-owned/maintained Third Party router/network device configurations and the output will be mailed to the appropriate PIX Transmissions Ltd network support group. Any unauthorized changes will be investigated immediately.

All Third Party Network Connections will be reviewed on a quarterly basis and information regarding specific Third Party Network Connection will be updated as necessary. Obsolete Third Party Network Connections will be terminated.

I. PIX Transmissions Ltd Corporate IT Information Security Organization
PIX Transmissions Ltd Corporate IT Information Security has the responsibility for maintaining related policies and standards. Corporate IT Information Security will also provide advice and assistance regarding judgment calls, and will facilitate information gathering in order to make a correct decision. Coordination of confidentiality and nondisclosure agreements with all third parties is also the responsibility of PIX Transmissions Ltd Corporate IT Information Security.

J. PIX Transmissions Ltd Enterprise Network Services
The Enterprise Network Services Partners Group is responsible for all global firewall design, configuration and engineering required for support of the Global Partners Network.

Attachment 3
THIRD PARTY CONNECTION REQUEST – INFORMATION REQUIREMENTS DOCUMENT

11.1 In accordance with the Network Connection Policy, all requests for Third Party Network Connections

must be accompanied by this completed Information Requirements Document. This document should be completed by the PIX Transmissions Ltd person or group requesting the Network Connection.

A. Contact Information

Requester Information

Name:
Department Number:
Manager's Name:
Director's Name:
Phone Number:
Email Address:

Technical Contact Information

Name:
Department:
Manager's Name:
Director's Name:
Phone Number:
Pager Number:
Email Address

Back-up Point of Contact:

Name:
Department:
Manager's Name:
Director's Name:
Phone Number:
Pager Number:
Email Address

B. Problem Statement/Purpose of Connection

What is the desired end result? Company must include a statement about the business needs of the proposed connection.

C. Scope of Needs **(**In some cases, the scope of needs may be jointly determined by the supporting organization and the Third Party.)

What services are needed? (See Section D. of Network Connection Policy)
What are the privacy requirements (i.e. do you need encryption)?
What are the bandwidth needs?
How long is the connection needed?
Future requirements, if any.

D. Third Party Information

Third Party Name
Management contact (Name, Phone number, Email address)
Location (address) of termination point of the Network Connection (including building number, floor and room number)
Main phone number
Local Technical Support Hours (7X24, etc).
Escalation List
Host/domain names of the Third Party

Names (Email addresses, phone numbers) of all employees of the Third Party who will use this access. If not appropriate to list the names of all employees, then provide a count of the number of employees who will be using the connection.

E. What type of work will be done over the Network Connection?

What applications will be used?
What type of data transfers will be done?
How many files are involved?
What are the estimated hours of use each week? What are peek hours?

F. Are there any known issues such as special services that are required? Are there any unknown issues at this point, such as what internal PIX Transmissions Ltd services are needed?

G. Is a backup connection needed? (e.g., are there any critical business needs associated with this connection?)

H. What is the requested installation date? (Minimum lead-time is 60 days)

I. What is the approximate duration of the Third Party Network Connection?

J. Has a Non-Disclosure Agreement been sign with the Third Party or the appropriate employees of the Third Party?

K. Are there any existing Network Connections at PIX Transmissions Ltd with this company?

L. Other useful information

Systems Change Request Form

This form is required in order to request changes to major systems. The person requesting the change shall complete the form after consulting with appropriate development, network and program staff. The authorizer shall sign the form before the change is put into place. All change requests shall be filed together to record system history.

Type of Request (Hardware, Operating System, Application, Configuration)		Request Date
Individual Requesting a System Change (Full Name)		Requested Implementation Date
Phone	Division	Supervisor / Manager

Change Request Description
Complete all information known at the time request is submitted.

Description of requested system change (To be Filled By User)		
Reason for the change request (To be Filled By User)		
List all technical changes to hardware, coding, database, networks, servers, reporting, etc., required in order to implement request.		
Roles: user impacts by type of user, changes to user roles		
Risks to be considered in the change, including a review of reporting, security, user training, system interfaces, backups and conversion		
Mitigation/Roll Back Options		
Estimate of costs and resources required to implement the change		
User training or other communications required		
Testing: Specify testing required prior to placement into production.		
Final Status		
	Implementation date:	Other status:

Requestor Approval:

_____

(Signature)
Date:

Authorizing Approval:

_____

(Signature)
Date:

Authorized Software Use Policy

Introduction : End-user license agreements are used by software and other information technology companies to protect their valuable intellectual assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable laws

Purpose : The purpose of the Software Licensing Policy is to establish the rules for licensed software use on PIX Transmission Ltd. Information Resources.

Audience : The PIX Transmission Ltd. Software Licensing Policy applies equally to all individuals that use any PIX Transmission Ltd. Information Resources.

Definitions : **Information Resources (IR):** Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
Information Resources Manager (IRM): The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of information activities, and ensure greater visibility of such activities within and between PIX Transmission Divisions. The IRM has been given the authority and the accountability by the Management to implement Security Policies, Procedures, Practice Standards and Guidelines to protect the Information Resources of PIX Transmission Ltd. If company does not designate an IRM, the title defaults to the company's Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.
Information Services (IS): The name of PIX Transmission Ltd. department responsible for computers, networking and data management.
Vendor: someone who exchanges goods or services for money.

Software Licensing Policy :

· PIX Transmission Ltd. provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities.
· Third party copyrighted information or software, that PIX Transmission Ltd. does not have specific approval to store and/or use, must not be stored on PIX Transmission Ltd. systems or networks. Systems administrators will remove such information and software unless the involved users can provide proof of authorization from the rightful owner(s).
· Third party software in the possession of PIX Transmission Ltd. must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.

As per PIX Transmission IT Software Policy, only the following software to be installed on a standard Desktop Laptop. Any other software will be considered unauthorized and will be liable to be deleted from the desktop.

Category / Type	**Software**	**Remarks**
Operating System	Windows XP with SP3/ Windows VISTA – Business Windows 7 Pro Windows 8/ 8.1 Pro, Windows 10 Pro	Mandatory
Office Productivity Tools	MS Office 2003/2007/2010 & 2013 Std. Open Office, WPS	Mandatory
Security products	Symantec Anti Virus	Mandatory
Client Software	**SQL Client**	
Other Utility Software	Acrobat Reader, WinZip, WinRar, RealVNC, Tight VNC	Mandatory
On Demand	Mozilla FireFox , Nero , Autocad, PDF Editor, PhotoShop, Illustrator, CorelDraw, PDF Editor & PageMaker	As per business need
On Laptop	Any desk	For remote access
With Approval from Business Head for purchase	PhotoShop, Illustrator, AutoCAD, CorelDraw, PDF Editor & PageMaker, etc.	Depends on requirement.

Laptop Policy

01.Overview
The purpose of this document is to clear how to handle & Care the Laptops owned by Pix Transmissions Ltd.

02.Scope
All users of Pix Transmissions Ltd. Are covered under this policy.

03.Policy
Laptop entitlement is solely depending on the business requirement & judged by respective Directors.
Those who are require the new laptop he/she must have to fill up asset requisition form & submit to with IT Dept. with the approval from respective director.
Any physical Damages are not covered under insurance & Maintenance contract; it will be borne by user only whether it is in working/ Non-Working Area/Time.
The Laptop must be use for only official Purpose; personal usage is not allowed.
User are not allowed to Write or Stick anything on Laptop, do not stick God Sticker or write any sign on Laptop.
All Laptops are covered under Insurance. In case of theft & burglary, user is the only responsible if any negligence found from user.
PIX is considering the Laptop Life of 7 years, after end of life Laptop gets replace.

04. Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
Application Service Providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

Desktop Policy

01. Overview

The purpose of this document is to clear how to handle & Care the Desktop owned by Pix Transmissions Ltd.

02.Scope

All users of Pix Transmissions Ltd. Are covered under this policy

03.Policy

Desktop entitlement is solely depends on the business requirement & judged by respective Directors.
Those who are require the new Desktop he/she must have to fill up asset requisition form with IT Dept. with the approval of respective director.
Any physical Damages which are not covered under insurance & Maintenance contract are born by user only whether it is in working/ Non-Working Area/Time.
The Desktop must be use for only official Purpose, personal usage are not allowed.
The Desktop life is considering 7 years during this time all physical damages will born by user.

04. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
Application Service Providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

------END OF POLICY------