



IT POLICY MANUAL

NETWORK USE REQUIREMENTS AND BEST PRACTICES

*To Protect Your IT Network, Data, and Business
From Cybersecurity Threats and Other Risks*

TABLE OF CONTENTS

TABLE OF CONTENTS.....	2
INTRODUCTION	3
ACKNOWLEDGEMENT & RELEASE.....	3
PROHIBITED USES OF YOUR IT NETWORK.....	4

There are certain actions that will almost always compromise the network on which they occur and/or subject the organization to unnecessary legal liabilities. This Policy outlines some of those actions, with a heavy focus on activities that are in most cases illegal, unethical, and harmful.

ACCOUNT MANAGEMENT, ACCESS & AUTHENTICATION POLICY.....	6
--	----------

Implementing consistent standards for account setup, management, access and authentication reduces the risk of security incidents and is often required by regulations and third-party agreements. The purpose of this Policy is to describe what steps must be taken to ensure that user accounts are properly managed and that all users connecting to Your IT Network are appropriately authenticated.

ANTI-VIRUS POLICY.....	8
-------------------------------	----------

All networks and devices connected to the Internet are exposed to the risk of viruses which can wipe out data, render devices inoperable, expose sensitive and confidential information, hold data hostage until a ransom is paid, and cause businesses to be exposed to lawsuits, fines and other liabilities. The requirements of this Policy outline the reasonable minimum steps that should be taken by all organizations and users to minimize these risks.

PASSWORD POLICY.....	10
-----------------------------	-----------

A solid Password Policy is among the most important security controls that an organization can implement. Strong passwords are Your first defense against many common cybersecurity threats and are a critical component of all cybersecurity risk management strategies.

INTERNET POLICY.....	11
-----------------------------	-----------

Since almost all security threats come from the Internet, it is important to have a solid set of rules designed to minimize these risks.

SECURITY INCIDENT REPORTING & RESPONSE.....	13
--	-----------

One of the most important components of minimizing and mitigating security risks and associated damages is a timely response. This Policy is designed to help organizations identify and promptly take action in the event of a potential cybersecurity incident, so that it can be addressed and mitigated hopefully before it has a chance to get out of hand and do major damage.

E-MAIL POLICY	14
----------------------------	-----------

E-mail has inherent security risks, which must be proactively addressed in order to avoid viruses or malicious code disrupting Your IT Network and Your ability to do business. This Policy is designed to protect Your business from the most common risks associated with business e-mail use.

COMPANY MOBILE DEVICE POLICY.....	16
--	-----------

Viruses and other security threats can enter IT networks through mobile devices in the same way that they infect PCs. Because a security breach can result in loss of information, damage to critical applications, and loss of revenue, it is important that all personnel who use mobile devices adhere to the requirements of this Policy.

PERSONAL DEVICE (“BYOD”) POLICY..... 18

While it may be unreasonable to require employees to leave their personal devices at home, certain steps must be taken in order to prevent unauthorized access to Your IT Network via employee’s personal devices. This policy contains the security protocols We recommend to be implemented in order to minimize the risk of a data breach or other security incident via a personal device.

POLICY REVISION HISTORY..... 20

INTRODUCTION

We'd like to begin by acknowledging one undeniable truth: no one likes IT policies – they're boring, technical, and take some work to understand and implement.

However, creating a solid set of rules and training team members to follow basic best practices when using any company network or device is a necessary "growing pain" that all successful small businesses have to go through in order to ensure the integrity of their IT infrastructure and the security of sensitive data.

Our goal is never to impose unnecessary restrictions on Your operations, but to protect your business from unnecessary interruptions, monetary losses and legal liabilities.

In many cases, risks like viruses, data breaches, ransomware attacks, compromised systems – and the resulting losses and liabilities that follow – *can* be minimized and even prevented when users abide by some basic IT security rules.

In addition, following the best practices described in these Policies ensures that your technology functions as intended – fast, reliable, and supportive of Your operations.

Because a security breach can result in loss of information, damage to critical applications, loss of revenue, massive legal liabilities and damage to the organization's reputation and public image, it is essential that all personnel who use or access data on Your IT Network (including employees, contractors, consultants, temporary users, and other users/workers who may have access to any account, data or device on the network) follow the requirements of the Policies in this Manual and understand what is required of them in terms of using electronic devices, network resources and company information.

These Policies may be amended and supplemented from time to time to reflect the latest industry standards, best practices and the newest solutions to the constantly evolving security threats that small businesses face every day. We will notify You of any updates by sending an e-mail with the updated policy to Your [Designated IT Contact](#).

The definitions used in your MSA and/or Client Handbook apply to all capitalized words and phrases used in the Policies in this Manual, unless another definition is specifically provided in the Policy.

ACKNOWLEDGEMENT & RELEASE

While We are experts in cybersecurity, even the most advanced IT firms with the most up to date, cutting-edge technology suite cannot protect a network and its data where users and administrators don't do their part in following basic security measures and industry best practices. In short, the protection of Your IT Network requires that we all do our part.

The Policies contained in this Manual outline the actions required of You and Your team in order to minimize exposure to common and well-known cybersecurity risks and ensure that Your IT Network functions as intended.

To ensure compliance with these Policies, all of Our clients are encouraged to implement internal systems, procedures and policies that reflect the requirements contained herein, and to require all employees, contractors and other users to review, accept and promise compliance in writing before being granted a device and/or access to any company-owned IT infrastructure/resources.

If You need help creating internal IT policies for Your organization, give us a call at (800) 260-3980 or contact Your Account Manager, who can either give You a quote for this service or refer You to one of Our trusted partners in legal/compliance.

Having all users follow the established industry best practices outlined in this Manual is essential to Our ability to do Our job.

Accordingly, if Your IT Network or any sensitive data is breached, exposed or compromised due to actions that are not in compliance with the Policies in this Manual and/or Your failure to follow Our specific recommendations regarding any hardware, software, security measure, policy or process, You fully accept all risks associated with such actions and agree that We are not liable for any losses or damages that may result.

By working with us, You agree to release, indemnify and hold Us harmless from and against any and all liabilities, claims, causes of action, lawsuits and/or demands that arise out of or are in any way related, directly or indirectly, to Your decision not to follow the Policies set forth in this Manual, as amended from time to time, and/or Our advice or recommendation with respect to any hardware, software or security solution which We advised you to install, implement, change, replace, upgrade or delete.

In addition, any labor that We perform to mitigate issues resulting from actions that are contrary to Our recommendations and/or the Policies contained in this Manual, is considered to be outside the scope of any Managed Service Plan and is billable according to Our hourly rates set forth in Your MSA.

For example, if a cybersecurity / data breach, data loss or other damage occurs involving any hardware, software or equipment which We recommended to be installed, upgraded or replaced, You accept full responsibility for remediating any such loss, breach or damage, and further accept and agree that any labor performed by Us to repair any damage or otherwise handle any issues associated with such loss, breach or damage will be billable at Our standard hourly rates.

PROHIBITED USES OF YOUR IT NETWORK

Let's start with the easy stuff – any activities that are illegal under local, state, federal or international law are strictly prohibited. Under no circumstances are You or any of Your personnel authorized to engage in any such illegal activities while using Your IT Network.

In addition, the following activities are strictly prohibited, with no exceptions:

- ⊗ Violations of the rights of any person or entity protected by intellectual property (“IP”) laws of any applicable jurisdiction. IP law includes copyright, trademark, patent, trade secret and similar regulations. This includes but is not limited to:
 - The installation, use or distribution of software products and subscriptions without obtaining the appropriate license that allows such activities.
 - The use, reproduction and distribution of copyrighted graphics, photographs, written content, music and other copyrighted content for which You or the end user do not have an active license that allows such activities.
- ⊗ Downloading, installing or otherwise introducing malicious software into Your IT Network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) or engaging in security breaches/disruptions of network communication, unless such activity is a part of the user’s normal job or duty. Examples include, but are not limited to:
 - accessing data of which the user is not an intended recipient;
 - logging into a server or account that the user is not authorized to access;
 - engaging in disruptive activities such as network sniffing, ICMP floods, denial of service, IP spoofing, forged routing information and other similar activities with a malicious purpose;
 - engaging in any form of network monitoring that intercepts data not intended for the user;
 - circumventing the security, for example the user authentication, of any host, network or account;
 - intentionally interfering with or disabling a user's terminal session via any means.
- ⊗ Revealing or failing to take reasonable steps to protect passwords as required by the Password Policy. This includes allowing the use/access of accounts by anyone other than the user to whom the password is assigned (unless an exception applies, such as authorized administrative staff acting on behalf of the account owner).
- ⊗ Engaging in any activity that violates the privacy rights of any employee or third party or using Your IT Network to procure or transmit materials violating laws that protect workers in the user's local jurisdiction, such as sexual harassment, non-discrimination, hostile work environment, and other similar regulations.
- ⊗ Altering, modifying, or adding to any component of Your IT Network without Our express written approval. This includes but is not limited to:
 - Downloading or installing any software, patches or updates on any computer or mobile device owned or serviced by Us;
 - Altering, disconnecting or moving any hardware owned or serviced by Us;
 - Using or connecting any hardware to Your IT Network without a compatibility review by Us;
 - Engaging in any activity that may a) degrade, slow or hinder the performance of any component of Your IT Network; b) deprive an authorized user access to a device or the network; c) circumvent any Policy in this IT Policy Manual;
 - Engaging in any activity which We have advised would jeopardize or compromise the safety, security, reliability, speed, or functionality of Your IT Network.
 - Downloading or installing any software or tools that reveal passwords and private information, or otherwise exploit any weakness in the security of Your IT Network.

This includes any and all spyware, port scanners, password cracking programs, and similar applications.

ACCOUNT MANAGEMENT, ACCESS & AUTHENTICATION POLICY

Implementing consistent standards for account setup, management, authentication and network access reduces the risk of security incidents and is often required by regulations and third-party agreements.

The purpose of this policy is to outline the steps to ensure that user accounts are properly managed and that all users connecting to Your IT Network are appropriately authenticated.

Account Setup

The following policies apply to account setup:

- ⇒ HR should confirm employee identity, title and job functions (for purpose of determining access limits) for any user to be granted access to Your IT Network.
- ⇒ Accounts must be set up with appropriate login credentials. All user names must use a consistent standard format (i.e., first initial + last name, with additional letters of the first name to be added until a unique username is created should a redundancy arise), and passwords must comply with the Password Policy.
- ⇒ All user accounts should be configured with the most restrictive set of rights, privileges and access permissions required for the performance of the user's job duties.
- ⇒ All devices connecting to Your IT Network must be configured to request authentication. If authentication cannot occur, then the machine should not be permitted to access the network.
- ⇒ Accounts must be for individual personnel only. Account sharing and group accounts are highly discouraged.
- ⇒ Users must not be given administrator or "root" access unless necessary to perform the functions of their position.
- ⇒ In the event that guests have a legitimate business need to access Your IT Network, temporary guest access may be allowed, provided that a) the request is formally made and approved by a manager with authority to do so; and b) it is specifically limited to only those resources that are required by that guest, and disabled when no longer needed.
- ⇒ All personnel requiring access to highly sensitive, proprietary or confidential information must have an individual account set up with special access permissions. Such accounts may be subject to additional monitoring or auditing at the discretion of the appropriate supervisory or executive team, and/or as required by applicable regulations or third-party agreements.
- ⇒ Users may be granted access only if they acknowledge and accept, in writing, the requirements of all Policies in this IT Policy Manual.

Account Use & Management

- ⇒ All accounts must have a unique username and password. Shared user accounts (whereby two or more users access Your IT Network under the same credentials) are not permitted.
- ⇒ Passwords for all accounts must comply with ALL requirements of the Password Policy.
- ⇒ Any device/account connecting to the network can have a serious impact on the security of the entire network. Accordingly, users should confirm that their antivirus software, as well as other critical software, are always upgraded to the latest versions before accessing the network.
- ⇒ No one is authorized to establish, activate, modify, disable, or remove any user accounts from Your IT Network without Our express written approval.
- ⇒ HR should notify Your internal IT management of all staffing changes, including employee termination, suspension, or a change in job functions, in order to ensure that a) access permissions can be adjusted so that they are always an accurate reflection of the team member's job requirements; and b) accounts of terminated employees can be disabled, and any devices used by them returned and wiped.

Monitoring & Restrictions

- ⇒ We monitor user accounts for inactivity. If an account is found to be inactive for 60 days, We will notify You of pending disablement. Unless otherwise instructed, We will disable the account if it remains inactive for an additional 30 days from Our notice of inactivity.
- ⇒ We periodically conduct account audit reviews to ensure that all accounts and network resources are appropriately used and managed.
- ⇒ All businesses should have written policies in place regarding a) whether users' access is removed or maintained while on a leave of absence or vacation; and b) the criteria and process for modifying a user account based on name changes, position changes and permission changes.

Remote Network Access

Remote access to Your IT Network can be provided to users for convenience; however, this carries its own security risks. For that reason, We recommend setting up remote access to require the use of two-factor authentication.

In addition, the following requirements apply to all users accessing Your IT Network remotely:

- ⇒ All remote access must be strictly controlled via approved encryption methods (such as VPNs) and strong pass-phrases.
- ⇒ Users must never share their login and password with anyone, including family members.
- ⇒ Before remotely connecting to Your IT Network, users should confirm that the remote host is not connected to any other network at the same time, except personal networks that may be under that user's or an authorized third party's complete control.

- ⇒ All devices connected to Your IT Network, remotely or otherwise, must use the most up-to-date anti-virus software approved by Us.
- ⇒ All Policies in this IT Policy Manual apply to remote users the same way they apply to everyone else.

Failed Logins

Repeated login failures could be a sign of an attempt to “crack” a password to obtain unauthorized access Your IT Network and sensitive data. In order to protect Your business from password-guessing and brute-force attempts, any user account with 5 consecutive failed login attempts will be locked. Depending on Your preference, the lockout may be for a specific amount of time (less secure) or require a manual reset by Us (more secure).

While all Policies in this IT Policy Manual apply to remote users of Your IT Network, the following Policies are particularly important and should be thoroughly reviewed before accessing the network remotely: [Password Policy](#); [Internet Policy](#); [Mobile Device Policy](#); [Personal Device \(“BYOD”\) Policy](#).

ANTI-VIRUS POLICY

Any IT Network and device connected to the Internet is exposed to security risks that threaten to wipe out data, render devices inoperable, expose sensitive and confidential information, hold data hostage until a ransom is paid, and cause businesses to be exposed to lawsuits, fines and other liabilities.

Common Cybersecurity Threats

Some of the most common cybersecurity threats that affect all businesses include the following:

Malware: Malware is the general collective term used to refer to software specifically designed to damage, disrupt or gain unauthorized access to a computer, system, server or network. It includes viruses, worms, spyware, ransomware and other software/code designed to cause damage to data or gain access to a network. It is usually delivered via email, in the form of a link or file, and is “activated” when the user clicks on the link or opens the file.

Virus: Computer viruses – a type of malicious code or program written to alter the way a computer operates – cause billions of dollars' worth of economic damage each year. Viruses are designed to spread from one computer to another, and have the potential to cause widespread damage to Your IT Network, such as harming the system software by corrupting or destroying data.

Trojan Horse: A Trojan horse is a type of malware that is used by hackers and thieves to gain access to a computer or system. They infect systems by tricking the user into opening the file, which is usually disguised as legitimate software. Once activated, Trojans can enable criminals to spy on you, steal your data, gain access to your system, and otherwise damage, disrupt, and inflict harm upon your data and IT Network.

Worm: A worm is a malicious software that replicates itself and spreads through networks like a virus. They are generally designed to target pre-existing vulnerabilities in the operating system of the computers they attempt to infect in order to steal data, install backdoors that can be used to access the network, and cause other types of harm. Worms consume large amounts of bandwidth and memory, which can lead to networks, devices and servers malfunctioning due to overload. Many of the most destructive types of malware have been worms.

Spyware: Spyware is loosely defined as software with malicious behavior that aims to enter your computer, perform surveillance to gather information about a person or organization, and send such information to another entity so that they may profit from the stolen data. Spyware activity leaves you open to data breaches and associated liabilities, while also slowing down network and device performance.

Adware: Adware refers to unwanted software designed to display advertisements to the user, most often in a web browser. It usually either disguises itself as legitimate software in order to trick the user into installing it, or it may get on a computer by being secretly buried in legitimate software. Once on a device, it engages in unwanted activities such as analyzing the websites visited, displaying burdensome advertisements, and sell your browsing behavior and other information to third parties.

Keyloggers: Keyloggers are a type of monitoring software designed to record every keystroke made by a user on any website or application, and send the information to a third party. Criminals use keyloggers to steal personal, financial and other confidential information such as passwords, banking details, and trade secrets. Some keyloggers can record audio/video, GPS location, and screenshots.

Ransomware: Ransomware is a form of malware that encrypts a victim's critical data, so that the organization cannot access its files, databases, or applications. In order to restore access, the organization must pay the attacker a specified sum. Ransom amounts demanded range from a few hundred dollars to tens of thousands and more. Ransomware often spreads quickly, encrypting files across a network and target database and file servers. It can easily paralyze an entire organization. Due to its effectiveness, it has cost businesses billions of dollars in damages and payments to cybercriminals.

Steps We Take to Prevent Malware Issues

On every file server and device that We service, We ensure that anti-virus software is installed, actively running, and configured to be automatically updated. We also install e-mail virus protection software to protect each e-mail gateway and periodically scan all computer devices for malware.

Once We have installed all required software, altering the settings in any manner is strictly prohibited, as inexperienced users may cause the effectiveness of the software to be reduced or eliminated. Users are specifically prohibited from altering the automatic update frequency of the virus protection software.

If a virus is detected, We may disconnect the infected device(s) from the network to prevent propagation of malware to other devices and resulting damages, until the infection has been removed.

User Requirements

All users must take the following precautionary measures in order to avoid unnecessary business interruptions and monetary losses caused by computer viruses:

- ⇒ Never open any attachments to any e-mail from an unknown, suspicious, or untrustworthy source. If anyone is unsure about an e-mail, We are always available to take a look and potentially avoid a costly and disruptive security incident.
- ⇒ All SPAM, chain, or other junk mail should be deleted without opening or forwarding.
- ⇒ Users must never download files from the Internet on any work devices unless specifically authorized by Us – especially not from unknown or suspicious sources.
- ⇒ Removable media (such as CDs, USB drives, external hard drives) must always be scanned for viruses before using it.

- ⇒ If Your service plan includes data backup, all data saved to network drives is backed up at regular intervals. Clients who have opted out of this service should take measures to back up all critical data on a regular basis and store the data in a safe place.

Incident Reporting

If any user detects or suspects that a virus that was not automatically cleaned by the anti-virus software, this should be treated as a security incident and must be immediately reported to Us by following the steps in the Security Incident Reporting & Response Policy so that any potential security issues can be mitigated before they have a chance to get out of hand or cause greater damage.

PASSWORD POLICY

Since weak passwords can compromise even the most secure IT networks, this policy is designed to ensure that the passwords used in Your organization are strong, secure, and provide a reasonable level of security for your network without posing an undue burden on users. Strong passwords are the first protection for user accounts and as such, they are a mandatory element of all cybersecurity solutions.

User Account Password Policy

- ⇒ Passwords must be used for all computers connected to Your IT Network.
- ⇒ Passwords must be at least 10 characters in length – typically, the longer the password, the more secure it is.
- ⇒ Passwords must be changed every 60-90 days.
- ⇒ Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (!@#\$%^&* _+=?).
- ⇒ Passwords should not contain information such as a name, proper name, acronym, or a dictionary word in any language.
- ⇒ Passwords should never be linked to any personal information about the password owner such as an address or phone number, a birth date, social security number, relatives' names, etc.
- ⇒ Passwords may not be reused for at least 1 year.
- ⇒ Screensaver passwords are recommended for PCs that are only used by one user, as they increase security by removing the opportunity for an intruder or unauthorized employee to access network resources through an idle computer. Screensaver passwords are not permitted for computers shared by more than one user, as they violate the “no shared passwords” policy.

System-Level Password Policy

- ⇒ All system-level passwords must be at least 12 characters in length and contain at least 3 of the following: upper case, lower case, numbers, and special characters.
- ⇒ Passwords must be changed at least every 90 days.

Rules Applicable to All Passwords

- ⇒ The same password should never be used for multiple accounts.
- ⇒ All passwords are to be treated as strictly confidential and must not be disclosed to anyone, including co-workers, managers, or family members.

- ⇒ Passwords must never be shared over the phone or disclosed on questionnaires or security forms.
- ⇒ Passwords must not be shared via e-mail, instant message, text or any other form of electronic communication without encryption. Because interception of this information can result in a serious security incident, authentication credentials must always be encrypted during transmission across any network.
- ⇒ Users must not use password hints from which a third party may deduce the password (for example, “mother’s name”, “home address”, etc).
- ⇒ Passwords must not be stored physically, such as written down on a notepad or post-it. Passwords may be stored in a file on a computer system or mobile device (phone, tablet) if they are appropriately encrypted.
- ⇒ Circumventing password entry via auto log-ons, application remembering, embedded scripts, hard coded passwords in client software, or otherwise, is strictly prohibited unless written approval is provided by Us and any additional security measures recommended by Us have been implemented.
- ⇒ Security tokens (such as smartcards, key fobs, etc.) must be immediately returned by any user whose relationship with the business was terminated for any reason.

Password Security Incidents

If there is any reason to believe that the security of an account may be compromised, You must:

- 1) Notify Us immediately via the methods specified in the Security Incident Reporting & Response Policy
- 2) Change the password (ensuring that the new password is compliant with the Password Policy)
- 3) If applicable, take control of and protect/destroy any passwords that may have been found written down or stored electronically without encryption

INTERNET POLICY

General Internet Use & Access Policy

The following policies apply to all users and devices accessing the Internet:

- ⇒ All software by which users access the Internet must be a) part of the Our Standard Technology Suite or otherwise approved by Us; b) up to date on all upgrades and incorporate all vendor-issued security patches.
- ⇒ PCs on Your IT Network may access the Internet only through Internet firewall or equivalent security device approved by Us.
- ⇒ Bypassing any network security requirements outlined in this Policy, by accessing the Internet directly, is strictly prohibited.
- ⇒ Accessing the Internet for the purposes of gaining unauthorized access to local and remote computer systems, software piracy, illegal activities, the transmission of threatening, obscene, or harassing materials, or personal solicitations, is strictly prohibited. Likewise, using the Internet to propagate malware is strictly prohibited.

- ⇒ Downloading or installing any software from the Internet on any device connected to the IT Network without Our express written approval, is strictly prohibited.
- ⇒ All software and files downloaded from the Internet must be scanned for viruses using the software designated or approved by Us for this purpose. If a virus is detected or suspected, We must be notified immediately so that we can take steps to mitigate any potential threat before it has a chance to cause further damage.
- ⇒ If software is downloaded, it may only be used in conformity with the terms of its license and applicable intellectual property laws.
- ⇒ Users should have no expectation of privacy in anything they create, store, send, or receive using the company's Internet access.
- ⇒ All confidential and sensitive information transmitted over the Internet or any external network must be encrypted.
- ⇒ Accessing websites containing sexually explicit material or other material deemed inappropriate in the workplace – along with any display, storing, archiving, or editing of such content on any company device – is strictly prohibited. To reduce Our clients' legal risks, We use software that identifies and blocks access to such websites. However, in the event that such a site is not automatically blocked and a user accidentally connects to same, the user must immediately disconnect from the site and the incident must be reported to Us immediately.

Incidental / Personal Use

To minimize security risks, incidental personal use of Internet access (this may include browsing for entertainment, playing games, participating in chat groups, uploading or downloading large files, streaming audio and/or video files, and other non-business purposes) should be restricted to a reasonable minimum, and should only be permitted for company personnel (i.e. it should not extend to family members or other third parties). Storage of personal files and documents within Your IT Network should be nominal.

Personnel should be advised that a) sending or receiving files or documents that may cause legal liability to the business should be strictly prohibited; and b) all files and documents, including personal files and documents, which are stored on Your IT Network are owned by the company and may be subject to open records requests, and may be accessed in accordance with this policy.

Computer resources, network bandwidth and storage capacity are not unlimited. As such, all users should be instructed to refrain from knowingly engaging in activities that waste or unfairly monopolize resources, or which are not essential to the performance of their job duties.

Our Rights

- ⇒ **Restricting Access:** In order to protect Your data and network, We may restrict access to programs, web apps and websites that harm network performance or which are known or found to be high-risk or compromised by malware. We may, in Our discretion, use technical controls to restrict users' ability to download and install software.
- ⇒ **Monitoring:** We may monitor, log, and analyze any and all user activity on Your IT Network. This includes, but is not limited to, monitoring and logging all Internet sites visited by users; social media usage; any chat, newsgroup and forum activities; file downloads and uploads; application usage; and all communications sent and received by users.

SECURITY INCIDENT REPORTING & RESPONSE

When it comes to security breaches – and responding to them – time is of the essence. The longer a cybersecurity incident such as a data breach or exposure goes undetected, the greater the damage such an event can cause.

As such, it is absolutely essential that **any individual who finds out or suspects that a security incident has occurred, must immediately contact Us to provide a full description of the events and all available information via the following methods:**

E-Mail: support@kinzit.com

Phone: [800-260-3980](tel:800-260-3980)

Examples of reportable incidents / suspicious circumstances:

- ⊗ You become aware that a password has been compromised.
- ⊗ You have identified a virus or other malware infection.
- ⊗ A theft, breach or exposure of Your data or IT Network has occurred.
- ⊗ You notice that Your network security or firewall has been uninstalled or disabled; you can't restart your anti-malware program or firewall and you didn't turn it off.
- ⊗ You notice an increase in error messages while completing routine tasks
- ⊗ Computers are freezing, crashing or running slowly for no apparent reason
- ⊗ E-mails from company addresses are being sent without Your knowledge, You are accused of sending SPAM.
- ⊗ Your Internet browser suddenly displays toolbars and extensions that you don't recognize
- ⊗ A password has suddenly changed without Your knowledge
- ⊗ You notice that files are missing or being deleted from Your network
- ⊗ You notice files are being re-named
- ⊗ You receive a ransom demand
- ⊗ You are unable to access files or applications
- ⊗ [Etc](#)

Next Steps in Responding to a Security Incident

Once a report is received, We will launch an investigation into the issue to confirm whether a theft, breach or exposure has occurred, and will follow the appropriate response procedure based on those findings.

If a breach has occurred, We may be required by Our insurer and legal team to provide access to forensic investigators and experts tasked with determining the nature and extent of the breach; the data that has been impacted or exposed; the number of individuals and/or organizations affected; and to determine the root cause of the breach or exposure.

We will also work with Your communications, legal, HR and other relevant departments in handling and communicating the events to employees and team members, the public, and any clients, end users and other parties directly affected by the breach.

E-MAIL POLICY

E-mail has inherent security risks, which must be proactively addressed in order to avoid viruses or malicious code disrupting Your IT Network and your ability to do business. The following policies are designed to protect Your business from the most common risks associated with business e-mail use:

Anti-Virus and Monitoring

For clients on our [E-mail Security Plan](#), we have software in place that scans all incoming and outgoing e-mails or spam and malicious code and files/attachments. If an attachment has an extension commonly associated with malware or is otherwise classified as high risk, it will be removed from the e-mail prior to delivery. In addition, e-mails from domains and IP addresses associated with malicious actors will be rejected, and messages identified as spam will be quarantined for the user to review.

Any e-mail account sending out spam will be shut down until You notify us that the issue has been addressed and the account should be reinstated. Likewise, any outgoing e-mail containing attachments with viruses or malicious code will be prevented from sending. Allowing such activities would not only harm the recipient's system, but may also result in legal liability, regulatory fines and significant damage to Your organization's reputation.

Retention and Archiving

To ensure that your Network runs optimally while giving you access to your messages for as long as possible, we have implemented the following policies regarding retention and archiving:

- ⇒ E-mails, calendar entries, tasks and notes are retained for 60 months, after which they are automatically purged.
- ⇒ Deleted and archived e-mails are automatically purged after 60 months from the original send/receive date.
- ⇒ Archived e-mails are only accessible by the owner of the account and the system administrator.

Diligence in E-mail Communications

All team members should be trained to recognize e-mail spoofing: the criminal practice of sending e-mails with a forged header that makes it appear as though the message as sent by someone other than the actual sender. The objective is usually to induce the recipient to open the e-mail, and either download a malicious file or inadvertently provide sensitive data or make a fraudulent payment to a criminal.

Employees should be trained to identify spoofed e-mail; should never open or respond to them; and should under no circumstances download any attachments. Users must use caution when opening attachments from unknown senders, as this is how many instances of malware infection occur.

If suspicious e-mail activity has been detected, users should be trained to report it immediately to the appropriate supervisory personnel and You must in turn notify Us immediately so the issue can be addressed.

Encrypting and Protecting Sensitive Content

All data sent via e-mail should be treated as sensitive information. Users should never send work documents or information to anyone outside of the company unless it is a required part of business and the contact is known and trusted. Additionally, sensitive information such as passwords, social security numbers, credit card and bank account numbers, pin numbers, and other information from which accounts can be hacked (think mother's maiden name, etc.) should never be sent without encryption. When data is sent encrypted, passwords to decrypt the data should not be sent via e-mail.

In order to ensure compliance with this policy, all e-mail activity on Your IT Network is subject to monitoring, logging and review.

Because there is nothing we can do to proactively monitor and protect information sent to or from personal accounts, team members should be discouraged from sending, receiving or forwarding confidential or sensitive information via personal e-mail accounts such as Gmail, Hotmail, Yahoo, etc.

Users must also comply with the Personal Device Policy for sending, forwarding, receiving, or storing information relating to your business.

Company E-mail and Personal Business

Just as storage of personal files and documents by employees on Your IT Network should be kept to a minimum, team members should also refrain as much as possible from using company e-mail accounts to send messages and files to family members, personal contacts, or other acquaintances.

Not only do such activities pose a heightened security risk, but it also increases the potential of subjecting Your organization to unnecessary legal liabilities arising from the transmission of files, messages and documents to contacts with no business relationship to your company.

It is also important to note that business e-mail is not private. All e-mails, files, and documents sent through the company network – including personal ones – are typically considered property of the organization, and may be subject to open records and similar requests.

E-Mail Conduct That Can Jeopardize Your Business

In order to protect Your business from unnecessary legal liabilities and damage / interruption to Your e-mail service, the following activities are prohibited:

- ⊗ Using company e-mail to send messages that may be deemed intimidating, harassing, or offensive. This includes, but is not limited to: abusive language, sexually explicit remarks or pictures, profanities, defamatory or discriminatory remarks regarding race, creed, color, sex, age, religion, sexual orientation, national origin, or disability;
- ⊗ Sending SPAM in any form, including unsolicited advertising or "junk mail" to individuals who did not specifically request such material, or creating/forwarding "chain letters" or promoting pyramid/Ponzi schemes;
- ⊗ Sending unsolicited e-mails to large groups, except as may be appropriate in the ordinary scope of the sender's job duties;
- ⊗ Knowingly sending or forwarding e-mails containing viruses or malicious code/software;
- ⊗ Excessive use of company e-mail to conduct personal business;
- ⊗ Violating copyright laws by illegally distributing protected works;
- ⊗ Forging or attempting to forge e-mail messages or e-mail header information;
- ⊗ Creating false identities to bypass any laws, regulations or policies;
- ⊗ Using unauthorized e-mail software;
- ⊗ Engaging in any activities for the purpose of circumventing this Policy, such as knowingly disabling the automatic scanning of e-mails for spam content, malicious code and

attachments; or otherwise intentionally circumventing any e-mail security measures implemented or recommended by Us;

- ⊗ Sending e-mails revealing any information known by the user to be confidential or proprietary, without specific authorization from the owner of the information;
- ⊗ Sending e-mails that may harm or tarnish the image, reputation and/or goodwill of the organization and/or any of its employees.

E-Mail Security Incident Reporting

If You detect or suspect that an e-mail address on Your network has been compromised or that you have received malicious e-mail, You must notify Us in accordance with the Security Incident Reporting & Response Policy immediately so that any potential security issues can be mitigated before they have a chance to get out of hand or cause greater damage.

COMPANY MOBILE DEVICE POLICY

As You probably already know, malware and other threats can enter IT networks through mobile devices in the same way that they infect PCs. Because a security breach can result in loss of information, damage to critical applications, and loss of revenue, it is important that all personnel who use mobile devices adhere to the requirements of this Policy.

All of Our clients are encouraged to implement internal policies that reflect the requirements contained herein, and to require all employees and other users to review and accept the terms of such policies before being granted a device and access to any company-owned IT infrastructure/resources.

Devices

This policy applies to all mobile devices belonging to Your organization that are used to access corporate resources and/or contain stored data belonging to You, Your clients and other parties. This includes but is not limited to mobile phones, tablets, laptops, notebooks, and other mobile devices owned by You and which are capable of storing corporate data and connecting to an unmanaged network.

Risks

Examples of the possible risks of using such devices to store, transfer, or access Your data and/or Your IT Network include:

- ⊗ Devices and their contents being lost or stolen;
- ⊗ Theft of proprietary and confidential information by an employee, contractor or third party;
- ⊗ Potential legal liability for intellectual property infringement due to team members copying files and software onto personal devices without a license permitting same;
- ⊗ Introduction of malware/viruses to Your IT Network via a mobile device;
- ⊗ Non-compliance with applicable laws and regulations (and liability for fines, penalties and lawsuits) due to theft or exposure of financial, personal or other confidential data protected by privacy and identity theft legislation.

Registration, Monitoring & Support

- ⇒ We manage network, application, and data access from all devices – including mobile devices – centrally, using technology solutions from Our Standard Technology Suite deemed suitable

for this purpose. Any attempt to circumvent Our work in this regard will be deemed an intrusion attempt and will be dealt with accordingly.

- ⇒ Prior to the initial use of any mobile device on Your IT Network, **the device must be registered on Your system by Us**. We will maintain a list of approved mobile devices and related applications and reserve the right to disconnect and refuse access to devices not on this list.
- ⇒ We reserve the right to inspect and monitor all mobile devices attempting to connect to Your IT Network through the Internet (or other unmanaged network).
- ⇒ We routinely patch and update mobile devices to ensure that all firmware, applications and operating systems are up-to-date and mobile devices are protected from vulnerabilities.
- ⇒ We also perform routine security audits on mobile devices to ensure that no potential threats to the company IT Network and data are present.
- ⇒ We reserve the right to temporarily restrict the ability to connect mobile devices to Your IT Network if We suspect that such equipment is being used in such a way that puts Your IT Network, its data, users, and your business at risk. We further reserve the right to limit the ability of any user(s) to download, transfer or access data to and from Your IT Network or specific components thereof.
- ⇒ Users connecting mobile devices to outside infrastructure to access corporate data must employ a **personal firewall approved by Us**, along with and any other security measure We deem necessary.
- ⇒ Company owned laptop computers may only access the corporate network and data using an SSL, VPN, or IPsec VPN connection. Mobile VPN software must be installed on all smart mobile devices in order for users of these devices to access Your IT Network and data.
- ⇒ In monitoring Your network, We may create audit trails and use the reports generated to optimize Our processes and for investigation of possible breaches and/or misuse. To identify unusual usage patterns, suspicious activity, and accounts/computers that may have been compromised, all end users' access and/or connection to Your IT Network may be monitored to record dates, times, duration of access, and the like.

Data Encryption Requirements

- ⇒ All mobile devices that store corporate data **must use an approved method of encryption** to protect data.
- ⇒ Laptops must employ full drive encryption with an approved software encryption package. No corporate data may exist on a laptop in clear text.

Passwords

- ⇒ All mobile devices must be protected with a password that complies with the requirements of the Password Policy – including the requirements for password strength, confidentiality, storage and encryption.

Physical Security

- ⇒ All users of company mobile devices must secure all such devices whether they are actually in use, being carried, or being stored while not in use.

- ⇒ Passwords and confidential data may not be stored on [unregistered](#) personal/non-company devices.
- ⇒ Corporate data must be permanently erased from all mobile devices once their use is no longer required. In such cases, please contact us immediately so We can assist with wiping this data.
- ⇒ No person may perform any modifications to any hardware or software required or installed by Us without Our express written approval.

Reporting, Help & Support

- ⇒ If a mobile device is lost or stolen, it must be reported to Us immediately. We use remote wipe software to disable and delete any data stored on a mobile device reported lost or stolen. Upon recovery, the device may be re-provisioned.
- ⇒ While We offer support for mobile devices that meet Our hardware and software requirements, We are under no circumstances liable for any losses, damages, or issues caused by a) the use of unapproved media, hardware, or software; or b) any violation of Our policies, recommendations and requirements outlined in this Handbook or Your MSA. These limitations apply even if We are aware of the existence of nonconforming devices, software or practices.

PERSONAL DEVICE (“BYOD”) POLICY

While it may be unreasonable to require employees to leave their personal devices at home, certain steps must be taken in order to prevent unauthorized access to Your IT Network via employee’s personal devices.

General Personal Device Security Protocols

We recommend implementing the following security protocols to minimize the risk of a data breach or other security incident:

- ⇒ All personal devices that connect to Your IT Network or which store / have access to company data, should be protected with a password conforming to the requirements of the Password Policy.
- ⇒ All personal devices should be configured to auto-lock after being idle for more than 5 minutes, with a password, pin, fingerprint, retina scan or unique drawing required to unlock.
- ⇒ Devices should be configured to lock after 5 failed login attempts. Contact us to help with this setting, as well as for regaining access on devices that We have configured.
- ⇒ “Jailbroken” devices should be restricted from accessing Your IT Network.
- ⇒ Devices belonging to anyone who isn’t a member of Your team should not be allowed to connect to Your IT Network.
- ⇒ Access to company data via personal device should be limited to the permissions granted to the specific user. We should be contacted to set up user profiles and automatic access enforcement/restrictions on all personal devices used to access Your IT Network.
- ⇒ All personal devices should use an approved method of encryption during transmission to protect data.

- ⇒ Personal devices used to access Your IT Network may not be reconfigured without Our express approval.
- ⇒ All users must agree in writing to immediately report any incidents or suspected incidents of unauthorized data access, data loss, and/or disclosure company resources, databases, networks, and the like.

Our Rights as Your IT Service Provider

In order to perform Our jobs, We reserve the right to do any of the following if deemed necessary to protect the security of Your IT Network and data:

- ⇒ Configure and install any software We deem necessary to ensure the security of your IT Network (for example, anti-virus, remote wiping and other software) on any personal device used to connect to Your IT Network;
- ⇒ Restrict or limit users' ability to download, install or use certain websites and applications;
- ⇒ Limit the use of network resources by personal devices;
- ⇒ Impose restrictions on users' ability to transfer data to and from specific resources on Your IT Network;
- ⇒ Remotely wipe a user's personal device if needed, for example if the device is lost, the team member's relationship with the company is terminated, or if We detect a virus, data breach, policy breach, or other security threat to Your IT Network and data;
- ⇒ Disconnect devices or disable services without notification;
- ⇒ Periodically inspect and update personal devices to ensure that all firmware, apps, operating systems and security setting are up-to-date in order to prevent vulnerabilities and make the device more stable;
- ⇒ Monitor all personal devices and activities to record dates, times, duration of access, etc. in order to identify unusual usage patterns, suspicious activity, and accounts/computers that may have been compromised;
- ⇒ Treat any attempt to circumvent, bypass or contravene the security Policies as a security incident / data breach and respond accordingly. This includes terminating, without notice, any device's access to Your IT Network if We detect irresponsible, unethical, illegal activities, or actions in violation of the Policies set forth in this IT Policy Manual.

Liabilities, Risks & Disclaimers

- ⇒ While We take reasonable precautions to prevent loss of personal data in the event that we must remotely wipe a device, at times these precautions fail. Accordingly, it is the user's responsibility to take additional precautions, such as backing up their personal media, email, contacts, and other data they wish to protect.
- ⇒ Lost or stolen devices must be reported to Us within 24 hours. Team members should also notify their mobile carrier within 24 hours of a loss or theft.
- ⇒ We are not responsible for any losses or damages if they result from a team member's use of a device that is illegal, unethical, or in violation of this Policy or Our recommendations. Any labor performed mitigating issues from such actions is outside the scope of any Managed Service Plan and is billable according to Our hourly rates set forth in Your MSA.
- ⇒ All team members should execute an agreement by which they assume full liability for risks arising out of their use of their personal devices on Your IT Network. These include, but are not limited to, any loss or exposure of personal data or sensitive company information as a result of error, malware or other hardware/software failures on their personal devices.

POLICY REVISION HISTORY

Date	Policy	Summary of Change