ACCEPTABLE USE POLICY

Document Number: *123*	**Version: 1.0**
Date of Issue: *10/9/2015*	**Contact:** info@initech.com

Overview

Initech Solutions, Inc. (Initech) is a leading edge technology company that relies on innovation to differentiate our products from our industry competition. Electronic Devices and Electronic Data Communication enable our Employees and Third Parties to deliver the products and services our Customers demand.

Initech's Electronic Devices, Electronic Data Communications, and Electronic Networks are expected to be used for business purposes only. Appropriate Use of Electronic Devices and Electronic Data Communication can enable our business to continue serving as a market leader within our industry. Unacceptable Use can lead to malware infection, disruption of information technology services, inappropriate disclosure of sensitive Customer, Employee, or Company data, litigation claims, and other adverse circumstances.

All users at Initech are responsible for reviewing this policy and conducting their business activities in a manner that aligns with what has been defined as Acceptable Use.

This Policy will be reviewed and approved by the Board of Directors and the Chief Information Security Officer on an Annual Basis.

Purpose

The purpose of this Policy is to inform employees and Third Parties of Acceptable Use practices when using Electronic Data Communications at Initech. This policy is established to protect Initech, our employees, and our customers from the risks associated with Unacceptable Use.
The Initech Acceptable Use Policy clearly defines expectations for Acceptable Use and Unacceptable Use, responsibilities for ensuring compliance, and consequences associated with non-compliance.

Scope

This policy applies to all Initiech employees and Third Parties that use Initech Electronic Data Communication Devices over an Electronic Network.

Definitions

Key terms used throughout this policy are defined within this section. Specific examples are provided, however these examples should not be considered "all-inclusive" due to our dynamic and ever-changing technology landscape.

"Electronic Data Communication" is defined as any information or data that is created, stored, transmitted, processed, accessed or received by an electronic medium or device. Electronic Data Communication occurs via Electronic Devices over an Electronic Network.

"Electronic Devices" are devices used for Electronic Data Communications. Such devices include, but are not limited to, the following examples:

- Personal Computers (desktops, laptops, thin clients, netbooks, and handheld wireless devices)
- Telephonic devices (including desktop "land-line" telephones, Voice over Internet Protocol (VoIP), Wireless telephones, including "smartphones")
- Personal Digital Assistants (PDAs)
- Facsimile (fax) machines (paper or electronic)
- Wearable technology (including smart watches and glasses)
- Tablets
- Video recording devices
- Audio recording devices

"Electronic Networks" facilitate electronic data communications. This includes, but is not limited to, the following examples:

- Internet, email, Short Message Service (SMS) text messages, instant messaging, and Social Media platforms
- Data transfer protocols (e.g. FTP, SFTP)
- LAN (Local Area Networks) and WAN (Wide Area Networks)
- Cloud storage platforms (including Dropbox, OneDrive, Google Drive)
- Telephone "land" lines
- Wireless (e.g. Wi-Fi) networks
- Teleconferencing and video conferencing
- Voicemail

"Social Media" is defined as all internet platforms that allow individuals to communicate and share information over the Internet. Examples of such platforms include, but are not limited to the following:

- Public social networking sites (e.g. Facebook and LinkedIn)
- Initech Private Social Media network (i.e. Yammer)

- Video sharing and blogging (e.g. YouTube)
- Blogs and micro blogs (such as Twitter)
- Review and rating sites (e.g. Yelp)

"Third Parties" are individuals that provide services to our company but are not directly employed by Initech. Such individuals may be provided with:

1. Electronic Data Communication Devices issued by Initech and / or
2. Access to Initech's Electronic Networks. Such Third Parties must also adhere to the Acceptable Use Policy. Initech employees that manage the relationships with Third Parties are responsible for providing Third Parties with the Initech Acceptable Use Policy and all other relevant Initech policies. These employees are also responsible ensuring Third Party compliance with this Policy and reporting any incidents associated with Unacceptable Use.

"Initech Data" refers to any data or information that relates to Initech, its business (including intellectual property, product information, business strategies, and industry), corporate matters (including financial results and litigation), its employees, directors, customers, suppliers and competitors.

Policy Statements

- No Expectation of Privacy Disclaimer: While Initech network administration wants to provide a reasonable level of privacy, users should be conscious of the fact that the data created by them on the company's systems remains the property of Initech. Because of the need to protect the Initech network, management cannot assure the confidentiality of the information stored on any Electronic Device or Network belonging to Initech.

- Data Classification: All information contained on Initech Electronic Devices and Networks should be classified according to the Initech Data Classification Policy.
    - Examples of confidential information include but not limited to the following:
        - Company private or confidential
        - Corporate strategies or projections
        - Competitor-sensitive or competitive analyses
        - Intellectual Property (e.g. trade secrets, patents, test results, and research data)
        - Specifications, operating parameters
        - Customer lists and data

    Employees should take all necessary steps to prevent unauthorized access to this information. If an employee suspects that such information has been released outside the company, he or she should notify the Initech Information Security department immediately.

- Data Protection: Initech recommends that Initech Data classified as internal or higher (refer to Initech Data Collection Policy) be protected via appropriate controls (e.g. Access and

Encryption). For guidelines on encrypting email and documents, go to Initech's Data Management and Encryption Policy.

- Personal Usage: Employees and Third Parties are accountable for exercising good judgement and moderation when accessing Initech Electronic Devices and Networks for personal use. Management within each Individual department is responsible for creating their own guidelines regarding personal use of Initech Electronic Devices and Network. Users are responsible for contacting management or supervisors for guidance in absence of departmental policies.

- Logging, Monitoring, and Audit Rights: All network traffic is subject to logging of monitoring for purposes of audit, investigation, and performance management. Therefore, all Electronic Data Communications can be monitored at any time, per the Initech's Audit Policy. Initech and Third Party auditors engaged by Initech are entitled to audit networks and systems on a recurring or ad hoc basis to ensure compliance with this policy.

- Password Management: Passwords must be kept secure and login credentials should not be shared. Authorized users are responsible for the security of their own passwords and accounts. Refer to the Initech Password Policy for additional guidelines and requirements for company passwords.

- Unattended Electronic Devices: All Electronic Devices must be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging off manually when the host will be unattended.

- Phishing Awareness: Employees must exercise caution and judgement when opening email attachments received from unknown senders. Lack of such judgment may result in malware (e.g. Adware, email bombs, Trojan virus, etc.). When in doubt, employees are advised to manually scan showing the original headers of the document and contact the Initech Information Security Department at spam@initech.com before opening them.

- Public Opinions: Postings by employees from Initech email address to Social Media and other public sites should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Initech, unless posting is in the course of business duties (e.g. Corporate Public Relations Department).

- Anti-Virus and Malware Scanning: All Electronic Devices issued to employees and Third Parties may be continually scanned to detect viruses and malware connected to the Initech Electronic Data Network.

Acceptable Use

1. Compliance and adherence with the policies and guidelines set by the organization for the Electronic Devices and systems which you are granted access.
2. Intech employee and Third Parties can only use Electronic Devices and user accounts which he/she is authorized to.
3. Initech employees and Third Parties must take the responsibility for proper handling and usage of Electronic Devices and systems that includes the software, hardware and the network addresses.
4. All the employees and Third Parties must comply with the contractual obligations and license agreements to use the third party resources that they are authorized to use.
5. The employees must adhere to the Initech Password Policy and take necessary efforts to protect and maintain the passwords as per the organization standards.
6. Initech hardware and software are to be configured as per Initech standards and procedures so that the unauthorized access can be prevented.
7. Incoming e-mail and messages must be monitored properly before opening it and necessary steps have to be taken to avoid opening spam mail – a scan with the antivirus is recommended. Contact spam@initech.com with suspicious e-mails.
8. To obtain privileged access to restricted network locations or applications, proper justification must be submitted to the Intitech Information Security team and proper authorization steps must be followed.
9. Only use the company provided anti-virus and always ensure the latest patch updates and virus definitions are being deployed.
10. For the newly hired employees and Third Parties, the Initech NDA (Non-Disclosure Agreement) must be signed and properly understood.
11. You must hand over all company provided Electronic Devices and IT equipment that are authorized to your name before leaving the organization or department.
12. Only use Initech internal chat or instant messaging services to communicate with someone from the organization.

Unacceptable Use

The following activities are strictly prohibited, with no exceptions:

1. Unauthorized copying of copyrighted material including, such as photos, videos, music, text and other sources as well as installation of pirated software or programs without license.
2. Unauthorized use, copying and/or circulation of Initech copyrighted materials, patents, and other company's materials.
3. Unauthorized copying, storage, and transmission of Initech Data that is classified as Internal or higher (refer to Initech Data Classification Policy) outside of Initech Electronic Devices and Networks (e.g. USB thumb drives, external hard drives, Dropbox, etc.).

4. Installation and deployment of malicious software into the network or systems, such as Trojans, viruses, worms and other malicious codes.
5. Employees and Third Parties shall not engage in gaming, gambling activities over the Initech Electronic Devices and Networks.
6. Employees and Third Parties shall not view pornography or other graphic and offensive material over Initech Electronic Devices and Networks.
7. Exfiltration or exporting software programs, technical data, encryption or other technology that would violate international or regional export control laws.
8. Sharing login credentials with any other individual, including, but not limited to co-workers, family members, and friends.
9. Using Initech Electronic Devices to purchase, copy, transmit, or distributed asset to sexually offensive material or conduct Electronic Communications that are in violation of a user's local laws or ordinances.
10. Conducting fraudulent transactions using an Initech Electronic Device or Network.
11. Initiating security breaches or disruption of any internal or external network communications. Security breaches are defined as facilitating the access and distribution of data in other individual(s) are not authorized to view. Disruption of internal and external networks includes, but is not limited to, denial of service attacks, packet/network sniffing, packet spoofing.
12. Network scanning and monitoring is strictly prohibited unless it is part of an employee's job function to do so.
13. Evading security protocols or circumventing routine authentication controls (e.g. brute force password attack) is strictly prohibited.
14. When using company resources to access and use the Internet and Social Media, users are prohibited from publishing opinions on behalf of the company. When stating an association to the company, Employees and Third Parties must indicate that “The opinions expressed are my own and not necessarily those of Initech Solutions, Inc.”
15. Sending unsolicited email messages, including the sending of "junk mail" or sending spam email to individuals who did not specifically request such material.
16. Harassment via email, telephone, texting, emailing, whether through language, frequency, or size of messages.
17. Unauthorized use, or forging, of email header information.
18. 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.
19. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
20. Use of uncalled-for email originating from within Initech's networks of other Initech Electronic Devices and Network service providers on behalf of, or to advertise, any service hosted by Initech or connected via Initech's network.
21. Posting the same or similar personal messages to large numbers of Users on Initech Network.
22. Initech’s Confidential Information policy is applicable to Social Media. Therefore, Employees are forbidden from revealing any Initech’s confidential information when engaged in blogging.
23. Employees and Third Parties shall not participate in any Social Media activities that may damage or smear the image and reputation of Initech and any of its employees. Employees are also proscribed from making any prejudiced, critical, or derogatory comments when blogging or

otherwise engaging in any conduct prohibited by Initech's Non-Discrimination and Anti-Harassment policy.

24. Initech's trademarks, logos and any other Initech intellectual property may also not be used in connection with any blogging activity

Compliance / Enforcement

Violation and or non-compliance of this policy will result in strict disciplinary action that may include termination and/or suspension for employees, Third Parties, contract workers, consultants, interns and volunteers; additionally, individuals are subject to loss of Information Resources access privileges, civil, and criminal prosecution.

Above stated policies in this document include action steps to be taken to determine whether or not an individual has, in fact, misused Initech's computing and/or network resources. Protections of the rights of individuals accused of policy violations afforded by those policies also apply.
Users who misuse Initech's computing and network resources or who fail to comply with the Initech's written usage policies, regulations, and guidelines are subject to one or more of the following consequences:

1. Temporary deactivation of computer/network access
2. Permanent deactivation of computer/network access
3. Disciplinary actions taken by the department or Human Resources up to and including expulsion from company or termination of employment
4. Subpoena of data files
5. Legal prosecution under applicable federal and state laws
6. Possible penalties under the law, including fines and imprisonment

(Note: Agencies need to be aware of the dynamic legal framework of the environment in which they operate, and they must adapt accordingly. Appropriate legal advisors and/or human resources representatives should review the policy and all of the procedures in use for policy enforcement.)

Exceptions

Exceptions to this policy will be considered only when the requested exception is documented using the Exception Handling Process and Form and submitted to the Chief Information Security Officer and Policy Review Committee.

Related Documents

- Email Maintenance and Archiving Procedures
- Data Collection Policy
- Data Classification Policy
- Human Resource policies
- Non-Discrimination and Anti-Harassment policy
- Audit Policy
- Data Management and Encryption Policy
- Password Policy

Version Control

Version	Published Date	Release Comments
1.0	October 9, 2015	First version of Initech Acceptable Use Policy released after approval from the Board of Directors and the Chief Information Security Officer