Data Privacy and Protection Policy for IT Systems

Table of Contents

1. Introduction

1.1. Overview

Our **Data Privacy & Protection Policy** refers to our commitment to treat information of employees, clients, stakeholders and other interested parties with the utmost care and confidentiality. With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

This policy is designed to protect Throughline Strategy Inc. (herein referred to as Throughline), our employees, customers and other partners from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions. This policy should be reviewed at minimum every two years and updated as needed.

Internet/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 Throughline. 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 Throughline 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. Everyone who works at Throughline is responsible for the security of our IT systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it impacts their role they should speak to the Managing Partners.

All Throughline employees, contractors or other users with access to Throughline data, must review and sign this policy on an annual basis. Throughline is committed to doing due diligence in background checks for all users, employees and contractors who will gain access to data.

1.2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and data at Throughline. Inappropriate use exposes Throughline and its clients to risks including virus attacks, compromise of network systems and services, and legal issues.

1.3. Scope

This policy refers to all parties (employees, job candidates, clients, contractors, suppliers etc.) who provide any amount of information to us, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Throughline, as well as personal mobile devices of employees and contractors.

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

This policy covers only internal use of Throughline's systems, and does not cover use of our products or services by customers or other third parties.

Some aspects of this policy affect areas governed by local legislation in certain countries (e.g., employee privacy laws): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases local teams should develop and issue users with a clarification of how the policy applies locally.

1.4. Data Privacy Officer

Nadia Sapiro, Managing Partner, is also designated as Throughline's Data Privacy Officer

2. Definitions

"Users" are everyone who has access to any of Throughline's IT systems (physical, network, documents stored in the cloud etc.). This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, customers and business partners.

"Systems" means all IT equipment that connects to the corporate network or access corporate applications and data. This includes, but is not limited to, laptops, desktop computers, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, cloud storage systems (namely Box and GSuite) and all other similar items commonly understood to be covered by this term.

3. Acceptable Use

3.1. General use & Ownership

3.1.1. Throughline proprietary information stored on electronic and computing devices whether owned or leased by Throughline, the employee or a third party, remains the sole property of Throughline.

3.1.2. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Throughline proprietary information.

3.1.3. You may access, use or share Throughline proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

3.1.4. Throughline's systems exist to support and enable the business. A small amount of personal use is, in most cases, allowed. However, it must not be in any way detrimental to users' own or their colleagues' productivity and nor should it result in any direct costs being borne by Throughline other than for trivial amounts (e.g., an occasional short telephone call).

Throughline trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company's IT systems. If employees are uncertain, they should consult their manager.

3.1.5. Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorized access is prevented (or at least made extremely difficult). However, this must be done in a way that does not prevent–or risk preventing–legitimate access by all properly-authorized parties.

3.1.6. For security and network maintenance purposes, authorized individuals within Throughline and/or it's contracted security company, namely ConnectAbility, may monitor equipment, systems and network traffic at any time. Throughline can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history of any users.

3.1.7. Throughline reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.2. Data Security and Confidential Information

Users must take all necessary steps to prevent unauthorized access to confidential information. Confidential information includes but is not limited to: internal working documents, information provided by clients about their business, health information and identifying information of any person included in any market research activity etc.

Users are expected to exercise reasonable personal judgement when deciding which information is confidential. When in doubt, users should assume information is confidential.

Users must not send, upload, provide access to, remove on portable media or otherwise transfer to a non-Throughline system/party or individual any information that is designated as confidential, or that they should reasonably regard as being confidential to Throughline, except where explicitly authorized to do so in the performance of their regular duties.

Users who are supplied with computer equipment by Throughline are responsible for the safety and care of that equipment, and the security of software and data stored it and on other Throughline systems that they can access remotely using it.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into Throughline's systems by whatever means and must report any actual or suspected malware infection immediately.

Requirements & Behaviours

3.2.1. All mobile and computing devices that connect to the internal network must comply with this policy. Only authorized devices may be used to access Throughline data and systems

3.2.2. System level and user level passwords must comply with the Password Standards (2.4). Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

3.2.3. All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

3.2.4. Laptops and confidential or proprietary information must be locked up every night in the office. Pedestals and cabinets where equipment and documents are stored must be locked and the key must not be hidden in proximity to the pedestal or cabinet.

3.2.5. You must never leave your device(s) unattended outside of the Throughline offices.

3.2.6. Use of Privacy Screens is mandatory in any public space (airport, coffee shop, client offices, etc.)

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

3.2.8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

3.2.9. The entrance to the physical office remains locked at all times. Employees are provided with a key to the office entrance during on-boarding. Under no circumstances should any employee or visitor prop the door open. To access elevators or building entrances outside of regular business hours (8am-6pm) Employees are required to use a digital keycard, provided during on-boarding.

3.3. Remote Access & Working From Home

It is the responsibility of Throughline employees, contractors, vendors and agents with remote access privileges to Throughline's cloud systems and tools to ensure that their remote access connection is given the same consideration as the user's on-site connection to Throughline.

General access to the cloud systems and tools (herein referred to as “systems”) Throughline uses to conduct business is strictly limited to Throughline’s employees, contractors, vendors and agents (hereafter referred to as “Users”). When accessing the system from a remote location, Users are responsible for preventing access to any Throughline computer resources or data by non-Authorized Users. Performance of illegal activities through Throughline’s systems by any User (Authorized or otherwise) is prohibited. The User bears responsibility for and consequences of misuse of the User’s access.

Requirements & Behaviours

3.3.1. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong passwords, Two-Factor authentication, etc. For further information see the guidelines on Passwords (2.4))

3.3.2. While using a Throughline owned computer to remotely connect to systems, Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an User or Third Party.

3.3.3. Use of external resources or systems to conduct Throughline business must be approved in advance by the Managing Partners and the appropriate manager.

3.3.4. All Users that are connected to Throughline’s systems via remote access technologies must use the most up-to-date anti-virus software (as provided by ConnectAbility)

3.3.5. Users using any Android device are responsible for ensuring the device is protected with anti-virus software and all data accessed via that device is encrypted

3.3.6. Any physical documentation containing or pertaining to confidential or proprietary information must be stored and disposed of in a manner that it will not risk the exposure of this information (i.e. locked up, shredded, etc.) If Users have any questions around the storage and disposal of documentation while working remotely, they should speak to their direct manager

3.4. Passwords & Encryption Standards

3.4.1. Passwords are required to comply with the following parameters: minimum of 8 characters, include upper- and lower-case letters, include at minimum one number, included at minimum one special character.

3.4.2. All standard passwords on new devices or user accounts must be changed immediately upon first login

3.4.3. Two-factor authentication must be enabled for all compatible systems (i.e. Gsuite, Box, etc.)

3.4.4. Any device (i.e. cellphone, laptop, USB key, etc.) where users access Throughline or client data or information must have a robust password or passcode

3.4.5. Encryption is required for all devices and folders where Throughline or client data is stored or accessed

3.4.6. Passwords for systems must be changed at a minimum every 180 days, with no reuse of the previous 6 passwords

3.4.7. It is prohibited to reveal 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.

4. Unacceptable Use

All employees should use their own judgment regarding what is unacceptable use of Throughline's systems. The activities below are provided as examples of unacceptable use, however it is not exhaustive. Should an employee need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from their manager before proceeding.

- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.
- All activities detrimental to the success of Throughline. These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation of the company.
- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).
- All activities that are inappropriate for Throughline to be associated with and/or are detrimental to the company's reputation. This includes pornography, gambling, inciting hate, bullying and harassment.
- Circumventing the IT security systems and protocols which Throughline has put in place.

5. Access Control

Access controls are necessary to ensure only authorized users can obtain access to specific information and systems. Access controls manage the admittance of users to systems resources by granting users access only to the specific resources they require to complete their job-related duties.

5.1. Throughline will provide access privileges to systems based on the following principles:

Need to know – Users or resources will be granted access to systems that are necessary to fulfill their roles and responsibilities.

Least privilege – Users or resources will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.

Role based – access to data and resources will be granted in accordance to the role of the User

5.2. Requests for users' accounts and access privileges must be documented and appropriately approved.

5.3. Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared / generic accounts, test accounts and remote access) must be documented and approved by either Robert Knox or Nadia Sapiro.

5.4. Review of access privileges for administrator level accounts is reviewed at minimum every 180 days, as well as at the completion of any project or initiative in which access to data or resources was granted, by an Administrator, namely the Managing Partners

5.5. Users access will be reviewed within 30 days of that User's role changing (i.e. moved clients or departments) by an Administrator, namely the Managing Partners

5.6. Access to systems will be revoked within 48 hours of a User's termination, whether it is an employee, contractor or any other previously authorized User.

5.7. Emergency Access Changes: Access elevation for required circumstances is occasionally permitted in order to remediate issues or restore service. Throughline limits elevated access required to only the duration of such an event. Access and activities are recorded, and access removed at the end of the event.

5.8. Throughline shall ensure that changing of the access rights are part of the normal change control process, including authorization, notification and removal when elevated access is no longer necessary

6. Data Breach & Response

Any individual who suspects that a theft, breach or exposure of data has occurred must immediately provide a description of what occurred via email to the Managing Partners, as well as notifying them by phone call and/or in person, to ensure the email does not get missed and action is taken immediately.

the Managing Partners, along with the ConnectAbility team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, they will follow the appropriate procedure depending on the class of data involved. See Throughline's *Data Breach Policy & Procedure* for more information

7. Enforcement

Throughline will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, employees should be aware that consequences may include the termination of their employment as well as potential for legal action.

Use of any of Throughline's resources for any illegal activity will usually be grounds for summary dismissal, and Throughline will cooperate with any criminal investigation and prosecution that may result from such activity.

8. Declaration

All employees must sign this agreement to adhere to the*Throughline Data Protection and Privacy Policy for IT Systems.*