Just the Tech (JTT)
Acceptable Use Policy

Created by IT Security Team

Zach Cehelsky-DeAngelo, Kerwing Hy, Ian Johnson, Steven Tang, David Wynne

Contents

Purpose of the Policy

The purpose of this policy is to create a clear understanding throughout Just the Tech (herein "JTT") about acceptable and unacceptable use of technology and network devices. This policy reflects the established legal, ethical, open, and honest culture at JTT.

JTT provides technology devices, networks, servers, and information systems to its employees to achieve goals and initiatives, while JTT strives to maintain the confidentiality, integrity, and availability of JTT assets. This policy asks employees to comply to prevent potential legal issues.

Scope

The policy encompasses all aspects of our company's environment (hardware, software, business systems, administration systems, environmental controls, databases, data, and networks). All JTT employees, contractors, and temporary workers fall within this policy's jurisdiction. JTT recognizes potential unacceptable uses in: (1) Information Assets, (2) Devices, (3) Networks, and (4) Electronic Communications.

JTT will utilize this document to inform employees so each employee understands the JTT's legal, regulatory, and client obligations.

Intended Protected Assets

The Acceptable Use Policy and associated standards have been established to protect the following:

1. JTT's investments
2. JTT's sensitive information contained within the company's systems
3. JTT's goodwill and reputation
4. JTT's financial standing
5. The customer's and JTT's proprietary information, including:
    - Confidential information
    - Personal information
    - Credit card information
    - Protected health information (PHI).

Timeframe

This Acceptable Use policy is applicable to the company's current infrastructure, systems, architecture, culture and it is effective from the date of issue of this policy.

Management Roles and Responsibilities

Given that this Policy could be violated by internal employees on JTT Networks and Electronic Communication, JTT has established the following categories of roles and responsibilities in lieu of a security vulnerability:

Information Security Board of Review

1. The Chief Information Officer and leaders from each business area make up the appointed authority who will provide overall oversight and direction regarding appropriate information usage
2. The board will oversee the data custodians, data owners, and data users so that they can enforce proper information usage, the company's policy, related recommended guidelines/Guidance Documents, operating procedures, and technical standards.

Data Custodians

1. The Data Custodians works with the Board of Reviewers to define the information system architecture, hardware, software, applications, and databases. These individuals understand how the company's information assets are stored.
2. After the Board's approval of above structures, the Data Custodians utilize physical and technical safeguards, the arrangement, strategy, and controls to safeguard the data that the users interact with.
3. Implement of an access control systems to help 7prevent inappropriate disclosure.
4. These individuals document and distribute managerial and operational procedures to the business users to ensure consistent storage, processing, and transmission of information resources.

Data Owners

1. Data owners are accountable for specific data that employees interact with, store, transmit, and process because of certain roles associated with their job functions.
2. These individuals manage and control the permissions and who has access to appropriate classifications of information resources (based on roles, sensitivity, and value). They supervise the use and protect the data owned by the firm.
3. These individuals ensure the compliance of the firm's employees and report any serious issues to the board of reviewers availability of information assets

Data Users

1. Users receive authorization, based on their roles and job function, to access use, process, store, and process specific company information and data that they are required to interact with in order to do their job.
2. Users are required to follow the policies, procedures, and guidelines that are put in place by the Data Custodians and Owners.
3. Report all suspected and/or actual security or policy breaches to the Data Custodians, Owners, and IT Security.

Policy Placement

Aside from general requirements, JTT recognizes four primary allocations of JTT Information Technology: (1) Accounts, (2) Assets, (3) Networks, and (4) Electronic Communications. Please find the following policies following each division below.

General Requirements

1. All employees are responsible for exercising good judgment regarding appropriate use of JTT's resources in accordance with JTT's policies, standards, and guidelines. JTT's resources may not be used for any unlawful or prohibited purpose.

2. Devices that interfere with other devices or users on JTT's network will be disconnected. In addition, blocking authorized audit scans is prohibited. Firewalls and other blocking technologies must have constant and consistent access to all JTT digital assets.

Accounts

1. All employees are responsible for the security of data, accounts, and system assets that are entrusted to them. Passwords must meet all of the following requirements:
   - Uppercase character(s)
   - Lowercase character(s)
   - A number
   - Non-alphanumeric character(s) – i.e. $, %, #
   - Be a minimum of 10 character(s)

2. Passwords must be kept secure and cannot be share with anyone under any circumstances. Failure to keep accounts secure, either deliberately or unintentionally, is a violation of this policy.

3. All employees must agree through legal or technical means that proprietary information remains within the control of JTT at all times. Storing proprietary information on non-JTT controlled environments are prohibited. JTT's information is owned by the organization and can only be used for projects to benefit the organization's interest. Employees are considered stewards who must protect and supervise the use of this information in order to benefit the company.

4. The Human Resources department must notify the IT department with 48 hours to revoke user rights if an employee leaves JTT for a period lasting longer than 14 days.

Assets

1. All employees are responsible for the protection of JTT's assets. This includes the use of computer cable locks and other security devices. For security reasons, JTT will provide devices and prohibits users from using their own devices. Any incident of theft must be promptly reported to JTT's IT Security department.
2. No workstation is to be left unattended for any duration of time. Employees are required to either logout or lock the computer before leaving their station. If a violation is spotted, employees are obligated to immediately notify a member of the IT department.
3. Third-party software installation will be unauthorized and blocked. Only the IT department will be able to update or install programs, after proper documentation and approval has been given.

Networks

All JTT employees are responsible for network resources under their disposal. The following actions are strictly prohibited

1. Creating a security breach on JTT networks or other affiliated networks, including, but not limited to, retrieving unwarranted and unauthorized data, information, or servers; bypassing authentication; or monitoring network activity.
2. Causing disruption of service to JTT networks or initiating said disruptions from JTT. This could include, but not is not limited to:
    - ICMP floods,
    - Packet spoofing,
    - Denial of service (DOS attacks)
    - Malicious forged routing information
3. Initiating honeypots, honeynets, or the like on JTT networks
    a. Note: honeypots and honeynets are decoy networks that redirect attackers from important or core servers.
4. Infringe upon copyright laws such as duplicating or sending copyrighted files (music, software, etc.)
5. Actively and purposely introducing malicious codes such as: viruses, worms, Trojan horses, spyware, adware, keylogs, etc.
6. Port or security scanning unless authorized by JTT Information Technology Security

Electronic Communications

The following actions are strictly prohibited

1. Supporting illegal activities and procuring or transmitting confidential or proprietary information
2. Sending Spam via any communication vehicle (email, text pages, voice mail, etc.)
3. Misrepresenting, spoofing, or forging a user identity
4. Posting to a public bulletin or arena that reveals your position at JTT. Use good judgement to not misrepresent JTT
5. Using JTT communication (email, office phone number) for personal subscriptions, newsletters, or leisurely affiliations

Established Security Mandates

Understanding JTT Data Classification

It is essential that all JTT employees understand the Data Classification Tier system. The tier system dictates and organizes JTT's assets to prioritize security measures.

- **Public/Unclassified**: information that is not confidential and can be made public without any implication for the organization:
- **Sensitive**: information that requires special precaution for its protection (ex: financial information about the organization). If disclosed it could result in a negative impact on the organization
- **Private**: information that is used privately within the organization (ex: customer data, employee records, etc.). Private data is intended for internal use only and if disclosed, it could result in a negative impact on the organization.
- **Confidential**: any proprietary information central to the operation of the organization (ex: trade secrets, research and development information for upcoming projects). If an organization's confidential data is disclosed, it could result in a significant negative impact on the mission of the organization.

Note: Sensitive, Private, and Confidential information should be handled with extreme care and any misuse or distribution of this data information will result in consequences (refer below).

Consequences for Non-Compliance

Any employee found violating this policy will be subjected to investigation by JTT's Information Technology Security department. Depending on the severity, impact, and timeframe of the violation, the JTT affiliate (employee, contractor, temp, etc.) may face suspension and/or employment termination.

Additionally, any local, civil, or federal laws that were violated by said non-compliance policy actions, will be followed through to the fullest extent possible.

Questions or Concerns

If there are any questions or concerns regarding this policy, please contact the JTT IT Security Team at Extension 1-1337

If you wish to report any suspicious or illegal activities, please call JTT's anonymous tip line at 1-877-264-6272

We appreciate your cooperation and understanding

Acknowledgement: SANS Institute, Forum of Incident Response and Security Teams (FIRST)

Effective Immediately (as of Friday, October 09, 2015 @ 11:59pm)

Revision notes:

Created by JTT IT Security – Friday, October 09, 2015