**WAT Team Members**
Zachary Cehelsky-DeAngelo, Kerwing Hy, Ian Johnson, Steven Tang, and David Wynne

**Executive Summary:**
Just the Tech (herein referred to as "JTT") has expressed a commitment to establish and maintain integrity, respect, trust, and transparency at its enterprise. As a result, JTT has recently enacted an Acceptable Use Policy (AUP). We Audit Tech's (WAT) goal and purpose is to ensure that JTT's controls are be implemented throughout the organization. This audit report correlates JTT's implemented controls with metrics to monitor effectiveness. Additionally, WAT has provided a series of other recommendations to JTT's AUP. WAT hopes to demonstrate its capabilities and dedication to being the best auditor for JTT.

**JTT's Acceptable Use Policy: "**Create a clear understanding throughout Just the Tech (herein "JTT") about acceptable and unacceptable use of technology and network devices. 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." (JTT - Acceptable Use Policy, October 9, 2015)

**Purpose of the WAT's Audit**: Just the Tech (JTT) has entered the market to ask third party consultants to ensure that JTT employees, contractors, and temporary workers are abiding by JTT's new implemented Acceptable Use Policy (AUP). WAT, one of these third party consultants, has expressed the following objections in conjunction to JTT's Acceptable Use Policy:

1. Establish and enforce an appropriate and acceptable practices in regards to accept use of JTT's equipments and information assets.
2. Ensure compliance with applicable rules and regulations in regards to the management of JTT's information assets
3. Educate JTT's employees understand the necessity of JTT's Controls and WAT's Audit in order to protect JTT's equipments and information assets.

**Scope**: Written permission and consent from the Board of Directors and JTT's Chief Information Officer (CIO), WAT will proceed to audit the following areas: (1) Accounts, (2) Assets (including both operation technology and information technology/infrastructure), (3) Networks, and (4) Electronic Communications. Associated parties include: employees, contractors, and temporary workers fall into the purview of WAT's audit of JTT's systems and infrastructure.

**Proposed JTT Auditing Plan**
The below matrix lists JTT's AUP intended policy goals, suggested JTT controls, the observed evidence/criteria WAT would monitor, and further actionable items.

| JTT Policy Goals | Implemented JTT Controls | Evidence/Metrics Criteria for WAT Audit | Further Actionable Items |
|---|---|---|---|
| Exercising good judgement with JTT resources in accordance with | Monitoring network, firewall logs, and activity logs | Number of attempts to connect to prohibited or blocked sites (for example: Facebook, | An analysis of other sites or URLs frequently visited by JTT Employees that could be considered inappropriate or |

| | | | |
|---|---|---|---|
| policies and standards | | YouTube, Twitter) using network monitoring software. | potentially harmful to JTT systems. |
| Password Security | Password Requirements are met and Passwords Changes are made every 6 months. Passwords are not affiliated with personal information. | How often JTT employees requires a password change and analyze whether the time frame is adequate for JTT's needs. | Collect and analyze the list of JTT employee passwords through a dictionary subscription/dictionary attack. |
| No Data Extraction of JTT Information | Hardening of all JTT USB ports<br>"Other unauthorized email services are blocked while on an authorized asset" | (Physical controls has achieved goal)<br><br>Analyze the amount of communication to third party email providers on firewall and network logs | Although JTT has hardened all of its USB ports, this could have been more detrimental to productivity:<br>- Analyze the effectiveness of this control and provide suggestions of certain operations that need this control<br>- Monitor and control communications between third party email providers. |
| Prohibited Use of Computers: Hacking or Illegal Extraction of PII | Data Loss Prevention (DLP) monitoring of JTT Systems | Evaluate the number of attempts and severity of each DLP record | Aside from effective monitoring, WAT can provide analytics and trending to see if certain employees are flagging DLP.<br>Scanning JTT Network and boxes for known hacking tools and software (Kali Linux, Nessus, Metasploit, etc.) |
| Ensuring information is only accessed from company machines | No Remote Access Availability to JTT Employees | Though this control achieves JTT's goals, this could hinder productivity | WAT can conduct brief surveys of each business unit to see if remote access would be beneficial.<br>Implement strong Remote Access Database Management and collection of non-JTT IPs<br>Explore the idea of VPNs for remote access for enhanced security. |

| | | | |
|---|---|---|---|
| Account Security and handling the dismissal of an employee | JTT notes that its HR must be notified if an employee leaves JTT for a period lasting longer than 14 days | How long it takes HR to respond to the notification.<br><br>The amount of time it takes for an employee to be relinquished of their permissions, passwords, and access. | Analyzing the effectiveness of JTT's HR and potentially noting if it would more effective if business unit managers should be given this responsibility.<br><br>Ensure this process is streamlined for employees that are fired, on disability leave, on maternity leave, or on an extended vacation. |

**Suggested Acceptable Use Policy Amendments**
WAT has noted additional items that JTT could consider implementing in its AUP Policy

| WAT Suggestion | AUP Value | Implemented Controls | Metrics/Evidence |
|---|---|---|---|
| Educational seminars about Employee Rights, Monitoring Expectations, and Legal Issues | JTT's policy needs to be understood and accepted by all JTT Employees and by requiring educational seminars can ensure that each JTT employee is aware and understands why the AUP is in place. | A required training course and monthly reminder emails to spread awareness about the AUP. | WAT can create legal forms of acknowledgement for each employee.<br>Additionally, WAT can monitor the traffic of the emails being sent out and provide effective metrics to ensure these emails are being read. |
| Erecting Language Filters or Barriers | Using profanity or other unprofessional language in a JTT Work setting can become a liability in the future. | Language filtering and flags. All profanity can be censored and any sexist language, obscenity, and offensive language will be flagged. | WAT can monitor this unacceptable language and note trends whether it be in a certain business unit or during a certain work season. |
| Implement a Reporting Process for Unacceptable Use | An anonymous vehicle for employees to report unacceptable use demonstrates JTT's commitment to enforcing the AUP and promotes a better working space. | JTT can either provide an anonymous email, a secure tip line, or developed portal to create tickets about unacceptable use seen throughout the company. | WAT can monitor these ticket submissions and analyze the frequency and origin of the ticket. |

| | | | |
|---|---|---|---|
| Offering an Amnesty Period of Employees | The goal of the AUP is to ensure that JTT employee understand what is acceptable and unacceptable on JTT systems. Offer a 14-day period for employees to clean out their computer disks, e-mail archives and personal network shares before regular audits and monitoring commence. | Nothing on-going.<br><br>This would be a onetime ordeal with current JTT employees to demonstrate that JTT Management is taking this seriously and actively enforcing the policy | Prior to offering this amnesty policy, WAT can perform a preliminary scan of JTT network of a "as-is" state and then perform the scan again after the amnesty period. WAT can collect information such as number of attempts to block sites, attempts to access 3rd Party email providers, a list of current passwords, etc. |
| Incorporating the AUP Policy into JTT Hiring Contracts | Though not explicitly stated in the policy, JTT should include an addendum noting that the future JTT employees will be required to follow the AUP Policy | Nothing on-going.<br><br>Implementing this suggestion would ensure that the AUP policy is being consistent despite JTT's recruitment of new employees | |

**Additional WAT Offerings**

Automation Change Detection: WAT can utilize and implement an Automaton Change Detection system to automate and reduce time for insuring that JTT has a current view of assets in its current environment. WAT would be able to lighten scripts, spreadsheets, and manual processes for compliance data collection. This will reduce 700 hours of work down to 150, while providing higher quality data for our auditors.

Summary of key benefits: multi-tool, multi-vendor, multi-location all in a consolidated view, improves accuracy and quality of compliance and reporting, reduces general cyber security risks (internal and external), monitors system performance, and improves situational awareness.

Encryption Services: Noted in JTT's AUP is a section regarding data classification. WAT can ensure that JTT is compliant in the encryption space for its confidential and private information as well as advising proper procedures and protocols for other data classification tiers. Encryption would include JTT hardware, systems, and internet services.

**Conclusion**

WAT has provided its opinions, auditing metrics, and further potential additions to JTT's Acceptable Use Policy. We hope JTT considers WAT as its IT Auditors given the work above. We look forward to this partnership with JTT.