Acceptable Usage Policy

Document No – TT-ITP/15

Document Release Note

Document Version	1.0	**Release Date**	

Prepared By		**Approved By**
Pathik Patel		**Chetan Patel**

Document Revision History

Version	Date	Change Description	Modified By	Reviewed By	Approved By
1.0					

Purpose

This Acceptable Usage Policy covers the security and use of all TechSture information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Techsture employees, contractors and agents (hereafter referred to as 'individuals').

Scope

This policy applies to all information, in whatever form, relating to TechSture business activities, and to all information handled by TechSture relating to other organizations with whom it deals. It also covers all IT and information communications facilities operated by TechSture or on its behalf.

Policy

Computer Access Control – Individual's Responsibility

Access to the IT systems is controlled using User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the TechSture IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any TechSture IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access TechSture IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorized changes to TechSture's IT systems or information.
- Attempt to access data that they are not authorized to use or access.
- Exceed the limits of their authorization or specific business need to interrogate the system or data.
- Connect any non- TechSture authorized device from TechSture network or IT systems.
- Store TechSture data on any non-authorized TechSture equipment.
- Give or transfer TechSture data or software to any person or organization outside TechSture without the authority of TechSture.

Respective managers must ensure that individuals are given clear direction on the extent and limits of their authority regarding IT systems and data.

Internet and Email Conditions of Use

Use of TechSture internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to TechSture in any

way, not in breach of any term and condition of employment and does not place the individual or TechSture in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which TechSture considers offensive in any way, including sexually explicit, discriminatory, defamatory material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to TechSture, alter any information about it, or express any opinion about TechSture, unless they are specifically authorized to do this.
- Send unprotected sensitive or confidential information externally.
- Forward TechSture mail to personal non-TechSture email accounts (for example a personal Gmail account).
- Make official commitments through the internet or email on behalf of TechSture unless authorized to do so.
- Download copyrighted material such as music media (MP3) files, film and video files ( ) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect TechSture devices to the internet using non-standard connections.

Social media applications must be accessed only for business use and as per project requirements. The afore-mentioned internet usage best practices guidelines apply for social media access as well.

Clear Desk and Clear Screen Policy

To reduce the risk of unauthorized access or loss of information, TechSture enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.

- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-Site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with **TechSture remote working policy**.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places).
- Care should be taken with the use of mobile devices such as laptops, mobile phones, smart phones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only TechSture authorized mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software

Employees must use only software that is authorized by TechSture on TechSture computers. Authorized software must be used in accordance with the software supplier's licensing agreements. All software on TechSture computers must be approved and installed by the TechSture IT department.

Individuals must not:

- Store personal files such as music, video, photographs or games on TechSture IT equipment.

Viruses

The IT department has implemented automated virus detection and virus software updates within the limits. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than using approved TechSture anti-virus software and procedures.

Actions upon Termination of Contract

All TechSture equipment and data, for example laptops and mobile devices including telephones, smart phones, USB memory devices and CDs/DVDs, must be returned to TechSture. All TechSture data or intellectual property developed or gained during the period of employment remains the property of TechSture and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on TechSture computers is the property of TechSture and there is no official provision for individual data privacy, however wherever possible TechSture will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. TechSture has the right (under certain conditions) to monitor activity on its systems, including internet and email use, to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes.

It is user's responsibility to report suspected breaches of security policy without delay to their line management, the IT department, the information security department or the IT helpdesk. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with TechSture disciplinary procedures.

Records

Server log with time

Effective Measures

Nil