Shreetron India Limited

Table of contents

Shreetron India Limited

Revision History

Version	Issue Date	Prepared By	Approved By	Changes
1.0	02.04.2021	Vaneet Soni	A P Panwar	Initial Draft

Purpose:

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

Scope:

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

Shreetron India Limited

1. Acceptable Usage Guidelines

An acceptable use policy or fair use policy, is a set of rules applied by the owner, creator or administrator of a network, website or service that restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used.

2. Computer Access Control – Individual's Responsibility

Access to the AUA IT systems is controlled by the use of 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 AUA IT systems.

Individuals must not:

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

Project managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

a. Internet and email Conditions of Use

Use of AUA 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 AUA in any way, not in breach of any term and condition of employment and does not place the individual or AUA in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

i. Use the internet or email for the purposes of harassment or abuse.
ii. Use profanity, obscenities, or derogatory remarks in communications.
iii. Access, download, send or receive any data (including images), which AUA considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
iv. Use the internet or email to make personal gains or conduct a personal business.
v. Use the internet or email to gamble.
vi. Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
vii. Place any information on the Internet that relates to AUA, alter any information about it, or express any opinion about AUA, unless they are specifically authorized to do this.
viii. Send unprotected sensitive or confidential information externally.
ix. Forward AUA mail to personal (non AUA) email accounts (for example a personal Hot mail account).
x. Make official commitments through the internet or email on behalf of AUA unless authorized to do so.
xi. Download copyrighted material such as music media (MP3)files, film and video files(not an exhaustive list)without appropriate approval.
xii. In any way infringe any copyright, database rights, trademarks or other intellectual property.
xiii. Download any software from the internet without prior approval of the IT Department.
xiv. Connect AUA devices to the internet using non-standard connections.

b. Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorized access or loss of information, AUA enforces a clear desk and screen policy as follows:

i. Personal or confidential business information must be protected using security features provided for example secure print on printers.
ii. Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
iii. Care must be taken to not leave confidential material on printers or photocopiers.
iv. All work-related printed matter must be disposed of using confidential waste bins or shredders.

c. Working Off-site

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

i. Working away from the office must be in line with AUA/GoA Premote working policy.
ii. Equipment and media taken off-site must not be left unattended in public places and not left inside in a car.
iii. Laptops must be carried as hand luggage when travelling.

iv. Information should be protected against loss or compromise when working remotely (for example at home or in public places).Laptop encryption must be used.
v. Particular 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.

d. 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 AUA authorized mobiles to rage devices with encryption enabled must be used, when transferring sensitive or confidential data.

e. Software

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

2. Individuals must not Store personal files such as music, video, photographs or games on AUA IT equipment.

f. Viruses

1. The IT department shall install virus detection and virus software updates on the systems within the AUA. All PCs have antivirus software installed to detect and remove any virus automatically.

2. Individuals must not:
   i. Remove or disable anti-virus software.
   ii. Attempt to remove virus-infected files or clean up an infection, other than by the use of approved AUA anti-virus software and procedures.

g. Telephony(Voice) Equipment Conditions of Use

1. Use of AUA voice equipment is intended for business use. Individuals must not use AUA voice facilities for sending or receiving private communications on personal matters, exceptin exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

2. Individuals must not:
   i. Use AUA voice for conducting private business.
   ii. Make hoax or threatening calls to internal or external destinations.
   iii. Accept reverse charge calls from domestic or International operators, unless it is for business use.

3. Actions upon Termination of Contract

1. All AUA equipment and data, for example laptops and mobile devices including telephones, smart phones, USB memory devices and CDs/DVDs, must be returned to AUA at termination of contract.

2. All AUA data or intellectual property developed or gained during the period of employment remains the property of AUA and must not be retained beyond termination or reused for any other purpose.

4. Monitoring and Filtering

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

2. 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. AUA has the right (under certain conditions)to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

3. It is individual responsibility to report suspected breaches of security policy without delay to respective project manager, management, the IT department, the information security department or the IT helpdesk.

4. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Government disciplinary procedures.

5. The fore going are subject to the laws of India and the jurisdiction of Hon'ble High Court of State, shall have the exclusive jurisdiction on any dispute that may arise out of breaches of information security policies.