Table of Contents

Reviewed By : Rajeev Rai

Modified On : 01-01-2024

Next Review Date : 31-12-2024

IT Policy & Guidelines

1.0.. **Purpose**

To ensure adequate handling of company assets by all users and setting policies for data back-up, data access and password protection of data in soft form.

2.0. **Applicability**

All employees on company's roll, External Resources and Contractual Employees.

3.0. **Policy & Procedure**

3.1. **IT Hardware Policy**

3.1.1. For all approved official assets to user, user shall sign. **"Assets Receiving"** form at the time of issue of asset.

3.1.2. User is not permitted to upgrade/change /install any hardware device RAM, Hard Drive Laptop Charger, and Battery etc.

3.1.3. For any up gradation/change in the device, User shall take approval from his Department head/IT Department for the same.

3.1.4. In case of any assets (Laptop, charger, Mobile Sim, and accessories such as Pen Drive, Mouse, Laptop Carry bag, Laptop Adaptor etc.) theft /Lose from user, User will be responsible for the assets a n d he/she has to bear the cost of the assets.

3.1.5 In case of any physical damage of Asset such as Laptop Screen, Laptop Keyboard, Laptop Body etc., User will be responsible for the assets and he/she has to bear the full cost of the asset maintenance.

3.2. IT Software Policy

3.2.1. User is not permitted to install any software without prior approval from IT Department/Department Head.

3.2.2. User is not permitted to upgrade/Change preinstalled operating system.

3.2.3. The Limit of Internet usage is 1.0 GB/day from AirteINI mobile sims through data card predefined for every user, in caseof user exceed the limit he/she has to pay the over limit charges.

3.2.4. User is not permitted to access any unauthorized website such as Social Networking Sites, Entertainment sites, any websites recommend UNSAFE by Antivirus.

3.2.5. The Limit of Mobile Sim card usage is prefixed for every user, in case of userexceed the limit he/she has to pay the over limit charges.

3.2.6. Users are not permitted to use any unofficial messenger (except IP Messenger). during the office time.

3.3. Data Backup

3.3.1. Shared drive is created function wise & the same is circulated to respective department.

3.3.2. Access of shared drive is protected by username/password which is dedicated to each user uniquely.

3.3.3. Identification of important data pertaining to the respective department is to be identified by respective user & shall be kept on their respective shared drive.

3.3.4. User will be able to read, edit and paste the data on shared folder. Deletion function of data once saved is disabled for all users. In case of deletion, one Junk folder is created in each shared drive where user will move the data. IT administrator will have the rights to delete data from junk folder.

3.3.5. Emails back up is done on Online Dell Storage system in real time basis. In case of any crash of laptop or any unforeseen event where all email need to be restored again in system, can be done with in 48 Hrs.

3.3.6. Backup of all shared data saved in encrypted form on online server storage system which is secured by SOPHOS firewall.

3.3.7. Hard disk mirroring is enabled in Dell storage system. In case of any crash, there will be no data loss.

3.4. Data Access Policy

3.4.1. Data which is required to be accessed by multiple users is kept at file server.

3.4.2. Data Access Matrix is maintained by IT I/C in discussion with divisional heads.

3.4.3. Access is generally identified into two categories, i.e., READ and WRITE, Delete access is restricted for all except IT admin.

3.4.4. If access rights are not granted to a person then person would not be able to access the concerned file/folder.

3.4.5. When there is a requirement for granting access to a new user or when an existing user's access rights are to changed/modified, concerned divisional head would intimate written/verbally to IT in charge for this.

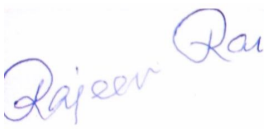
3.5. Password Policy

3.5.1. All users are in provided with a user ID and password at the time of issuance of laptop/desktop.

3.5.2. All users are required to change their password once in every 45 days.IT In charge retains admin rights and can be approached for help in case anyuser forgets his password.

3.5.3. All users are advised to ensure that their laptop/desktop is in hibernation mode or Shut Down before they leave their seats for any reason.

3.5.4. All users are advised to not to share passwords of their machines with anyone as they would be answerable for any breach of data due to any negligence on their part.



Approved By:

Mr. Rajeev Rai

Technical Director
Qauality austria central Asia