

Password Policy

1. Purpose.

The main purpose of this policy is to have a standard password system (in accordance to Industry best-practices) in place to ensure the security of confidential official data. Effective implementation of the Password Policy will minimize risk from password cracking or guessing and ensure the Confidentiality, Integrity and Availability of data.

2. This policy applies to all employees (who have access to official computer systems and confidential data)

3. Policy.

3.1. All users should be responsible for managing the passwords of their systems.

3.2. Users should their change their default password allotted by the administrator, on their first log-in.

3.3. The password should be alphanumeric. The password should be a combination of upper and lower case, should have punctuation characters as well as letters, for example the following characters can be used along with letters: 0-9,!@#\$%^&*()_+|~-=\{}[]:;'\<>?,./)

3.4. The complexity of the password should vary with the level of Information that it is used to protect.

3.5. The length of the password should be minimum eight (8) characters. It should not be any word from the dictionary or formed in any known pattern like a1b2 etc.

3.6. The server password should be changed every 15 days and other passwords should be changed in 30 days. The system should remember last 5 passwords.

3.7. The password should not be disclosed to any other person either over the phone, mail or any other medium.

3.8. The “remember password” feature present in applications and browsers should not be used.

3.9. As good practice passwords for official mail account and non-official mail personal accounts should be different.

4. Responsibilities.

VINOD SHARES LTD.

4.1. All employees should be aware of the Password Policy and it will be the responsibility of the Administrator to ensure employee awareness for the same.

5. Enforcement

5.1. Any employee/user found to have violated this policy should be subject to disciplinary action as per the rules of the organization.

6. Amendment/Termination of this policy.

6.1. Company reserves the right to modify, amend or terminate this policy at any time.

Back up storage and retrieval Policy

I. Purpose and Scope

The purpose of this policy is as follows:

- To provide secure storage for data assets critical to the work flow of official business
- To prevent loss of data in the case of accidental deletion /corruption of data, system failure, or disaster.

To permit timely restoration of archived data in the event of a disaster or system failure

This policy applies to all computers, both mobile and desktop, owned by the company

Backups are NOT meant for the following purposes:

- Maintaining a versioned history of data
- Personal data such as photos, videos, music, non-work e-mail accounts, etc.
- Programs (i.e., applications) of any type (personal or officially supported)
- Exceptionally large images (scanned or digitized material) and large video files. If you need this type of storage space, please contact Administrator to discuss alternative backup options available.

II. Backup and Recovery Policy

The following resources are made available:

- External USB hard drive: To backup user folders that are in excess of the 2 Gigabytes. Member from Administering will perform the initial configuration and schedule a backup policy.

All external drives must be locked in a secure location at the end of the work day.

- USB Thumb drive: Not supported as an official means of backup. These devices can easily be misplaced or lost resulting in the potential breach of official data. If utilized, the data must be encrypted if taken off the premises.

Backup Schedule and Retention

The Network backup system is utilized to retain data for 6 weeks or 42 days.

A combination of incremental and full backups is executed on the dataset. A full backup is performed every Friday with incremental backups thereafter.

Data Restoration

- **Emergency recovery:** Systems staff will make every attempt to recover the data within a business day. However, in the event of a catastrophic event, such as fire damage, services and data may be unavailable for an extended period of time.
- **Non-Emergency recovery:** These restorations will be performed on a time available basis, and will occur within the next five business days.
- **Required Information:** Users that need files restored must submit a help desk ticket request or contact Systemdept. The detail of the request should include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.