

## **Password Management Policy**

### **Introduction**

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Organization's resources. All users, including contractors, vendors, individual or organization with access to Organization's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and frequency of change. The scope of this policy includes all personnel who have or are responsible for an account, or any form of access that supports or requires a password, on any system that resides at our Organization's facility, has access to its network, or stores any non-public information.

### **Policy Details**

All user-level and system-level passwords must conform to the basic password creation rules as follows:

- The password must contain more than eight characters.
- Use a combination of upper case and lower case of letters, numbers, and special characters.
- Don't use personal information or common words.
- Use unique password for each account.

Each password must be unique; the passwords used for one account must not be used for another account. The Line Manager concerned must ensure that no password is repeated.

All employees must use KeePass Password Safe to store and retrieve all the passwords. The master password for the password database must be unique and conform to the password creation rules mentioned above.

All the master passwords must be documented, by IT Department, and submitted to Group Managing Director.

To ensure the safety of all the passwords all Line Managers must ensure that no password is stored in any medium except KeePass Password Safe. Line Managers concerned must ensure that all employees are using KeePass Password Safe for accessing the credentials, and no passwords are stored in the browser or in any other form or media.

All passwords must be changed by employee concerned as per the instructions of IT Department, unless the frequency is specified by the service provider. The Line Manager concerned must ensure that all passwords are changed, and the KeePass Password Safe is updated to reflect the updates.

In the event of any additions or change of passwords, due to additional responsibilities or additional subscription of services, Line Manager must ensure that the KeePass Password Safe is updated to ensure that all the credentials, usernames and passwords, are documented.

Passwords must not be shared with anyone, including co-workers while on vacation. All passwords must be treated as sensitive/confidential information. However, a password can be shared with co-workers if the business operation requires multiple employees to access said resource. Any event requiring an individual to share the password must be reported to, and approved by, the Line Manager concerned.

Passwords must not be transmitted to anyone, including contractors or vendors, over email, phone calls or any other means of electronic communication until the third-party has acknowledged the non-disclosure agreement, and approval of the Line Manager concerned is obtained.

Passwords must not be revealed in questionnaires or security forms to ensure the confidentiality of all passwords is maintained.



Do not document passwords and store them in any media, including sticky notes. No password should be stored in plain text format.

Any employee suspecting that their password may have been compromised must report the incident to IT Department and Line Manager concerned for further course of action.

In the event of lost or forgotten passwords, the Line Manager concerned must ensure the new password is generated for the said account within two working days to minimize any business disruption.

At the end of services of an employee, the Line Manager concerned must ensure that KeePass Password Safe is complete and accurate to mitigate any business disruption.

Any exemptions from these directives must be referred to, and approved by, the Group Managing Director.

Any breach of this policy must be referred Group Managing Director for reviewing the consequences of the breach and may be subject to disciplinary action, which can include confiscation of the device and/or termination of employment.