Document Name	Password Policy
Document Version	1.x
Effective Date	2022/04/01
Document Owner	
Document Classification	Internal Use

Table of Contents

PURPOSE

The purpose of this document is to establish rules and requirements related to configuration of password management systems and use of passwords by users

SCOPE

The policy contained within this document applies to all personnel managing information systems (applications, operating systems, tools, etc. that have a password management system feature for controlling passwords) as well as all users responsible for maintaining their passwords for accessing different information systems made available by Doceree. The users include, but are not limited to, employees, contract staff, vendors, etc.

TERMS AND DEFINITION

Following is an explanation of various terms used within this document –

Information System	:	An integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products. Examples – applications installed on servers and personal computers, cloud applications, servers, personal computers, standalone devices having firmware / operating system, tools, utilities, etc.
Password	:	A secret word or phrase a user of an information system needs to access such information system(s).

POLICY

1.0 General Rules

1.1 All information systems owned / operated / used by Doceree shall require identification and authentication through passwords, passphrases, one-time passwords, and similar password mechanisms as a minimum (a more restrictive/secure authentication mechanism is acceptable) prior to allowing user access.

1.2 Passwords for Doceree information systems shall be created in accordance with this policy and Doceree's other security policies, as applicable.

1.3 The Doceree's information systems (or their access control systems) shall be configured (where such configuration is possible) to fulfill the requirements of this policy and Doceree's other security policies, as applicable.

1.4 Passwords must be regarded as confidential information and shall not be disclosed to any other person.

1.5 Users shall be responsible and liable for all actions including transactions, information retrieval or communication on the Doceree's information systems performed by using their user-id(s) and password(s).

2.0 Password Validity Policy

2.1 All user-level passwords (e.g., application user, email, web, desktop computer, etc.) shall be changed at least every 3 months.

2.2 Doceree's information systems shall be configured (where this is possible) to enforce change of password every 3 months.

3.0 User Account Lockout Policy

3.1 Doceree's information systems shall be configured (where this is possible) to lock the User-ID and prevent user access to the information system where an incorrect user password has been used in sequence 3 times.

3.2 Locked Out user accounts shall be reactivated within 4 business hours if using an automated reactivate system or shorter, but no less than 15 minutes. Requesting a manual reactivation shall require identification of the user and determination of the reason for the lockout as a minimum for re-instating the user account and providing a new user password.

4.0 Password Uniqueness Policy

4.1 User accounts that have system-level privileges granted through group memberships or programs shall have a unique password from all other accounts held by that user.

4.2 Passwords used for Doceree's accounts shall not be the same as passwords used for other non-Doceree access (e.g., personal ISP account, option trading, benefits, etc.).

4.3 If possible, the same password shall not be used to access multiple Doceree systems.

4.4 Users shall not reuse any of their last 5 passwords.

5.0 Password Communication Policy

5.1 Passwords shall not be revealed in conversations, inserted into email messages or other forms of electronic communication except for the initial password during the setting up of their account or a password reset by an administrator.

5.2 Passwords shall not be written down, stored on any information system or storage device except in accordance with any existing Doceree password management procedures for safekeeping of passwords.

5.3 Users shall not use the "Remember Password" feature of applications. Doceree's information systems shall be configured (where this is possible) to disable remembering of passwords by users.

5.4 If an Doceree employee either knows or suspects that his or her password has been compromised, it shall be reported to the IT Team and the password changed immediately. (Note: Users can also request a new password through the automatic password reset mechanism on the application).

5.5 The IT or Information Security Team may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user shall be required to change his or her password immediately.

5.6 Initial passwords shall be communicated to users either verbally or via encrypted email. Emails containing passwords shall be deleted once they are read.

5.7 Initial passwords shall only be valid for the first log-on attempt. Doceree's information systems shall be configured (where this is possible) to force users to change the password on first use.

6.0 Password Composition Policy

6.1 All user-level & system-level passwords shall not be easily guessable and shall conform to the guidelines described below: -

a. Passwords must contain
   - At least one capital letter (A to Z)
   - At least one small letter (a to z)
   - At least one number (0 to 9)
   - At least one special character (!, @, $, *, etc.)

b. Passwords must be at least 8 characters long

c. A new password must contain at least 4 characters that are different than those found in the old password which it is replacing.

d. Passwords should not be a word in any language, slang, dialect, jargon, etc.

e. Passwords should not be based on personal information (such as name, birthday, address, phone number, social security number), names of family, friends, relations, colleagues, etc.

f. Passwords cannot contain all or part of your username/ID.

g. Passwords must not be based on publicly known fictional characters from books, films, and so on.

h. Passwords must not be based on the company's name or its geographic location.
i. As far as possible, passwords should be easy to remember. For this purpose pass-phrase based passwords may be used. For example –
A phrase might be: "I am really happy to solve customers' issues" and the password would be: " I@rhtsc1" (NOTE: Do not use this example as your password since that would not be an intelligent choice, since this document is published to many individuals.)

RELATED DOCUMENTS

1.0 Information Security Policy
2.0 Logical Access Control Policy and Procedures