LEI SHING HONG LIMITED

PASSWORD POLICY

Version	Prepared by	Reviewed by	Approved by	Effective Date
1	Corporate MIS	Andrew Won	K.H. Kai	2014-03-03
2	Corporate IT	Kevin Yick	Kai-Uwe Seidenfuss	2020-06-22

This document contains LSH proprietary information and is supplied for internal use only. It is confidential and shall not be copied or reproduced (other than for internal use), nor disclosed to any other party, without the express permission of LSH.

Objective

The purpose of this policy is to define and establish the requirements necessary to secure access to information technology systems and resources through a proper authentication process using unique combinations of user identification (user ID) and password. A password is a string of characters used to verify the identity of the person accessing the system with the user ID during the authentication process.

Applicability

This policy applies to:

- All software, applications, computers, and data communication systems owned or otherwise operated by or for the LSH group of companies.

- All permanent or temporary staff, contractors, and consultants employed by the LSH group of companies, including those employees affiliated with third parties who access LSH information technology resources.

Responsibilities

The Business Managing Directors and the Operation/Function Heads are ultimately responsible for ensuring compliance with this policy.

All users authorized to access LSH information technology resources are expected to comply with the rules stated in this policy.

Users who willingly and deliberately violate those rules will be subject to disciplinary action up to and including termination.

Exception

Deviations from this policy require approval of the Head of Corporate IT. The deviation can be invoked in those instances where designated security measures are not legally, technically or practically viable and suitable alternative strategies are available.

Setting up Password

All computers permanently or intermittently connected to LSH information technology resources must have password access controls. Multi-user systems must employ user identifications and passwords unique to each user, as well as user privilege restriction mechanisms.

Uniqueness of Password

Computers, applications and communication systems access control must be achieved via user identifications and passwords that are unique to each individual user. Access control to files, applications, databases, computers, networks and other system resources via shared passwords (also called “group password”) is not allowed. Where no alternative solution is available, shared usage must be documented and approved by local IT manager.

Displaying Password

Where supported by system software, the display and printing of passwords must be masked, suppressed or otherwise obscured such that unauthorized parties will be unable to observe or recover them.

System Setup Guideline

Applications must not transmit passwords to the server for authentication in clear text over the network.

Applications and communication systems must not store passwords in clear text or in any easily reversible form.

Storing Password

Passwords must not be stored in computers without access control, or in other locations where unauthorized persons might discover them.

Users must not use the "Remember Password" feature of applications.

Initial Password

Where enabled by system software, the initial passwords issued to a new user by a security administrator must be valid only for the new user’s first online session. During the first session, the user must choose another password. This same process applies to the resetting of passwords in the event that a user forgets a password.

Length and Aging of Passwords

The minimum length of a password must be eight (8) characters. Where enabled by system software, users must change their passwords every ninety (90) days (see Password Standards in Appendix I).

Default Password

All vendor-supplied default passwords must be changed before any computer, application and communication systems or third party products are used for LSH business. This policy applies to passwords associated with end user identifications, as well as passwords associated with systems administrator and other privileged user identifications.

Choosing Password

Users must choose passwords that are difficult to guess. This means that passwords must NOT be related to one’s job or personal life, e.g. first name, car license plate number, relative’s name, birth date, place, etc. nor be a word in any language, slang, dialect, jargon, etc.

This also means that words found in the dictionary should not be used in order to prevent the most common password-cracking techniques based on dictionaries.

Guidelines for choosing passwords:

- String several words together (the resulting passwords are also known as “passphrases”).
- Shift a word up, down, left or right one row on the keyboard.
- Bump characters in a word, a certain number of letters up or down the alphabet.
- Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word.
- Combine punctuations or numbers with a regular word.

- Deliberately misspell a word (but not a common misspelling).
- Replace a letter with another letter, symbol or combination.

Re-Using Password

Users must not construct passwords that are identical or substantially similar to passwords they have previously used. Where enabled by systems software, users must be prevented from re-using any eight (8) previous passwords (see Password Standards in Appendix I).

Disclosing Password

Passwords must not be written down and left in a place where unauthorized persons might discover them. Apart from initial password assignment and password reset situations, the password must be immediately changed if there is reason to believe that a password is suspected of being disclosed or known to have been disclosed to someone other than the authorized user.

Regardless of circumstances, passwords must not be shared or revealed to anyone in the company or any third party except the authorized user. If users need to share computer resident data, they should use electronic mail, shared internal directories on local area network servers and other appropriate channels.

Password must not be sent to users unencrypted especially via email and must not be sent together with the user ID.

Compromising the Security of Systems

Whenever system security has been compromised, or if there is a convincing reason to believe that it has been compromised, the relevant system administrator must immediately:

- Reassign all relevant passwords, and
- Force every password on the involved system to be changed at the time of the next login.

If system software does not provide the latter capability, a broadcast message must be sent to all users requesting them to change their passwords.

An account lockout policy should be implemented, if available, to automatically lock a user account for a certain lockout period after a specified number of consecutive failed login attempts within a predetermined period of time to protect the network and/or application from intruders guessing users' passwords.

Appendix I

Password Standards

Security Settings	Current Settings
Minimum password length	8 characters
Maximum password age	90 days
Minimum password age	Allow changes immediately
Password history	8 passwords
Password complexity requirement	Enabled
Reset count age	5 minutes
Lockout threshold	5 consecutive invalid logon attempts
Lockout duration	15 minutes

Password Composition Complexity Requirement

- Password may not contain all or part of the user's account name.
- Password is not to be your name, address, date of birth, username, nickname, or any term that can easily be guessed by someone who is familiar with you.
- Password contains characters from three of the following categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphanumeric characters (exclamation point [!], dollar sign [$], pound sign [#], percent sign [%], etc.)

Password Handling

- No password (except the initial setup or password reset) are to be spoken, written, emailed, hinted at, shared or made known to anyone other than the user involved. This includes supervisors and personal assistants.
- No passwords are to be shared in order to "cover" for someone out of the office. In exceptional circumstances, the IT will create a temporary account if there are resources you need to access.
- Passwords are not to be displayed or concealed in your workspace.

Systems Involved

The LSH Password Policy applies to the passwords for the following systems with their rules:

- Network and client operating system
  Windows username and password (users will be automatically prompted at login to change the password every 90 days). This account is also used for email and VPN access.
- Other application accounts
  Software proprietary standards are applied.