# Document Control

## Versioning

|  |  |  |
| --- | --- | --- |
| Name | Date | Reason |
| Corp. Change Ctrl Officer | 11/22/2018 | Annual review |

## Applicable Parties

This document is strictly confidential and should only be distributed or viewed by the following parties:

* HAL Designated Associates
* HAL Regional Employees (Compartmented to the Division)
* HAL Management Team
* HAL Auditing Team

## Review Period

This document is subject to review by the Information Security Policy Committee (ISPC) at a minimum interval of quarterly (every 3 months) at a maximum interval of bi-annually (every 6 months).

### Previous Reviews

|  |  |  |
| --- | --- | --- |
| Committee | Review Date | Approval Date |
| ISPC | 7/15/2018 | 8/1/2018 |
| CEO | 8/21/2018 | 8/21/2018 |
| Corporate CIO | 9/23/2018 | 9/23/2018 |

# Purpose

The purpose of this policy is to provide guidance for the administration and use of passwords on all HAL corporate owned systems and networks, where corporate owned is defined as any system operating in a HAL production environment on the company network, whether within the company owned facilities or issued to company agents or employees for use at remote locations for company business.

This policy seeks to minimize systems and networks disruption introduced by poor password structure, revision and management. It is management’s intent that improved communication and coordination be used to improve the storage and use of passwords within HAL systems.

# Scope

## Applicability

This policy applies to all HAL employees and affiliates at all HAL facilities and locations world-wide.

## Ownership

This policy is under the direct control of the HAL Corporate CIO with input from the CISO and other members of management with an interest in the program.

This policy is implemented by the HAL CIO and representatives from the corporate IT division, and each HAL branch office. The CIO will appoint an *ad-hoc* committee to periodically review current password policy, and to ensure all systems are properly configured to audit password strength, use, management and system configuration.

# Policy

## General Guidelines

All passwords used on any network or system device that houses HAL data are subject to this policy. In general, all passwords should be properly formatted, periodically reset and changed, and managed in accordance with industry best practices. Passwords should be securely stored in such a manner as not to compromise the password strength or the security of HAL information assets.

## Specific Guidance

### Username Structure

All employee usernames should be formatted so as to be easily identifiable. They should be formatted to include the first initial and up to 7 characters of their last name. When the employee’s last name is less than 7 characters, a number should be assigned to pad the username to 8 characters total (e.g. twilson1, ahake001). Employees with the same initial/last name should similarly be issued usernames with numbers as needed (e.g. sjohnson, sjohnso1).

### Password Structure

Employees must use strong passwords on their accounts, changed regularly, and protected against disclosure.

All passwords to be deployed on HAL systems must be of sufficient strength as to deter brute force or social engineering attacks. Therefore:

Passwords must be:

* at least 10 characters long,
* incorporate at least one of each of these:
  + lower case letter (a-z)
  + upper case letter (A-Z)
  + numerical digit (0-9)
  + special character permitted by our system (&%$#@!).

This is referred to as the 10.4 standard.

When specifying passwords, employees should not use personal information in password such as phone numbers, social security numbers, dates of birth, pet names, names or key dates associated with family members, or employee-based information such as employee numbers.

The following guidelines, extracted from NIST SP 800-118: Guide to Enterprise Password Management, April 2009 will assist in creating strong yet easy to remember passwords.

* Mnemonic Method. A user selects a phrase and extracts a letter of each word in the phrase (e.g., the first letter or second letter of each word), adding numbers or special characters or both.
  + - Example: May the force be with you always, young Jedi

becomes Mt44bwya-yJ

(requires two fours replace the *f* in forces, to meet password format standards)

* Altered Passphrases. A user selects a phrase and alters it to form a derivation of that phrase. This method supports the creation of long, complex passwords. Passphrases can be easy to remember due to the structure of the password: it is usually easier for the human mind to comprehend and remember phrases with a coherent vocabulary than a string of random letters, numbers, and special characters.
  + - Example: *Never Give Up! Never Surrender!*  
      becomes *Nv.G.Up!-Nv.Surr1*(replacing the last exclamation mark with a *1*, to meet password format standards)
* Combining and Altering Words. A user can combine two or three unrelated words and change some of the letters to numbers or special characters.
  + - Example: Jedi Tribble   
      becomes J3d1\*Tr1bb13!

### Password Storage

The following sections provide policies and guidance on the recording and storage of passwords.

#### Employee Password Storage

Employees:

Employees must not write their passwords down. Employees may also NOT use integral OS or Web browser password support functions that automatically enter user credential in web or application fields to store HAL passwords. Employees that have been issued a HAL purchased smartphone, may request that their department purchase an approved password management application like eWallet for storing passwords. A similar application is available for use on PCs.

Employees must not store organizational passwords in non-HAL owned devices, systems and integral OS or Web browser password support functions.

#### System Password Storage

System administrators must ensure that all systems that record user passwords do so using encrypted or hashed mechanisms. Whenever possible, HAL systems should be configured to coordinate with the centralized authentication system, deployed in some HAL branches.

Branches without centralized authentication systems, should exercise additional caution in the storage of passwords files in clients and servers, to prevent capture and extraction.

#### Password Storage Logs

All HAL system administrators must ensure that all system passwords and password changes are accurately recorded and updated immediately, using the approved HAL Password Log Template, in a secure location. At the end of every business day, or on request, all administrators must print out and store the day’s system password changes in HAL branch secure password binders.

*For the purposes of the SECCDC competition, these binders are to be considered secure. However, the electronic copies of the password logs must be protected using some form of encryption to prevent unauthorized disclosure.*

Failure to record accurate system passwords in this manner WILL result in points penalties being levied against the teams. Handwritten password logs are unacceptable.

### Password Resets

All client systems must be configured to reset passwords every 180 days.

All server systems must be configured to reset passwords every 120 days.

Password history limits on all systems capable of being thusly configured, to prevent the immediate reuse of previous passwords, such that the last 2 passwords may not be reused.

Automated system resets should be enabled on all systems capable of being thusly configured, forcing users to reset their own passwords, subject to the previous policy components.

## Password Issuance

All employee must be provided with new passwords through protected channels as follows:

### Manual Password Reset

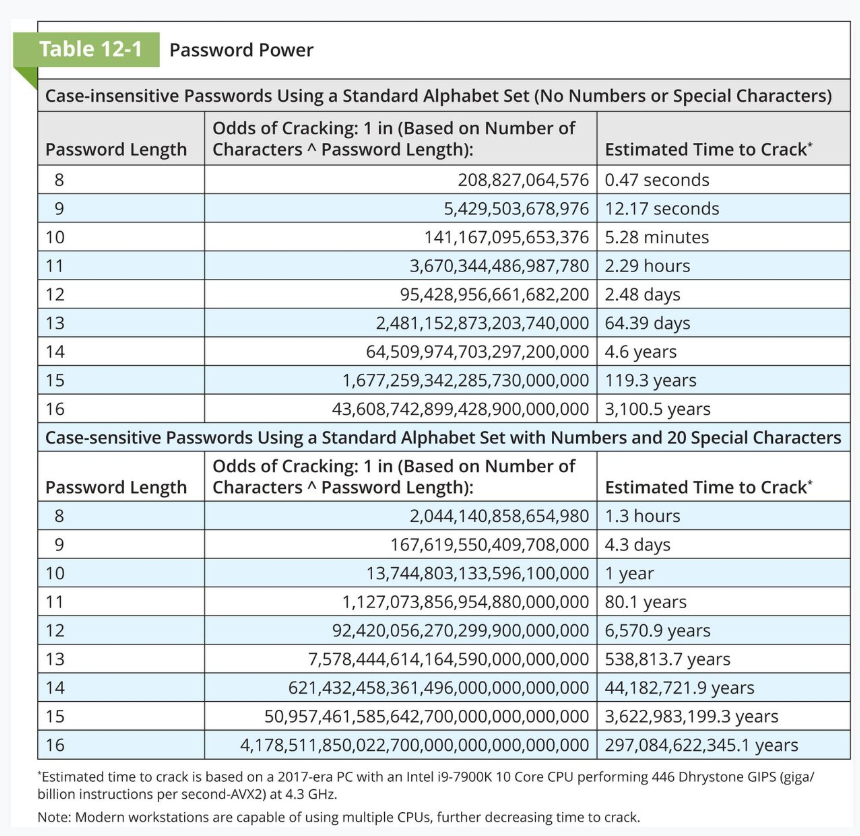
All systems using manual password resets must do so by requiring temporary passwords to be sent through HAL email. These temporary passwords must be configured so that they are only valid for no more than 4 hours, and expire upon first successful login, requiring the user to immediate reset a valid password. Password systems must log all password requests. This log must be reviewed weekly to ensure no unauthorized requests were processed.

### Automated & Scheduled Password Reset

All systems using automated and/or scheduled password resets must do so by prompting the user to change their password immediately upon the first successful login after a scheduled password change.

# Threats to Password Security

As shown in the table below (from Management of Information Security, 6th ed., Whitman & Mattord, Cengage Learning © 2019), the strength of a password determines its ability to withstand a brute force attack. By using best practice password policies like the 10.4 password rule and systems that allow case-sensitive passwords, HAL systems can be sufficiently protected against such attacks.

 (Table 12-1, Management of Information Security, Whitman & Mattord (2019), Cengage Learning.)

## Password Definitions

Brute force password attack: An attempt to guess a password by attempting every possible combination of characters and numbers that could be used.

Cracking: Attempting to reverse engineer, remove or bypass a password or other access control protection, such as the copyright protection on software. See Cracker

Dictionary password attack: A variation of the brute force password attack that attempts to narrow the range of possible passwords guessed by using a list of commonly used passwords and possibly including attempts based on the target’s personal information.

Rainbow table: a table of hash values and their corresponding plain text values that can be used to look up password values if an attacker is able to steal a system’s encrypted password file.

# Enforcement

Any employee found to be in violation this policy may be subject to disciplinary action, up to and including termination of employment.