HARRIS COMPUTER SYSTEMS

CORPORATE PASSWORD POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: 

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	08/13/15	Rick Martin	Major	Initial version of policy.	Dwayne Martin
1.1	08/16/15	Katie Rose	Minor	Updated format, minor grammatical changes.	Todd Richardson
1.2	10/22/18	Katie Rose	Minor	Annual Review	Dwayne Martin
1.3	3/25/2020 *2019 review waived as approval for 2018 review cycle completed end of Q1 2019	Katie Rose	Minor	Annual Review	Dwayne Martin
1.4	3/24/2021	Katie Rose	Minor	Annual Review; Add Definitions Document	Dwayne Martin

Harris Computer Systems
Corporate Password Policy

POLICY

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

This policy applies to all Harris Computer Systems (Harris) Users, including but not limited to Workforce Members, Contractors, subcontractors or vendors using information technology at Harris ("User" or "Users"). Access to Harris-owned computer facilities, equipment, hardware, software, printing services and technology staff-provided User support, is a privilege, not a right. Accepting access to this technology carries an associated expectation of responsible and acceptable use. When accessing any remote resources using Harris technology resources, Users are required to comply with both this policy, the Corporate Remote Access Policy and all applicable policies governing the use and access of the remote computer system.

Passwords are an important aspect of system and data security. They are the front line of protection for User accounts. A poorly chosen password may result in the compromise of Harris' entire corporate network. As such, all Users with access to Harris systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

PROCEDURE

General Password Management

1. All system-level passwords (e.g., root, enable, domain admin, application administration accounts, etc.) must be configured to use One-Time Passwords (OTP) where practical or an exception may be granted that requires the password to be changed on a quarterly basis. Exceptions to OTP must be approved by management and appropriately documented.
2. All system-level passwords (e.g., root, enable, domain admin, application administration accounts, etc.) are managed by Corporate IT.
    a. Employees with system-level access to systems that are managed by both the business unit and CIT are expected to NOT change "administrative" passwords maintained by Corporate IT.
3. All system-level passwords (e.g., root, enable, domain admin, application administration accounts, etc.) are recorded, by Corporate IT, in a secure database.
4. All user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least every 90 days.
5. Each successive password must be unique. Re-use of the previous passwords will not be allowed for a period of 1 year.
6. Passwords must be a minimum of eight (8) characters long and meet complexity requirements of using uppercase, lowercase, numbers and special characters. See the Strong Password Guidelines below.
7. User accounts that have system-level privileges granted through group

memberships or programs such as "sudo" must have a unique password from all other accounts held by that user. One Time Password (OTP) or Multi-Factor Authentication (MFA) must be enabled for those privilege accounts when possible.

8. Passwords must not be inserted into e-mail messages or other forms of electronic communication.
9. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system," and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
10. All user-level and system-level passwords must conform to the guidelines described below.
11. Passwords should never be written down or stored insecurely online.
12. When new systems or applications are brought on-line, all default (first use) passwords are changed immediately upon use.
13. Null passwords or passwords which are the same as user ID's are not allowed.
14. User accounts are disabled after three (3) invalid login attempts and reset themselves after 15 minutes or when manually reset.
15. Terminal timeouts are invoked after 15 minutes of inactivity and password protected.
16. Passwords are masked when entered and encrypted during transmission.

Management of Reset Passwords for Support Purposes

1. Prior to resetting a user's password per the user's request, the user must be authenticated by means of legitimate Harris contact such as a Teams message or direct phone call before resetting the password.

2. Prior to resetting a user's password, the user must be notified and consent to having the password reset.

3. The temporary password must meet minimum requirements outlined above.

4. The password must be different for every user.

5. The "User must change password at next logon" option must be checked prior to informing the user of the new password. This is to ensure that the user can and will change their password.

STANDARDS:

General Password Construction Guidelines

Passwords are used for various purposes at the Harris. Some of the more common uses include user-level accounts, web accounts, e-mail accounts, screen saver protection, voice-mail password and local router logins. MFA or OTP will be enabled for the various

accounts when possible and appropriate. Because MFA or OTP may not be possible for all accounts, everyone should be aware of how to select strong passwords.

1. Poor, unacceptable passwords have the following characteristics:
   - The password contains fewer than eight characters
   - The password is a word found in a dictionary (English or foreign)
   - The password is a common usage word such as:
     - Names of family, pets, friends, co-workers, fantasy characters, etc.
   - Computer terms and names, commands, sites, companies, hardware, software
   - Acronyms for the agency or city
   - Birthdays and other personal information such as addresses and phone numbers
   - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
   - Any of the above spelled backwards
   - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

2. Strong (acceptable) passwords have the following characteristics:
   - Contain both upper and lowercase characters (e.g., a-z, AZ)
   - Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";í<>?,./)
   - Are at least eight alphanumeric characters long
   - Are not a word in any language, slang, dialect, jargon, etc.
   - Are not based on personal information, names of family, etc.
   - Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W> r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

Password Protection Standards

Do not use the same password for Harris accounts as for other non-Harris access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for the various Harris access needs.

Here is a list of "don'ts":

1. Don't reveal a password over the phone to ANYONE.
2. Don't reveal a password in an e-mail message.
3. Don't talk about a password in front of others.
4. Don't hint at the format of a password (e.g., "my family name").
5. Don't reveal a password on questionnaires or security forms.
6. Don't share a password with family members.
7. Don't reveal a password to co-workers while on vacation.
8. Don't write a password in an obvious place that is accessible to others.
9. Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Harris information. If someone demands a password, refer them to this document or have

them call someone in Corporate IT.
10. Do not use the "Remember Password" feature of applications or web browsers.
11. Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer or personal device without encryption.

Also, change passwords at least once every three months. If an account or password is suspected to have been compromised, report the incident to Corporate IT and change all passwords immediately.

The Corporate IT team may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Enforcement
Any employee found to have violated this policy may be subject to disciplinary action up to and including termination.

DEFINITIONS

See attached policy definitions or click here.