1.0 Overview
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of a user’s data and ultimately lead to unauthorized access of UHD’s network and information systems. As such, all UHD employees, students (including contractors and vendors with access to UHD systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

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

3.0 Scope
The scope of this procedure 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 has access to the UHD network, or stores any non-public UHD information.

4.0 Password Procedures

4.1 General
• All production system-level passwords must be part of the Information Technology Technical Services administered global password management database.
• All users are required to change their passwords at least once every 90 days. Please note that the university’s password standards enforce password history by prohibiting the reuse of old passwords.
• Account lockouts are enforced at a minimum of 5 failed attempts and locked out for a minimum of 15 minutes.
• Administrative accounts for High risk systems will remain locked until reset by an administrator.
• 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.
• All UHD user account passwords must conform to the password standards described below.

4.2 General Password Construction Standards
Passwords are used for various purposes at UHD. Some of the more common uses include: user level accounts, web accounts, screen saver protection, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

UHD requires that all users to establish strong passwords in order to gain UHD system access. As such, the university has put in to place strengthening attributes that all passwords must possess in order to be valid.

System policies require that all new or changed passwords meet the following standards:
• include a minimum of eight (8) characters and maximum of 16 characters; and
• contain a character from at least three (3) out of the following four (4) character sets:
  o capital letter (A – Z)
  o lower case letter (a – z)
  o digit (0 - 9)
  o special character (such as !, $, #, %)
• Must NOT contain more than two (2) consecutive characters from the authorized users name (e.g., John George Doe) or User Name (e.g., DoeJ1)
Poor, weak passwords have the following characteristics:

- The password is short, alpha characters only and single case.
- 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.
  - The words "UHD", "DOWNTOWN", "HOUSTON" or any derivation.
  - 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, 2004, 2005)

### 4.3 Password Protection Standards

Do not use the same password for UHD accounts as for other non-UHD access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don’t use the same password for various UHD access needs. For example, select one password for the Engineering systems and a separate password for IT systems.

Do not share UHD passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential UHD information.

Here is a list of best practice "don’ts" for your reference:

- Don’t reveal a password over the phone to ANYONE.
- Don’t reveal a password to the boss.
- Don’t talk about a password in front of others.
- Don’t hint at the format of a password (e.g., "my family name").
- Don’t reveal a password on questionnaires or security forms.
- Don’t share a password with family members.
- Don’t reveal a password to co-workers while on vacation.
- Don’t create a password binder to store passwords.
- Don’t use the "Remember Password" feature of applications.
- Don’t store passwords in a file on ANY computer system (including mobile devices) without encryption.
- Don’t insert passwords into email messages or other forms of electronic communication.

**IMPORTANT:** UHD, or other legitimate entities (including banks, airline companies, PayPal, eBay and the IRS) WOULD NEVER request that you submit personal information such as passwords, social security numbers, birthdates, etc. by replying to an e-mail message. It is also important to avoid visiting links or opening attachments associated with any messages of this type.

If someone demands a password, refer them to this document or have them call someone in Information Technology.

If an account or password is suspected to have been compromised, report the incident to Information Technology and change all passwords.

### 5.0 Enforcement

Any employee found to have violated this procedure may be subject to suspension of their UHD network and system access and/or disciplinary actions.