POLICY TITLE: Password Policy

I. Policy Statement

All users are responsible for safeguarding their HUC-JIR login username and password credentials. Users must follow the password parameters and standards found in this policy. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this policy and procedure.

II. Purpose of Policy

The purpose of the Password Policy is to outline procedures to securely manage passwords and ensure strong authentication mechanisms for all information management systems in Hebrew Union College – Jewish Institue of Religion to support and maintain a safe and secure environment for the College-Institute's data.

III. Applicability

The Password policy applies to the following while using HUC computer equipment or accessing data through HUC software and/or systems:

All Employees of Hebrew Union College
All Contractors of Hebrew Union College
All Students / Full-time and Part-time Faculty of Hebrew Union College
All vendors / third-party / visitors
All information systems
All 3rd party applications and websites

IV. Definitions

"MFA (MULTI FACTOR AUTHENTICATION)" Multiple forms of authentication are used to confirm the credentials are from the allowed user. This reduces the risk of impersonation or the use of compromised credentials by a bad actor. The types of credentials typically fall into three categories - something you "know,' such as a PIN or a password, something you "have," such as a one-time passcode generator, token or key, and something you "are," such as fingerprint or other biometrics.

"Minimum Password Length" refers to the smallest quantity of characters a password can have to be considered valid.

"Password" is a code, which, when associated with a user account, is the first step in confirming the identity of the user and authenticaztes access to HUC Data and systems.

"Password History" refers to a user's previous passwords for the specified system.

"Security Tokens" are logical codes or physical items that must be used in conjunction with a password to successfully authenticate to a system. Examples of a security token include security keys, PIN codes to be used on smartphones; codes generated by "one-time password" device or software (usually used for multi-factor authentication).

"Users" are students, faculty, employees, consultants, vendors

"Windows Hello" is a personal, secure way to get instant access to your Windows devices using a PIN, and biometrics such as facial recognition or a fingerprint. You will need to set up a PIN as part of setting up fingerprint or facial recognition sign-in, but you can also sign in with just your PIN. These options help make it easier and safer to sign into your device because your PIN is only associated with one device, and it is backed up for recovery with your Microsoft account.

V. Procedures and Implementation

Password complexity and strength

All passwords should be at least 12 characters, including an UPPER CASE, lower case, number, and a keyboard special character. The maximum number of characters will be 32. Consider using pass phrases that only you would remember. Blank spaces are allowed in the creation of a pass phrase.

The goal is to create a well-crafted password not temporary ones that are easily hacked.

Passwords or Pass Phrases should not have personal information such as birthdates, full names, dog names, city of birth or anything that can be gleaned from the user's social media site.
Common patterns such *as QWERTY12345, your name, and PASSWORD* are not allowed.
Your password history remembers the last 5 passwords you have used. They cannot be reused.
Do not reuse the HUC password with any other account.

When do you change your password?

All system and user-level passwords should be well crafted and used until you suspect it has or might have been compromised.

If a credential is suspected of being compromised, the password in question should be changed at once, and the IT (Information Technology) team should be notified (techsupport@huc.edu)

Recommended practices for secure password management

All passwords are treated as confidential information and should not be shared with anyone. If you receive a request to share a password, report to your manager or information security team at once.

Do not write down passwords, store them in emails, electronic notes, or mobile devices, or share them over the phone.

If you must store passwords electronically, do so with a password manager that has been approved by HUC's IT Department. Currently approved password managers are: 1Password, Nord Pass, Bit Warden, and Dash Lane. Do not use the 'Remember Password' feature of applications and web browsers. Use a Password manager instead.

Avoid using the same password for multiple products or services. Do not use the HUC password for any other service or use it on multiple HUC email accounts you handle.

Multifactor Authentication (MFA) is Required

MFA (MULTI FACTOR AUTHENTICATION) supplies added protection to systems beyond password authentication. All publicly accessible systems such as a website or Microsoft Office 365 should be secured using a multifactor authentication method.

Multifactor authentication can include a password and security token/device verification, password and email verification, password and an authenticator app verification, and a password and a SMS/text code or phone call verification, among other methods. Security keys, passwordless authentication, and a "windows hello" using biometrics are allowed but require the user to notify techsupport@huc.edu for it to be used.

HUC requires 2 methods of MFA password recovery to be set up for automated password recovery to work.

MFA is not optional and must be used whenever it is available.

Password Failed Limits – Account Lockout

HUC systems are set up with limits on password attempts. The purpose of password limits is to protect against dictionary attacks or password guessing attempts by robots.

The IT department set a limit of 8 failed password attempts. After 8 failed password attempts, the user will be automatically locked out. The account lockout duration is 30 minutes.

If you need to reset your password email, click on the forgot password link on the sign in page or contact the IT helpdesk techsupport@huc.edu for support.

VI. Enforcement

The Information security team and each employee is responsible and accountable for following and enforcing password policy requirements.

VII. Policy Owner, Management and Point of Contact Information

The Director of IT manages this process. All requests for help should be sent to techsupport@huc.edu

VIII. Exclusions

There are no exclusions for the use of MFA and passwords to access HUC Data by its end users.