TABLE OF CONTENTS

Basic Password Policy

1. Overview

1.1 Purpose of Policy

Passwords are an important part of Fairleigh Dickinson University's [herein after referred to as FDU's] efforts to protect its technology systems and information assets by ensuring that only approved individuals can access these systems and assets.

FDU recognizes that passwords have serious weaknesses as an access control. For some higher-risk systems, other approved authentication methods that provide higher levels of trust and accountability may be used.

Since most of FDU's systems continue to rely on passwords alone, this policy is designed to address their weaknesses by establishing best practices for the composition, lifetime and general usage of passwords.

1.2 People Affected

All members of FDU's student, faculty and staff population as well as all contractors and temporary staff who are approved to access the University's network and systems.

1.3 People Responsible

The Chief Information Security Officer in consultation with the Data Security Incident Response Team shall be responsible for implementing, changing, enforcing and communicating this policy.

1.4 Structure of Policy

- Policy schema
- End users' responsibilities
- Help desk operators' responsibilities
- System developers' and administrators' responsibilities

1.5 Enforcement

This policy will be enforced by technical controls wherever feasible; otherwise, this policy will be enforced by line management.

All members of FDU's faculty and staff have a responsibility to promptly report any known instances of noncompliance to the CISO.

1.6 Consequences of Noncompliance

Failure to comply with this policy can result in disciplinary action as set out in FDU's Written Information Security Policy [herein after referred to as WISP].

1.7 Language

In the Responsibilities sections of this policy (3, 4 and 5), the keywords **"must," "must not," "should," "should not"** and **"may"** are to be interpreted as follows:

- **"Must"** and **"must not"** mean that compliance with the policy statement is mandatory.
- **"Should"** and **"should not"** mean that compliance with the policy statement is strongly recommended. While these recommendations are not required if technical, operational or business issues make them infeasible, supporting rationale may be requested when audit or compliance review findings cite those responsible for noncompliance.
- **"May"** means that compliance with the policy statement is recommended but optional.

2. Policy Schema

2.1 Password Confidentiality

A password can provide effective authentication if and only if it is known only to the individual user. End users will ensure the confidentiality of their passwords at all times. System developers and administrators will ensure that whenever technically possible, systems do not store passwords in clear text.

Administrative processes may necessitate temporary exceptions to this principle, but these will be kept to an absolute minimum.

2.2 Password Construction

Password length and complexity requirements provide resistance to common kinds of attacks. Because of technology constraints, password construction rules may vary from one system to another, but they will meet (or exceed) these requirements wherever possible.

FDU recognizes that long and complex passwords may be difficult for users to remember, and thus, this policy provides guidance to end users on how to construct a memorable password that meets (or exceeds) these requirements.

2.2.1 Password Construction Rules

A password will be made up of:

- Eight (8) or more characters
- At least one uppercase letter
- At least one lowercase letter
- At least one digit (0 through 9)
- At least one special character ($, @, # and so on)

A password will not include a single instance of a dictionary word.

Note: The above rule is enforceable only on some systems.

A password will not include:

- The user's user ID or email address
- The name of a group the user account belongs to

A password should not contain anything that is meaningful to the user, such as a name (either real or fictional), a date (such as family birthdays and anniversaries), telephone numbers, postal codes and car registration numbers.

Note: The above is not enforceable on any system.

2.3 Password Change and Reuse

Users will be forced to change their passwords periodically in order to minimize the window of opportunity for an attacker who has discovered a user's password.

A user's new password will be completely different from any recently used password.

A user will be free to choose a new password at any time. However, performing multiple changes in quick succession to enable continued use of a recently used password will be prohibited.

2.3.1 Password Change and Reuse Rules

A user will change his or her password every 84-90 days depending on the system.

- Datatel/Ellucian password life is set at 84 days
- Alpha password life is set at 84 days
- Windows Desktop/Office365/NetID password life is set at 90 days
- Others not specifically identified shall be 90 days

Note: The above rule may not be enforceable on all systems.

A user's password will be different from his or her previous (X) passwords as follows:

- Datatel/Ellucian: 5
- Alpha: 5
- Windows Desktop/Office 365 and NetID: 10
- Others not specifically identified shall be 10

Note: The above rule is only enforceable on some systems.

2.4 Password Entry

Whenever technically possible, the password field in a login panel will be configured to mask the password entered by a user to minimize the risk of opportunistic observation by another.

A system will allow multiple successive login attempts ("grace logins"). If the password is not correct on the last allowed attempt, the user's account will be suspended, and the user will have to contact the University Technical Assistance Center (UTAC) and open a ticket to resume the account and, if necessary, reset the password.

2.4.1 Password Entry Rules

A system will allow between 5 and 10 failed login attempts as noted below:

- Datale/Ellucian: 5
- Alpha: 5
- Windows Desktop/Office 365/NetID: 10
- Others not specifically identified shall be 10

Note: This rule is enforceable on only some systems.

2.5 Password Storage

Whenever technically possible, a system will not hold passwords in clear text; it will use an approved irreversible cryptographic transform to protect its users' passwords.

A system that stores users' passwords for other systems, and brokers those passwords to those systems on behalf of the user, will use an approved (reversible) encryption algorithm.

3. End Users' Responsibilities

If you are an end user of FDU's systems, you have the following responsibilities regarding the password you use on any of FDU's systems. (See 1.7 Language section for the meanings of the terms in **bold** type.)

These responsibilities apply even if the system does not enforce any specified rules:

a) You **must** keep your password confidential at all times.

b) You **must not** disclose your password to anyone, including FDU's management and technical support staff, even if they demand it.

c) *If this happens, you **must** escalate to the CISO immediately.* You **should not** use any password that you use on any FDU systems on any external system (including Internet banking and social networking services).

d) You **should not** write down your password.

e) You **should not** use the "remember password" feature in any Web browser.

f) You **must only** use a "password keeper" or "password wallet" software or service that has been approved by policy or otherwise in writing by the CISO.

g) You **must** choose a password that meets or exceeds the length and complexity requirements set out in 2.2.1 Password Construction Rules section.

   *This is your responsibility even if these rules are not enforced by a particular system. Sometimes, technical restrictions on a system do not allow you to choose a password that meets these requirements. Such systems are enumerated in Schedule **[X],** along with the password construction rules that apply.*

h) You **should** choose a password that meets or exceeds the other requirements set out in 2.2.1 Password Construction Rules section.

   *A help desk operator, system administrator or other user should never ask you to choose a password that doesn't meet requirements (g) and (h). If this happens, you **must** escalate to the CISO immediately.*

   Further, if any help desk operator asks you to change your password on a portal that does not use an HTTPS website with an SSL lock, you should escalate to the CISO immediately.

The following rules, (i) to (l), are enforced on most systems. If the rules are not enforced by the system, you are still expected to comply.

i) You **must** change your password at least every 90 days.

   There is no need to access a rarely used system just to change an old password. Most systems will automatically expire the password after 90 days, and you will be prompted to change the password when you next log in.

j) You **should not** use any of your previous six (5) passwords.

k) You **should** choose a new password that has no more than four (4) characters in a row in common with your current password.

For example, if your password is "anTelope1," a new password of "anTelope2" is not acceptable, but "anTecede1" is.

l) You **should not** change your password more than twice in any three (3) days.

Tips for Choosing a Good Password (Advisory)

The length and complexity requirements may appear to make it hard to choose a password that is easy to remember, but it can be pretty straightforward to do so.

A password that meets the minimum length requirement must be rather complex. You can readily construct such a password from the initial letters of a favorite quotation, song lyric, poem and so on, capitalizing some letters, and substituting a number or special character in an appropriate place.

For example:

- Ww1dwysm — What would I do without your smart mouth?
- Itwbtd2A — In the week before their departure to Arrakis.

A "very long" password can be relatively simpler. Choose three simple words, capitalizing some letters, and link them with a number or special character.

For example:

- gorilla8banana@SanDiego

4. Help Desk Operators' Responsibilities

If you are an FDU IT technician or a system administrator providing support normally done by the help desk, you have the following responsibilities regarding users' passwords on any of FDU's systems that you support. (See 1.7 Language section for the meanings of the terms in **bold** type.)

a) When a user asks you to reset his or her password, you **must** corroborate the user's claimed identity in line with approved procedures in Appendix A.

b) You **must not** disclose a user's new password to anyone other than the user himself or herself.

c) You **must not** write down a user's new password.

d) You **must not** send any new password to a user electronically.

e) You **must not** ask any user to tell you his or her password.

5. System Developers' and Administrators' Responsibilities

If you are a system developer or system administrator, you have the following responsibilities regarding the passwords used on any of FDU's systems that you own, develop or maintain. (See 1.7 Language section for the meanings of the terms in **bold** type.)

If compliance with (a), (c), (g), (h), (i), (j) or (k) is not technically feasible because of system constraints, contact the CISO to agree on and document the exception.

a) You **must** configure each system to require that any user's password meets the length and complexity requirements set out in 2.2.1 Password Construction Rules section.

b) You **should** configure each system to require that any user's password meets as many of the other requirements set out in 2.2.1 Password Construction Rules section as are technically feasible.

c) You **must** configure each system to force a user to change his or her password every 90 days.

d) You **should** configure each system to prohibit a user from using any of his or her previous five (5) passwords.

e) You **should** configure each system to prohibit a user from choosing a new password that has more than four (4) characters in a row in common with his or her current password.

f) You **should** configure each system to prohibit a user from changing his or her password more than twice in any three (3) days.

g) You **must** configure the password field in a login panel to mask the password entered by a user to minimize the risk of opportunistic observation by another.

h) You **must** configure each system to allow 5 successive login attempts ("grace logins"). If the password is not correct on the 5th attempt, the system must suspend the user's account such that the user will have to contact an administrator to resume the account and, if necessary, reset the password.

i) Passwords must be implemented in the strongest form the system supports and supports the intended business function. You should implement a cryptographic transform to protect the passwords of the users on each system

5.1 Requirements for Third-Party Systems

All **mandatory** requirements noted in this section (that is, those denoted by **"must"** or **"must not"**) constitute part of the minimum security specification for third-party system software that FDU acquires and implements. That is, it is essential that system software enables system developers and administrators to fulfill these responsibilities.

> *If a third-party system cannot meet the minimum security specification, contact the CISO to agree on and document the exception.*

All **optional** requirements noted in this section (that is, those denoted by **"should"** or **"should not"**) constitute desirable features of third-party system software.