QUANTA

IT COMPLIANCE DEPARTMENT

Password Security Standard

For Enterprise-Wide Use

Standard No.: ITC – STD – S1000

Version 1.6

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OBJECTIVE

The objective of the Password Security Standard is to define the enterprise-wide minimum format and functional requirements for authorized access to Quanta network-based information and applications.

The minimum requirements documented in this standard may be exceeded as required.

1.2 SCOPE

This standard applies to all information owners, information custodians, employees, and authorized third party users of Quanta network information and applications.

An authorized user is defined as an employee, consultant, contractor, business partner or other third party who has been granted access to Quanta information. Although Quanta customers are authorized users of their own personal information, any information security requirements relevant to Quanta customers are called out separately from other authorized user requirements. If Quanta customers are not called out explicitly, the requirements defined within this standard are to be considered out of scope for Quanta customers.

This standard applies to applications, custom or commercial, that process, handle, or transmit Quanta information in any form. This includes but is not limited to:

- Operating Systems
- Databases
- Applications
- Cloud Service Providers (CSPs)

All administrators and managers responsible for the implementation, configuration and maintenance of Quanta information and applications shall follow the requirements documented in this standard. Refer to the following section, for more information on Operating system password standards:

- Appendix A: Microsoft 2003, 08, 12 – Account Configuration Settings
- Appendix B: AS/400 (OS/400) – Account Configuration Settings
- Appendix C: UNIX (IBM AIX) – Account Configuration Settings
- Appendix D: LINUX (Oracle Red Hat) – Account Configuration Settings

1.3 DETECTIVE AND REACTIVE CONTROLS

Detective and reactive controls shall be used to measure the effectiveness of controls defined within this standard. The scope, frequency and implementation method of these

detective and reactive controls shall be based on risk and can be domain-specific or enterprise-wide.

1.4 STANDARDS

This standard will be consistent with industry accepted and recognized best practices outlined in ISO 27001, NIST 800, SANS 20, CIS 20, and other industry recognized and accepted best practices.

1.5 COMPLIANCE

- Mandatory: All OpUs shall adhere to these standards as of the effective date.
- Minimum Requirements: These standards represent minimum requirements with which all applications shall comply. OpUs may, within reason and if deemed appropriate in Local OpU Management's judgment, implement standards that are more restrictive than the Quanta Standards.
- IT Framework: Local OpU IT Framework must be amended, as necessary, to assure that the documented Framework, including any associated documents, e.g., PISUP, are consistent and aligned with these standards

1.6 NON-CONFORMANCE

Applications that cannot adhere to these standards must be assessed and shall require the residual risks to be accepted by the applicable business owner or custodian in accordance with the IT Risk Assessment and Exception Process.

1.7 OWNERSHIP AND REVIEW

- This standard is owned by the IT Compliance department
- This standard shall be reviewed on a yearly basis.
- Changes to this standard shall be in accordance with the Quanta Policy and Standard Management Process

2. PASSWORD REQUIREMENTS

2.1 AUTHENTICATION

At a minimum, all accounts shall require a password for authentication. The use of dual-factor authentication meets and exceeds the password requirements included within this section.

2.1.1 PASSWORD COMPLEXITY

- Passwords shall consist of a minimum of twelve (12) characters for Windows based operating systems and Cloud Service Providers (CSPs) that will collect, transmit, store or host data or applications containing unconsolidated or pre-release financials, Personally Identifiable Information (PII), Electronic Protected Health Information (ePHI), financial/SOX, banking or customer information, sensitive business information, Trade Secret / Patented / Copyright protected information, customer data, etc. For others, passwords shall consist of a minimum of eight (8) characters.
- Passwords shall contain characters from three of the following four categories:
    - Uppercase characters (A - Z)
    - Lowercase character (a – z)
    - Numbers (0 – 9)
    - Non-alphanumeric characters (e.g.,!, $, #, %)
- Passwords shall not be easily guessable
- Easily guessable passwords are defined as poor, weak passwords that are comprised of commonly used or well-known words, phrases, and patterns.

2.1.2 ACCOUNT LOCKOUT

- Accounts shall be automatically locked after sixteen (16) consecutive unsuccessful failed logon attempts for windows devices and eight (8) consecutive unsuccessful logon attempts for other platforms.
- Administrative accounts: The locked out administrative account must be manually re-enabled by an authorized administrator.
- User accounts: Until it is manually re-enabled by an authorized administrator.

2.1.3 PASSWORD EXPIRATION

- At a minimum, passwords shall expire every 90 days and will be required to be changed

2.1.4 PASSWORD HISTORY

- Users shall not be permitted to reuse any of the previous twenty-four (24) for Windows based operating system. For others, password retention history shall be twelve (12).

2.1.5 PASSWORD RESETS

- A user's identity shall be verified before their password is reset
- Reset and newly assigned passwords shall be required to be changed by the user upon first use
- This may be implemented via technical or procedural controls

2.1.6 PASSWORD RESETS – MANUAL CHANGE

- Passwords for applications that cannot be automatically changed will be sent in a "confidential" manner to the user
- Notification of manual password changes will be sent to the user prior to the password expiration
- A user's identity shall be verified before their manually changed password is sent
- This may be implemented via technical or procedural controls

2.1.7 PASSWORD ENCRYPTION

- Stored passwords shall be encrypted or hashed where stored at all times
- Encryptions algorithms shall include the use of salt values, where technically feasible

2.1.8 MULTI-FACTOR (MFA) AUTHENTICATION

- When connecting remotely to the network, users shall do so using multi-factor authentication through approved means (Microsoft Authenticator, token, etc.)
- Network administrator accounts for administration activities must be carried out using MFA.
- End users connecting to Quanta Office 365 (or email and OneDrive) tenant for email

2.1.9 ACCOUNTABILITY

- Users shall be uniquely identified
- Individual user accounts and passwords shall not be shared
- Service accounts, help-desk type accounts, and hot logon accounts may be shared if appropriate controls are in place

2.1.10 ACCOUNT AND APPLICATION ACCESS REVIEW

- A complete review of all user accounts and application access shall be conducted, and unnecessary accounts and application access disabled or removed, on a minimum of a semi-annual basis
- This is in addition to any on-going operational procedures that look for and remove unnecessary accounts

2.1.11 DEFAULT (VENDOR-SUPPLIED) ACCOUNTS

- Default (vendor-supplied) accounts shall be disabled or removed
- If default accounts these accounts cannot be disabled or removed for business or technical reasons, the password shall be changed to conform to the authentication requirements in section 2.1.1

2.1.12 ANONYMOUS ACCOUNTS

- Anonymous accounts shall be disabled or removed
- For the purpose of this standard, an anonymous account is an account which has no corresponding authentication credentials, e.g. GUEST, ANONYMOUS.

APPENDIX A: MICROSOFT 2003, 08, 12, 16 – ACCOUNTS CONFIGURATION SETTINGS

Password Parameter Setting	Quanta Standard	Disclose To Users?	Rationale for Standard
1. Maximum Age (Days)	90	Yes	Generally Accepted Standard.
2. Minimum Age (Days)	0	No	To discourage Users from repeatedly changing their Password to quickly cycle through Retained History to get back to the same (desired) Password. If there becomes a known Security Threat to the User's Login Account, then the User may contact a System Administrator to have their Password "reset".
3. Minimum Length	12	Yes	Generally Accepted Standard.
4. Retained History (Prior Instances)	24	No	System "Remembers" the User's twenty-four (24) previous Passwords so that they may not be re-used.
5. Must meet Complexity Requirements?	Yes (Enabled)	Yes	Password must contain at least one character from at least three of the following four categories: - English Uppercase Characters (A-Z) - English Lowercase Characters (a-z) - Numeric Digits (0 - 9) - Non-Alpha-Numeric (! $, #, or %)
6. Store Passwords using Reverse-Encryption?	No (Disabled)	Yes	A User's Password should be known only to the User. Reverse Encryption would enable the User's existing Password to become known to System Administrators, which potentially undermines the User's 100% Accountability for all activity that occurs under their Login Account.
7. Account Lockout Threshold (# of Unsuccessful	16	Yes	Generally Accepted Standard. A System / Application Administrator would have to be contacted to "Reset" the User's Password. This setting was realigned from 8 to 16 in light of vendor guidance on acceptable controls.

Password Parameter Setting	Quanta Standard	Disclose To Users?	Rationale for Standard
8. Account Lockout Duration (Minutes)	0-forever	Yes	If the User becomes Locked Out, a System / Application Administrator would have to be contacted to “Reset" the User's Password. In this way, an Administrator could quickly become aware of potential intrusion attempts, thus eliminating the requirement of "Logging Failed Login Attempts" and then having to periodically review such Logs.
9. Reset Lockout Counter (Minutes)	360 minutes	No	This is the Maximum Setting Value that may be associated with this Parameter. 60 MPH x 24 HPD=1,440 MPD. Therefore, 99,999 Minutes=Approximately 69 Days. This Counter Controls the minimum duration between Successful Logins that the Account Lockout Threshold (Item-7 above) is maintained in protecting against Invalid Login Attempts.

APPENDIX B: AS/400 (OS/400) – ACCOUNT CONFIGURATION SETTINGS

Password Parameter Setting	Quanta Standard	Disclose To Users?	Rationale for Standard
1. Sign-On Lockout Action (QMAXSGNACN)	Setting 2 (Locks Out User ID Only)	No ,	Generally Accepted Standard. With the given parameter setting, the User's Sign- On ID is "Locked" until released by a SysAdmin, e.g., when the Maximum Invalid Sign-On Attempts is exceeded, or the Inactive Session Timeout interval is exceeded.
2. Maximum Invalid Sign-On Attempts (QMAXSIGN)	8	Yes	Generally Accepted Standard.
3. Required Difference in Passwords (QPWDRQDDIF)	4	No	Number of previous passwords checked for duplicated passwords. A value of 4 means the system will not allow 12 previous passwords. .
4. Maximum Age (Days) (QPWDEXPITV)	90	Yes	Generally Accepted Standard.
5. Minimum Age (Hours) (QPWDCHGBLK)	0	Yes	The number of hours a user must wait after the last successful password change operation before the user can change the password again.

AS/400 (OS/400) Account Configuration Setting must meet the above criteria. In addition, Operating units must comply with **either Option A or Option B** for AS/440 (OS/400) Password Standards (See below). **Option A** is more suitable for OpUs who want their users to use AD passwords for AS400 authentication.

OPTION A: AS/400 (OS/400) – ACCOUNT CONFIGURATION SETTINGS

1. Password Rules (QPWDRULES)	MINLEN 8 MAXLEN 8 or more REQANY3 LMTPRFNAME	Yes	Generally Accepted Standard. Consistent with QCO AD Password Standard.

IF OPU HAS ADOPTED OPTION A THEN OPTION B IS NOT APPLICABLE

OPTION B: AS/400 (OS/400) – ACCOUNT CONFIGURATION SETTINGS

1. Limit Adjacent Digits in Password (QPWDLMTAJC)	1	Yes	Generally Accepted Standard.
2. Limit Characters in Password (QPWDLMTCHR)	None	No	
3. Limit Repeating Characters in Password (QPWDLMTREP)	2	Yes	Generally Accepted Standard.
4. Maximum Length (QPWDMAXLEN)	8 or more	Yes	Maximum length of the password.
5. Minimum Length (QPWDMINLEN)	8	Yes	Minimum length of the password. Generally Accepted Standard.

APPENDIX C: UNIX (IBM AIX) – ACCOUNT CONFIGURATION SETTINGS

Password Parameter Setting	Quanta Standard	Disclose to Users?	Rationale for Standard
1. Invalid Login Attempts (loginretries)	8	Yes	Generally Accepted Standard.
2. Retained History (Prior Passwords) (histsize)	12	No	System "Remembers" the recently used instances used of the User's Password so that they may not be re-used
3. Minimum Age (Weeks) (minage)	0	No	Enough days, e.g., one calendar week, to discourage Users from repeatedly changing their Password to quickly cycle through Retained History to get back to a recently used Password. If there is a known security threat to the User's account, then the User may contact a System Administrator to have their Password "reset".
4. Maximum Age (Weeks) (maxage)	13	Yes	Generally Accepted Standard. 13 Weeks x 7 DPW= 90 Days
5. Alpha Characters Required (minalpha)	1	Yes	Generally Accepted Standard.
6. Other Characters Required (minother)	1	Yes	Generally Accepted Standard.
7. Minimum Length (minlen)	8	Yes	Generally Accepted Standard.
8. Maximum Repeating Characters (maxrepeats)	2	Yes	Generally Accepted Standard.
9. Inactive Session Timeout (seconds) (TMOUT=n)	1800	Yes	Generally Accepted Standard. OpU may allow more time to any non-interactive accounts (e.g., service accounts) to run long reports and other processes.

APPENDIX D: LINUX (Oracle Red Hat) – ACCOUNT CONFIGURATION SETTINGS

Password Parameter Setting	Quanta Standard	Disclose to Users?	Rationale for Standard
1. Invalid Login Attempts (fail_lock_count) (pam_policy::settings::fail_lock_count)	8	Yes	Generally Accepted Standard.
2. Retained History (Prior Passwords) (password_history) (pam_policy::settings::password_history)	24	No	System "Remembers" the recently used instances used of the User's Password so that they may not be re-used
3. Minimum Age (pass_min_days) (shadowpwd_pass_min_days)	0	No	Mitigated by Password Retained History
4. Maximum Age (pass_max_days) (shadowpwd_pass max_days)	90	Yes	Generally Accepted Standard.
5. Alpha Characters Required (pw_quality_minimum_digits) (pam_policy::settings::pw_quality_minimum_digits)	1	Yes	Generally Accepted Standard.
6. Lowercase Characters Required (pw_quality_minimum_lower) (pam_policy::settings::pw_quality_minimum_lower)	1	Yes	Generally Accepted Standard.

Password Parameter Setting	**Quanta Standard**	**Disclose to Users?**	**Rationale for Standard**
7. Uppercase Characters Required (pw_quality_minimum_upper) (pam_policy::settings::pw_quality_minimum_upper)	1	Yes	Generally Accepted Standard.
8. Other Characters Required (pw_quality_minimum_other) (pam_policy::settings::pw_quality_minimum_other)	1	Yes	Generally Accepted Standard.
9. Minimum Length (pw_quality_minlen) (pam_policy::settings::pw_quality_minlen)	12	Yes	Generally Accepted Standard.