DENTONS

IT Policy

IT Password and Authentication Standard

Contents

1 Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of the Firm's information assets by establishing secure standards for passwords, and ensuring user awareness about the importance of secure password management.

2 Summary

Passwords are an important aspect of IT security. The first step towards securing a midsize business network is to understand what vulnerabilities an attacker is likely to exploit. The primary task of an attacker who has infiltrated a network is to initiate escalation of privileges, which is how an attacker attempts to gain more access from the established foothold that they have created. After an escalation of privileges has occurred, there is little left to stop an intruder from effectively escalating their abilities in pursuit of the compromise goals. Attackers can use many different mechanisms to achieve an escalation of privileges, but primarily they involve compromising existing accounts and account passwords, especially those with administrator-equivalent privileges.

All too often, users and services are granted access to greater privileges than necessary for reasons of convenience. Although this approach guarantees users have access to the resources they need to do their jobs, it also increases the risk of a successful attack.

3 Scope

This policy applies to all IT personnel and systems within the Firm's environment. The accounts and passwords referred to in this document are applicable (but not limited to) operating system programs, databases, voicemail accounts, and local or online applications.

4 Policy

4.1 Authentication

- Authentication credentials, such as identifiers IDs and passwords must not be:
  - shared
  - written down or stored in readable form
  - stored in clear text such as automatic login scripts, software, source code, macros, terminal function keys, in computers without access control, shortcuts, or in other locations where unauthorized persons might discover them
- Authentication data (e.g., passwords) must be stored in a cryptographically-hashed format
- Authentication data transmitted to any system must be encrypted
- Establishing trust through use of IP address or DNS name (whitelisting) as an authenticating credential is unacceptable. Windows Systems
  - The following standards apply to unattended systems and domain controllers that require trust:
    - Only systems controlled by the Firm can be granted trust relationships with existing Firm-controlled/owned systems
    - The more trusted system must initiate communication with the less trusted system
    - Windows domain controllers at the Firm should not trust non-Firm domain controllers
- Multi-Factor Authentication

    - Multi-Factor authentication solutions must be approved by the IT Security team prior to deployment
    - Multiple single-factor authentications must not be used in place of multi-factor authentication
    - Multi-Factor authentication solutions must be deployed for direct access to Firm systems from untrusted environments

4.2 Account Privileges

- Domain user accounts must be set with only the permissions required. We operate a principle of "Least Privilege" to carry out the task.
- Account lockouts are required. This will limit the likelihood of compromise due to brute force attack methodologies.
- If the service will run on multiple systems, or interacts with other domain systems (as in the case of backup), a domain user account must be used.
- Domain accounts tied to individual employees must never be used to run a service.
- Account rights and privileges must be granted through group membership and not through direct rights assignment to user accounts.
- Accounts must have owners defined and assigned with the name of the person whom is responsible for the account usage. Generic and/or shared accounts are prohibited.
- Accounts are considered inactive after 90 days of inactivity and will be disabled. Accounts will be reviewed and monitored regularly to identify inactive accounts[1]

4.3 Account types and usage

- Administrative accounts
    - Administrative accounts must only be used for system management tasks which require elevated access above the standard user account. They must not be utilised for standard user activities.
- Domain Administrators
    - This is a special case which relates to Active Directory administrative accounts. The use of Domain Administration privilege must be kept to a minimum number of employees. Passwords must be changed in line with the User Policy.
    - Privilege escalation monitoring is in place to prevent unapproved assignment of domain administrator rights.
    - Creating or updating accounts to escalate privileges to the administrator level requires multi-level approval by *at least* one IT Manager AND IT Director or CIO. All requests and approvals for privileged access are tracked in the Firm's request tracking system.
- Service accounts
    - Service accounts must follow the same password complexity as domain administrative accounts.
    - Service accounts must not be used for Interactive (User) Logon. It is permissible to set passwords to not expire on service accounts. Service accounts will have additional monitoring that should be aware of the potential of an unauthorized login attempt on the account.
    - If an employee with knowledge of the service account credentials leaves the firm, the password needs to be reset.
    - User accounts must not be used to run services on IT systems.
- Training accounts

    - The number of training accounts must be kept to a minimum. Passwords on the training accounts must be changed after each training session. If remote training will be provided, multi-factor authentication must be used.
    - Training accounts must not be used for activities other than participation in training.

4.4 General Password Guidelines

- All members of the firm are under obligation to adhere to the following for user and administrative accounts:
    - All user-level accounts, including accounts with administrative privileges, must be uniquely identified. Interactive shared, group, or generic user/administrator accounts are strictly prohibited.
    - Strong passwords are required and enforced according to industry standards and any applicable regulatory compliance requirements.
    - Appropriate account timeout, password expiration, and password history must be required and enforced according to industry standards and any applicable regulatory compliance requirements. Current settings are:
        - Maximum password age (Password expiration): 90 days
        - Minimum password age: 1 day
        - Minimum password length: 8 characters
        - Password history: 5 passwords remembered
        - Account lockout threshold: 5 invalid login attempts
        - Account lockout duration timeout: 1 hour
        - Reset account lockout counter: 30 minutes
    - Passwords should never be stored or transmitted in clear text.
    - All vendors/default accounts and passwords must be changed according to the password standards set forth in this document prior to production deployment.
    - All IT users who are also administrators must have separate user and administrator accounts. Administrator accounts should only be used to carry out administrative tasks.
    - Remote access and access to secured data shall require a multi-factor of authentication over and above the user ID/password.
    - A randomly generated, unique, temporary password that meets the minimum password complexity requirement must be assigned for each new account and for each password reset.
    - Temporary passwords must be changed upon first use.
    - If there is a suspicion that ANY password has been compromised, notify IT immediately and have the password reset as soon as possible.
    - Users should apply the same principles to any web-based sites that are not maintained by the firm.
- All members of the IT department are under obligation to adhere to the following:
    - Different appliances and / or devices must have different passwords.
    - Passwords must be reset following the departure of staff that is privy to the account details.
    - All user-level accounts, including accounts with administrative privileges, must be uniquely identified. Interactive shared, group, or generic user/administrator accounts are strictly prohibited.
    - All accounts must be centrally managed when possible.
    - Accounts must be clearly marked with an owner and appropriate description.
    - All production passwords must be part of the firm password management database.

  - All vendors/default accounts and passwords must be changed according to the password standards set forth in this document prior to production deployment.
  - All IT users who are also administrators must have a separate user and administrator accounts. Administrator accounts must only be used to carry out Administrator tasks.
  - Accounts thought to be compromised must be reported to your manager immediately then change the password. Staff must then initiate an information security event investigation in accordance with the appropriate policy.
  - Remote access and access to secured data shall require a multi-factor of authentication over and above the user ID/Password.
  - A randomly generated unique temporary password that meets the minimum password complexity requirement must be assigned for each new account and for each password reset.
  - Password reset requests must be logged and follow approved identity validation procedures.
  - Any temporary passwords must be changed upon first use.
- Prohibited Activities:
  - Do not use passwords based on:
    - Words found in a dictionary (English or foreign)
    - Passwords based on a common usage word such as names of family, pets, friends, co-workers, fantasy characters, company, places, etc.
    - Personal information such as birthdays, addresses, phone numbers, and social security numbers
    - Word or number patterns like aaabbb, QWERTY, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards or any of the above preceded or followed by a digit (e.g., secret1, 1secret)
  - Do not:
    - Transmit a password in an email message
    - Reveal a password on questionnaires or security forms
    - Reveal a password electronically or verbally to anyone. IT will provide appropriate guidance for password exchange for support purposes.
    - Use the "Remember Password" feature of applications (such as email clients and web browsers)
    - Write passwords down and store them anywhere in your office
    - Store passwords in a file without applying security/encryption
    - Use the same password for firm accounts as for other non-firm access (e.g., personal ISP account, etc.)
  - Do not misuse your own or other user’s password to elevate system privileges or to access information that you do not need to know.
  - Please refer to the firm Code of Conduct for more information regarding passwords and access to user accounts.

4.5 Password Complexity

- All account types
  - Passwords must contain characters from three (3) of the following categories where full keyboard functionality is available:
    - Upper-case characters of European languages (A to Z, with diacritic marks, Greek or Cyrillic characters)
    - Lowercase characters of European languages (A to Z, sharp-s, with diacritic marks, Greek or Cyrillic characters)
    - Base-10 digits (0 to 9)

        - Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
        - Any Unicode character that is categorised as an alphabetic character but is not uppercase or lowercase (includes Unicode characters from Asian languages)
- IT Administrators
    - Passwords must be at least ten (10) characters long for IT system accounts. Where possible, use a password generator to ensure complexity is set.
    - Passwords or passphrases must contain characters from three (3) of the following categories:
        - Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
        - Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
        - Base-10 digits (0 through 9)
        - Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
        - Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase (including Unicode characters from Asian languages)

4.6 Passwords and Passphrase Guidelines

We recommend the use of passphrases, which can heighten the security of our systems.

What to do	**Example**
Start with a sentence or two.	Complex passwords are safer!
Remove the spaces between the words in the sentence.	Complexpasswordsaresafer!
Turn words into shorthand or intentionally misspell a word.	ComplekspasswordsRsafer!
Add length with numbers. Put numbers that are meaningful to you after the sentence.	ComplekspasswordsRsafer!2011

Some guidance is given as to what makes a password or passphrase strong.

A strong password:	**A strong passphrase:**

• Is at least eight characters long • Does not contain your user name, real name, or company name • Does not contain a complete word • Is significantly different from previous passwords	• Is 20 to 30 characters long • Is a series of words that create a phrase • Does not contain common phrases found in literature or music • Does not contain your user name, real name, or company name • Is significantly different from previous passwords or passphrases (e.g., do not simply add a 1 at the end of a previous password)

5 Definitions

Administrative account - Although there is a default Administrator account created on any new installation of Microsoft Windows or Active Directory domain, the term administrator account is often used in a general sense to describe any account that has been granted administrator level privileges. This document will make distinctions between the two for the sake of clarity.

Limited account - A limited account is any account that is not a member of any administrative group and that does not have any elevated privileges that are equal to that of a local or domain administrator account. Typically, a limited account would be a member of the Domain Users group or the local Users group.

Principle of least privilege - The Department of Defence Trusted Computer System Evaluation Criteria, (DOD-5200.28-STD), or Orange Book, is an accepted standard for computer security. This publication defines least privilege as a principle that "requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use."

Services - Services are executable and run at start up or can be triggered by other events or scheduled instances. Services often run in the background without much user prompting or interaction.

Service accounts - Simply put, a service account is often described as any account that does not correspond to an actual person. These are often built-in accounts that services use to access resources they need to perform their activities. However, some services require actual user accounts to perform certain functions, and many businesses still employ the practice of using domain accounts to run services as well.

6 Violations and Enforcement

Any person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Non-compliance with or breach of this policy will be reported to the violator’s immediate manager and/or appropriate Firm management.

7 Exceptions

Exceptions to this policy must be requested via email to the IT Security Team & the Office of the General Counsel. Requests must include:

- clear business justification for the exception
- duration of exception request
- any appropriate details regarding compensating controls or information that reduces the risk of the exception.

Exceptions, approved or denied, will be logged in our IT ticket tracking system for follow up and/or control purposes as appropriate.

Appendix 1 Document control

Ownership and responsibility

Document Owner	IS Security Team
Author	Fishnet / Michele Gossmeyer
Contact for amendments	IS Security Team

Amendment History

Date Issued	Issued by	Reason for Change
2-June-2017	Michele Gossmeyer	Annual IT Security team review. Updated with password enforcement details
31-Aug-2017	Dave Beck	Updated to reflect multi-level approval for privilege escalation
18-Dec-2017	IT Security Team	Updated with reset requirements
31-Oct-2018	IT Security Team	Annual IT Security team review cycle
2-Oct-2019	IT Security Team	Annual IT Security team review - added inactive acct piece

Distribution List

This document has been issued to the following people for information (I) and / or review (R):

Name	Position	I / R
Eddie Reich	US General Counsel	R

Related Documentation

Reference	Doc Reference
User Password Policy and Authentication Standard	83670388

Approval

Name	Role	Date	Comments
Michele Gossmeyer	Director, Information Governance & Compliance	9-Nov-2016	Separated from End user password policy to eliminate elevated/escalated privilege language (inapplicable) for standard users. Also reduces risk of broader exposure of our IT pwd policy to non-IT users.
Michele Gossmeyer	Director, Information Governance & Compliance	2-June-2017	
Michele Gossmeyer	Director, Information Governance & Compliance	31-Aug-2017	
Michele Gossmeyer	Director, Information Governance & Compliance	18-Dec-2017	

Michele Gossmeyer	Global Director, Information Governance, Risk & Compliance	9-Jan-2019	
Michele Gossmeyer	Global Director, Information Governance, Risk & Compliance	6-Feb-2020	