Dunder Mifflin Password Policy

Effective Date: September 22, 2023

1) **Purpose**:

The purpose of this Password Policy is to establish guidelines and best practices for creating, managing, and protecting passwords within Dunder Mifflin.

2) **Policy Scope:**

This policy applies to all employees, contractors, and any other personnel who have access to Dunder Mifflin systems, networks, and data. It covers the creation, use, and management of passwords across all company-related accounts and services.

3) **Password Creation:**

Passwords must be a minimum of 12 characters in length.
Passwords should include a combination of the following elements:
Uppercase letters
Lowercase letters
Numbers
Special characters (e.g., !, @, #, $, %,+)
Avoid using easily guessable information, such as names, birthdays, or other dictionary words
Do not use the company name
Passwords should be unique and not reused across different systems or accounts

4) **Password Management:**

Passwords must be kept confidential and not shared with anyone, including supervisors, coworkers, or IT employees.
Do not write down passwords or store them in easily accessible locations.
Passwords should not be inserted into email messages, or any other form of electronic communication, nor revealed over the phone to anyone.
Utilize company-approved password management tools and avoid saving passwords in web browsers.

5) **Password Changes:**

Passwords must be changed at least every 120 days.
If you suspect that your password has been compromised, report the incident immediately to IT and change all affected passwords.

6) **Account Lockout and Failed Login Attempts:**

After 3 consecutive failed login attempts, user accounts will be temporarily locked to prevent unauthorized access.
Contact IT support for assistance in unlocking accounts.

7) **Secure Storage of Passwords:**

Passwords should be securely stored in authorized password managers.
Passwords should not be included in system documentation, scripts, or configuration files.

8) **Non-Compliance:**

Failure to comply with this Password Policy may result in disciplinary action, including but not limited to warnings, suspension, or termination of employment or contractual agreement.

9) **Policy Review:**

This Password Policy will be reviewed periodically to ensure its effectiveness and relevance. Any updates or revisions will be communicated to all relevant employees.

For questions or concerns related to this policy, please contact Sneha Irukuvajjula (sneha.irukuvajjula@dundermifflin.com)

Dunder Mifflin
Boulder, CO
09/22/2023