# Dunder-Mifflin Password & Protection Policy

## 1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to **Dunder-Mifflin** systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

## 2. Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords and the protection of those passwords.

## 3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any **Dunder-Mifflin** facility, has access to the **Dunder-Mifflin** network, or stores any non-public **Dunder-Mifflin** information.

## 4. Policy

### 4.1 **Password Creation**

4.1.1 All new passwords must be contrived at a minimum of 2 digits, 2 uppercase letters, 1 special character/symbol, and a minimum of 10 characters.

4.1.2 All user-level and system-level passwords must conform to the Password Construction Guidelines.

4.1.3 Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.

4.1.4 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommend that some form of multi-factor authentication is used for any privileged accounts

### 4.2 **Password Change**

4.2.1 Passwords should be changed only when there is reason to believe a password has been compromised.

4.2.2 Password cracking or guessing may be performed on a periodic or random basis by the Security Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

### 4.3 **Password Protection**

4.3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential **Dunder-Mifflin** information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

4.3.2 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.

4.3.3 Passwords may be stored only in “password managers” authorized by the organization.

4.3.4 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.5 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

### 4.4 **Multi-Factor Authentication**

4.4.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

## 5. Policy Compliance

### 5.1 **Compliance Measurement**

The Security Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### 5.2 **Exceptions**

Any exception to the policy must be approved by the Security Team in advance.

### 5.3 **Non-Compliance**

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

**Email to Jim**

**To:** Jim Halpert
**From:** Mark Davis
**Subject:** Admin access for servers

Hey Jim,

In response to your request for full administration access to all the servers, we are unable to fulfill your request at this time. We just implemented a new password and protection policy here at Dunder-Mifflin to protect company resources. Major points for this new policy:

Passwords:

Must NOT be shared with anyone, including supervisors, coworkers, family, etc.

Must NOT be in any form of communications such as email, text, over the phone, etc.

May be stored in company approved ‘password managers’ but nowhere else.

-Do NOT use any ‘remember password’ options such as in web browsers

Will be checked randomly to ensure compliance.

Must be changed if thought to be compromised and reported as well.

Will need to follow the new criteria for creating a strong password from the following:

-using passphrases,upper/lower case, numbers, special characters, etc.

-no common dictionary words or common sequences like ‘123’ should be used.

Thank you for your understanding and for your compliance.

Best regards,
Mark Davis
IT System Admin
Dunder-Mifflin

**Handling email requests**

Added new file in /etc/sudoers.d/01_corp_D-H_config on each machine

-containing all the commands and hosts and users I'll need

Meredith's request on machineC:

added entry into the new file via an alias

-FTP_ADMIN FTP=(root) FTP_RESTART

added new group & them to it to be able to edit those files & changed permissions

-groupadd ftpadmin && usermod -aG ftpadmin mpalmer

-chgrp ftpadmin /var/ftp/ -R && chmod 775 /var/ftp/ -R

Pam's request on machineB:

added entry for her, kelly, and andy via alias

-WEB_ADMIN WEB=(root) HTTP_RESTART

added new group and them to it to be able to edit those files & changed permissions

-groupadd webadmin && usermod -aG webadmin pbeesly && usermod -aG webadmin abernard && usermod -aG webadmin kkapoor

-chgrp webadmin /var/www/dundermifflin/ -R && chmod 775 /var/www/dundermifflin/ -R

System admin entries added as well

-mdavis ALL=(root) ALL (ME)

-dschrute ALL=(root) ALL (DWIGHT)

Michaels shutdown/cancel request:

added entry to shutdown system with parsing up to 10000 & cancel it using custom aliases

-mscott ALL=(root) CANCEL,SHUTDOWN

**Pam tools and files**

-added entry for pam_access.so in /etc/pam.d/login, /etc/pam.d/sshd on each machine

-added entries to /etc/security/access.conf on each machine

+:root:ALL, +:mdavis:ALL, +:dschrute:ALL, +:mscott:ALL

+:pbeesly@machineb.dundermifflin.com:ALL

+:kkapoor@machineb.dundermifflin.com:ALL

+:abernard@machineb.dundermifflin.com:ALL

+:mpalmer@machinec.dundermifflin.com:ALL

+:ALL@machinee.dundermifflin.com:ALL

-changed pwquality.conf to ensure new passwords conform to policy

-minlen = 11, dcredit = -2, ucredit = -2, ocredit = -1, minclass = 3

-change default umask created by /etc/profile need rwxrwx--- or 770

-then umask 007

logged into machines as users and tested many functionalities.