Password Protection Policy

1. **Overview**
   Passwords are extremely important to Dunder Mifflin and computer security. All employees or contractors that are employed by Dunder Mifflin are responsible for taking the appropriate steps as outlined below.
2. **Purpose**
   The purpose for this document is to establish a standard for creating a very strong password at Dunder Mifflin.
3. **Scope**
   The scope of this policy includes all personnel who have an account here at Dunder Mifflin.
4. **Policy**
   - 4.1 Password Creation
     - 4.1.1 All users must create a unique password for each of their managed accounts or machines.
     - 4.1.2 All passwords must be >16 characters long, have at least 1 uppercase letter, number, and special symbol.
     - 4.1.3 Passwords must be changed quarterly for those who have higher privileged access.
   - 4.2 Password Change
     - 4.2.1 If a password has been compromised, it must be changed within 7 days or account access will be lost.
   - 4.3 Password Protection
     - 4.3.1 Do not share your password with anyone, including your coworkers. All passwords are confidential information of Dunder Mifflin.
     - 4.3.2 Passwords should not be inserted into any type of messaging application, this includes but not limited to: email, direct messages, company phone text messaging.
   - 4.4 Multi Factor Authentication
     - 4.4.1 Multi-factor authentication at Dunder Mifflin is a requirement for work related accounts and is highly recommended for personal accounts.
5. **Policy Compliance**
   - 5.1 Compliance Measurement
     - 5.1.1 The infosec team will be monitoring your compliance through multiple methods of surveillance.
   - 5.2 Exceptions and Non-compliance
     - 5.2.1 Any exceptions must be approved by the infosec team. Also any non-compliance of this policy will result in immediate termination.