

2025 Password Policy Checklist for Businesses



Managed IT | Co-Managed IT | Cybersecurity







2025 Password Policy Checklist for Businesses

info@andersontech.com | andersontech.com | 314.394.3001 | © 2025 Anderson Technologies



Creating Your Password Policy

Follow these simple checklists to guide you through creating and rolling out a comprehensive password policy for your business.




1. Define Password Creation Guidelines

-  **Minimum length** (12 characters recommended).
-  **Mix of uppercase and lowercase letters, numbers, and special characters.**
-  **Avoid easily guessable information** (e.g., names, dates).
-  **Prohibit common words and phrases.**

2. Establish Password Storage Rules



-  **Encourage the use of secure password managers.**
-  **Discourage writing passwords down or storing them in unsecured digital files.**

3. Set a Password Change Frequency



-  **Require immediate password changes in the case of a suspected breach.**
-  **Enforce password updates at a set cadence via IT (if available).**
-  **If IT cannot enforce monitoring, request an annual password update.**





4. Configure locking mechanisms to protect accounts

-  Lock accounts after a certain number of failed login attempts.
-  Set a lockout duration or require manual account unlocking by an administrator.

5. Require Two-Factor Authentication (2FA)

-  Enable 2FA for sensitive systems and data access.
-  Configure the option to automatically clear browser sessions on exit to prevent session jacking.

6. Develop an Employee Training Program



-  Educate employees on password policy rules and best practices.
-  Provide resources and training materials to support password management.





Rolling Out Your Password Policy



1. Communicate the Policy to All Employees



-  Announce the new policy via email, meetings, or internal communication channels.
-  Explain the importance of strong password practices for company security.

2. Provide Training and Support

-  Offer training sessions or workshops on creating and managing passwords.
-  Make resources available for employees to reference (e.g., guides, videos).

Password



3. Enforce the Policy Using Technology

-  Implement password managers and 2FA systems to support policy adherence.
-  Use IT tools to monitor and enforce password change frequency.







4. Regularly Review and Update the Policy

-  Assess the effectiveness of your password policy over time.
-  Update the policy as needed to address evolving cybersecurity threats.

5. Consider Partnering with IT Experts

-  Consult with IT professionals, like Anderson Technologies' cybersecurity team, for guidance in developing and implementing your password policy.
-  Stay informed on best practices and emerging cybersecurity risks.

Defend Your Data

By following these checklists, you can create a robust password policy that will help protect your business from unauthorized access and data breaches. Regularly review and update your policy to ensure it remains effective against the ever-evolving cybersecurity landscape.



**ANDERSON
TECHNOLOGIES**

Password Policy Checklist for Businesses

info@andersontech.com | andersontech.com

| 314.394.3001 | © 2025 Anderson Technologies