San Bernardino County Superintendent of Schools
Policy 4012.5

ORGANIZATIONAL PASSWORD POLICY

Passwords remain a critical element of our cybersecurity posture. To safeguard SBCSS data, systems, and networks, all certificated and classified staff, contractors, and vendors with access to SBCSS technology resources must follow the guidelines outlined in this policy. Weak or reused passwords, as well as unattended devices, can lead to unauthorized access and compromise our organization's security.

This policy defines standards for creating and protecting strong passwords, outlines requirements for multi-factor authentication (MFA), and sets expectations for managing authentication securely across all SBCSS-connected systems.

This policy applies to all individuals who access SBCSS systems, networks, or applications, whether onsite or remote, including certificated and classified staff, contractors, and vendors.

Users should have no expectation of privacy when using SBCSS-provided systems or networks. All activity on SBCSS networks may be logged and monitored and may be reviewed in response to operational needs, audits, or legal requirements.

Account Requirements

- Multi-Factor Authentication (MFA) is mandatory for all accounts using SBCSS-managed Microsoft identity platform or any system containing confidential or sensitive data.
- All applications and services must authenticate through SBCSS-managed Microsoft identity platform. If integration is not possible, the system owner must work with Technology Services to implement equivalent or enhanced protections.
- SBCSS devices with privileged access to the network will lock and require the user to put in their password after 15 minutes of inactivity
- Any account that has not been logged into in 180 days will automatically be disabled. Users will need to contact Technology Services to re-enable the account.

Password Requirements

- Always use different passwords for SBCSS accounts from other non-SBCSS access (e.g., personal email, banking, social media, etc.).
- Do not share your personal SBCSS password with anyone, including administrative assistants or secretaries, supervisors, or Technology Services. All passwords are to be treated as sensitive, confidential SBCSS information.
- SBCSS enforces a deny list of commonly used, weak, or previously compromised passwords to prevent vulnerable selections.

- Minimum password length: For MFA protected accounts 8 character minimum password length. For non-MFA enabled accounts a 14 character minimum password length
- Password complexity rules are not enforced for MFA accounts. For non-MFA accounts, at least one number or special character is required.

- Passwords are not required to be reset on a schedule. If there is a known or suspected compromise of an account, the password will be reset immediately.
- Users cannot reuse any of their last 5 passwords.

Compromised Passwords

If a user/account password or a computing device is compromised or suspected of being compromised, the employee **MUST** immediately notify the Technology Services Department of the incident.

Enforcement

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

Approved: August 14, 2014

Revised: July 8, 2025