

Michael Scott Paper Company

Cybersecurity Authentication Policy


Revised January 2024

Purpose

Michael Scott Paper Company's Cybersecurity Authentication Policy aims to establish a secure, standardized, and rigorous process to protect the integrity, confidentiality, and availability of the corporation's digital assets. By defining stringent authentication and access control measures, this policy aims to safeguard the organization from potential cyber threats, unauthorized access, data breaches, and other security incidents that could jeopardize our business continuity, compromise sensitive data, harm our reputation, or potentially lead to regulatory penalties. Ultimately, the policy will serve as a guideline to create a robust cybersecurity culture, promoting awareness, adherence, and understanding across all levels of the organization, thereby fostering a secure digital environment that supports our corporate objectives.

Scope

The scope of this Cybersecurity Authentication Policy extends to all individuals who access and use the corporation's digital resources, including employees, contractors, consultants, interns, and third-party entities with access privileges. The policy governs all systems, networks, devices, and data owned, operated, or controlled by the corporation, whether located on-premises, in the cloud, or on mobile platforms. It encompasses every aspect of user authentication, including password creation and management, multi-factor authentication, biometric identification, and cryptographic controls. The policy is applicable across all locations and situations where corporate data is accessed, including remote work scenarios and during travel, thereby providing an all-encompassing umbrella of protection for the corporation's digital assets.



Policy Statements

1. **User Authentication:** All users must provide valid credentials to access the corporation's digital assets. Authentication procedures must include at least two factors of identification, one of which must be a strong, unique password.
2. **Password Management:** Passwords must be at least twelve characters long, comprising a mix of uppercase and lowercase letters, numbers, and special characters. They should not include easily guessed information such as personal details or common words. Passwords must be changed every 90 days and cannot be reused within a cycle of five password changes.
3. **Multi-Factor Authentication (MFA):** MFA must be enabled on all accounts wherever possible, requiring at least two independent ways of proving user identities, such as something the user knows (password), something the user has (smart card, mobile device), or something the user is (biometric verification).
4. **Password Updates and Reuse:** Users must change their passwords every 90 days. Reusing previous passwords or using the same password across multiple systems is strictly prohibited.
5. **Biometric Authentication:** Where available and appropriate, users should employ biometric authentication methods, such as fingerprint recognition or facial recognition, as an additional layer of security.
6. **Secure Storage of Authentication Information:** No user shall store passwords or other authentication credentials in an insecure manner, such as written notes, unprotected files, or non-encrypted digital storage.
7. **Sharing of Credentials:** Users must never share their credentials with others, including colleagues, friends, or family. Any necessary password sharing for system administration purposes must be done through secure methods approved by the IT department.
8. **Cryptographic Controls:** Where data is sensitive or highly valued, additional cryptographic measures should be implemented, such as digital signatures, data encryption, or public key infrastructure.
9. **User Access Privileges:** Access to information and system functionality must be granted based on the principle of least privilege and role-based access control. Users should be given only those essential privileges to perform their work.
10. **Account Management:** Accounts must be disabled immediately upon terminating a user's employment or contractual relationship. Regular audits should be performed to identify and disable dormant accounts and unnecessary access privileges.
11. **Reporting Suspicious Activities:** Any suspected compromise of a user's authentication credentials must be immediately reported to the IT department.
12. **User Training:** All users must complete cybersecurity training annually, including current best practices for authentication.

Sanctions

Failure to comply with the Cybersecurity Authentication Policy may result in disciplinary action, which will be administered in accordance with the corporation's Human Resources procedures. This can range from formal warnings and mandatory cybersecurity training to temporary suspension of access privileges and, in severe cases, termination of employment or contractual relationship. Additionally, individuals may be subject to prosecution for any illegal activities under applicable local, state, national, or international laws. This is to underscore the critical nature of cybersecurity and everyone's role in maintaining the safety and integrity of our corporate digital assets. Sanctions will be enforced impartially and consistently to all parties covered by the policy, with severity proportional to the extent of the policy violation.

Definitions

Authentication: the process of verifying the identity of a user, device, or system that attempts to access the corporation's digital assets. This is typically achieved by presenting evidence, or credentials, that prove an entity is what or whom it claims to be. These credentials can be something the user knows (like a password), something the user has (like a smart card or mobile device), or something the user is (like a biometric trait).

Integrity: the guarantee that data remains unaltered and consistent from creation to retrieval unless modified by an authorized entity. It safeguards the accuracy and trustworthiness of information by preventing unauthorized alteration and ensuring data, systems, and networks function correctly and reliably.

Confidentiality: the principle of ensuring that information is accessible only to those authorized to view it. It involves implementing measures to protect data from unauthorized disclosure or theft, thereby maintaining the privacy and secrecy of sensitive information.

Availability: ensures authorized users have reliable and timely access to information and resources when needed. It safeguards systems, networks, and data from disruptions due to technical failures, malicious attacks, or natural disasters, thereby maintaining consistent operational performance.

Access Control: the process of granting or denying specific privileges to individuals, systems, or entities to access certain data or resources. It's a critical security measure designed to prevent unauthorized access, ensuring only approved entities can interact with sensitive information based on their role, responsibility, or a specific set of criteria.