CYBERATOS
SMART STRATEGY
STRONG SECURITY

"Sample" Access Control Policy

and Supporting Procedures

The following document, provided by Cyberatos, is a sample Access Control Cybersecurity Policy developed for the fictitious retail entity, StyleTrendz. StyleTrendz, for the purpose of this example, operates as a mid-sized online and brick-and-mortar retailer specializing in contemporary fashion. Due to its handling of customer personal data, payment information, and inventory management systems, StyleTrendz faces a range of cybersecurity risks that necessitate a robust access control framework.

This sample policy is intended to serve as a template for Chief Information Security Officers (CISOs) and Information Security Officers (ISOs) in the development of their organization's specific policies. However, it is imperative to note that this document necessitates substantial customization to reflect each organization's distinct operational requirements, regulatory obligations, and security framework.

Direct implementation of this sample without thorough adaptation is strongly discouraged. We advise reviewing our comprehensive guide on cybersecurity policy development, available on our blog, for further assistance in tailoring policies to your organization's unique needs. Consultation with legal and security professionals is recommended.

STYLETRENDZ ACCESS CONTROL POLICY

AND SUPPORTING PROCEDURES

INTRODUCTION

This document outlines StyleTrendz's approach to managing access to its information assets. It is designed to ensure that only authorized individuals and systems can access, use, and manage StyleTrendz's data and resources, thereby protecting their confidentiality, integrity, and availability. This policy is aligned with ISO/IEC 27001:2022 standards. It also addresses gaps and vulnerabilities identified in StyleTrendz's systems.

PURPOSE

The purpose of this policy is to:

- Define the rules for granting, modifying, and revoking access to StyleTrendz's information assets.
- Protect StyleTrendz's information from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Ensure compliance with relevant legal, regulatory, and contractual requirements, including PCI DSS, GDPR, and CCPA.
- Support StyleTrendz's business objectives by enabling secure and efficient access to information for authorized users.
- Mitigate identified vulnerabilities, including the lack of strong authentication and inadequate access controls, and address the risks they pose.

SCOPE

This policy applies to all StyleTrendz employees, contractors, vendors, and any other third parties who access StyleTrendz's information assets, including:

- All computer systems, networks, and devices (including company-owned and BYOD were permitted).
- All software applications and databases, including POS systems and e-commerce platforms.
- All electronic and physical records, including customer data and transaction logs.
- All company premises and facilities, including retail stores, warehouses, and offices.
- All information, regardless of format (electronic, paper, verbal).

DEFINITIONS

- **Information Asset:** Any data, system, device, or resource that has value to StyleTrendz.
- **Access:** The ability or opportunity to read, write, modify, execute, or otherwise use an information asset.
- **User:** Any individual or system that accesses StyleTrendz's information assets.
- **Authorization:** The process of granting access rights to a user.
- **Authentication:** The process of verifying the identity of a user.
- **Multi-Factor Authentication (MFA):** An authentication method that requires a user to provide two or more verification factors to gain access to a resource.
- **Least Privilege:** The principle of granting users only the minimum access rights necessary to perform their job duties.
- **Need-to-Know:** The principle of granting access to information only to those users who require it to perform their job duties.

POLICY STATEMENTS

1. **Access Control Principles:**

   1.1 Access to StyleTrendz's information assets shall be based on the principles of least privilege and need-to-know. (ISO 27002:2022 - 5.15, 8.3)
   1.2 Users shall be granted access only to the information assets required to perform their job duties.
   1.3 Access rights shall be clearly defined, documented, and regularly reviewed. (ISO 27002:2022 - 5.18)
   1.4 Strong authentication methods, including multi-factor authentication, shall be used to verify user identities. (ISO 27002:2022 - 5.17, 8.5) This is a critical requirement to address the identified lack of strong authentication.
   1.5 Multi-Factor Authentication (MFA) is required for all access to:
   - Systems containing sensitive customer data (e.g., payment information, personal details).
   - Privileged accounts (e.g., system administrators, database administrators).
   - Remote access to StyleTrendz's network.
   - All financial systems.
   - All POS systems.
   - All cloud-based applications.

   1.6 Access to sensitive information, such as customer payment data and personal information, shall be strictly controlled and monitored.
   1.7 Temporary access may be granted for specific business needs, with appropriate justification and approval.
   1.8 Access rights shall be revoked promptly upon termination of employment or change in job duties. (ISO 27002:2022 - 5.18)
   1.9 Users are responsible for protecting their login credentials and shall not share them with others.

1.10 Bypass of access controls , including MFA, is prohibited.
1.11 Inactive user accounts will be disabled after 30 days of inactivity.

2. User Access Management:

2.1 A formal process shall be established for requesting, approving, granting, and revoking user access to information assets. This process is detailed in the **User Access Provisioning Procedure.** (ISO 27002:2022 - 5.16)
2.2 Each user shall have a unique identifier (User ID) for accessing systems.
2.3 Access requests shall be documented and approved by the appropriate data owner or system administrator.
2.4 User access rights shall be reviewed and re-certified at least annually. (ISO 27002:2022 - 5.18)
2.5 System administrators are responsible for the correct implementation of access rights.
2.6 Regular audits of user access will be conducted to ensure compliance with the principle of least privilege.

3. Password Management:

3.1 Users shall be required to create strong passwords that meet the following minimum requirements: (ISO 27002:2022 - 5.17)
- At least 12 characters in length.
- A combination of uppercase and lowercase letters, numbers, and symbols.
- Not easily guessable (e.g., dictionary words, personal information).
- Passwords must be changed regularly (at least every 90 days).
- Password history must be enforced.

3.2 Multi-factor authentication (MFA) shall be implemented for all systems, especially those containing sensitive information, including POS systems, e-commerce platforms, and customer databases. (ISO 27002:2022 - 5.17, 8.5) This is a direct response to the identified vulnerability.
3.3 Users shall not store passwords in plain text or share them with others.
3.4 The management of passwords shall be carried out as described in the **Password Management Procedure**.

4. Multi-Factor Authentication (MFA)

4.1 Multi-Factor Authentication (MFA) is mandatory for all employees, contractors, and third-party users accessing the following:

- Point-of-Sale (POS) systems.
- E-commerce platform administrative interfaces.
- Customer databases and any system containing Personally Identifiable Information (PII).
- Financial systems and applications.
- Remote access to the StyleTrendz network.
- Administrative accounts with elevated privileges.
- Employee email accounts.

4.2 StyleTrendz supports the following MFA methods:

- One-time codes generated by an authenticator app on a smartphone.
- Time-based One-Time Password (TOTP) tokens.
- Biometric authentication (where supported by the device and approved by IT).
- Push notifications to registered mobile devices.

4.3 All users will be required to enroll in MFA upon initial account setup.
4.4 Users must register at least two approved MFA methods for account recovery purposes.
4.5 MFA should be enabled on all devices used to access the resources listed in section 4.1.
4.6 Failure to enroll in and use MFA when accessing required systems may result in restricted access or account suspension.

5. **System and Application Access Control:**

5.1 Access to systems and applications shall be controlled based on user roles and responsibilities. (ISO 27002:2022 - 5.15, 8.3)
5.2 System and application access control mechanisms shall be implemented to enforce the principles of least privilege and need-to-know.
5.3 Default passwords for systems and applications shall be changed immediately upon installation.
5.4 Access to system administration functions shall be restricted to authorized personnel only. (ISO 27002:2022 - 8.2)
5.5 Remote access to StyleTrendz's systems shall be secured using strong authentication and encryption and shall be strictly controlled and monitored. (ISO 27002:2022 - 8.20), MFA is required for all remote access.
5.6 Access to POS systems shall be strictly controlled, with unique login credentials for each employee and regular audits of POS activity logs, and MFA where technically feasible. This addresses the risk of POS compromises.
5.7 System and application access shall be managed according to the **System and Application Access Control Procedure**.

6. **Network Access Control:**

6.1 Access to StyleTrendz's networks shall be controlled to prevent unauthorized access. (ISO 27002:2022 - 8.20)
6.2 Network access control mechanisms, such as firewalls, intrusion detection/prevention systems, and network segmentation, shall be implemented. (ISO 27002:2022 - 8.20, 8.22)
6.3 Wireless network access shall be secured using strong encryption and authentication methods. (ISO 27002:2022 - 8.20). MFA should be considered for wireless access where feasible.
6.4 Guest network access shall be segregated from the corporate network.
6.5 Access to network devices shall be restricted to authorized personnel only. (ISO 27002:2022 - 8.2). MFA is required for access to network devices.
6.6 Network access shall be managed according to **the Network Access Control Procedure**.

7. **Remote Access**

7.1 All remote access to StyleTrendz's network and resources must comply with the StyleTrendz **Remote Access Policy**.
7.2 MFA is mandatory for all remote connections to the StyleTrendz network.
7.3 Remote access must be established through secure methods, such as Virtual Private Networks (VPNs).

8. **Physical Access Control:**

8.1 Physical access to StyleTrendz's facilities and areas containing sensitive information shall be controlled to prevent unauthorized access. (ISO 27002:2022 - 7.2, 7.3)
8.2 Physical access control mechanisms, such as door locks, access cards, and surveillance systems, shall be implemented. (ISO 27002:2022 - 7.2, 7.4)
8.3 Visitors shall be required to register and be escorted while on StyleTrendz's premises. (ISO 27002:2022 - 7.2)
8.4 Access to server rooms and data centers shall be restricted to authorized personnel only, shall be logged, and should utilize MFA where possible.
8.5 Physical access shall be managed according to **the Physical Access Control Procedure**.

9. **Access Control for Mobile Devices:**

9.1 This applies to both company-owned and personal devices used to access StyleTrendz information.
9.2 Strong authentication, such as biometric authentication or a strong passcode is required. (ISO 27002:2022 - 5.17, 8.1)
9.3 Devices must be encrypted. (ISO 27002:2022 - 8.1)
9.4 Devices must have up-to-date security software, including anti-malware and mobile device management (MDM) where applicable.
9.5 Remote wipe capability must be enabled.
9.6 Access to sensitive company data on personal devices will be strictly controlled and may be prohibited.
9.7 MFA is required to access sensitive company data on mobile devices.
9.8 Mobile device access shall be managed according to the **Mobile Device Access Control Procedure**.

10. **Review of User Access Rights:**

10.1 User access rights shall be reviewed (ISO 27002:2022 - 5.18):

- At least annually.
- When job roles change.
- Upon termination of employment.
- When there are changes in the systems

10.2 The review shall ensure that users have the appropriate level of access based on the principles of least privilege and need-to-know.
10.3 Access reviews shall be documented, and any necessary changes to access rights shall be implemented promptly, as detailed in the **Access Rights Review Procedure**.

11. **Addressing Identified Vulnerabilities and Threats**

11.1 The lack of strong authentication, as identified in our assessment, is addressed by the mandatory implementation of multi-factor authentication (MFA) for all systems, especially those handling sensitive data, privileged accounts, and remote access.

11.2 The risk of unauthorized access to POS systems is mitigated by the requirement for unique login credentials for each employee and regular audits of POS activity logs.

11.3 The policy mandates regular review of user access rights to prevent privilege creep and ensure adherence to the principle of least privilege.

11.4 All systems, especially those accessible remotely, must use strong authentication and encryption.

RESPONSIBILITIES

- **Cybersecurity Steering Committee:** Oversees the implementation and enforcement of this policy.
- **Chief Information Security Officer (CISO):** Develops, implements, and maintains this policy.
- **Data Owners:** Determine access requirements for their respective data.
- **System Administrators:** Implement and enforce access controls on their systems.
- **Managers:** Ensure that their employees comply with this policy.
- **All Users:** Comply with this policy and protect their access credentials.

COMPLIANCE

- Violation of this policy may result in disciplinary action, up to and including termination of employment, as well as potential legal consequences.

EXCEPTIONS

- Any exceptions to this policy must be approved in advance by the CISO and the Cybersecurity Steering Committee.

POLICY REVIEW

- This policy shall be reviewed and updated at least annually or when significant changes occur to StyleTrendz's business operations, the threat landscape, or identified vulnerabilities.

REQUIRED PROCEDURES

- The following procedures are required to support the implementation of this policy:
    - User Access Provisioning Procedure

- User Account Management Procedure
- Password Management Procedure
- Access Rights Review Procedure
- System and Application Access Control Procedure
- Network Access Control Procedure
- Physical Access Control Procedure
- Mobile Device Access Control Procedure
- Incident Reporting Procedure
- Compliance Monitoring Procedure

ANNEX A: USER ACCESS PROVISIONING PROCEDURE

This procedure outlines the process for requesting, approving, granting, modifying, and revoking user access to StyleTrendz's information assets.

1 **Access Request:**

1.1 A formal access request form (electronic or paper) shall be used to request access to StyleTrendz's information assets.

1.2 The form shall include:

- User's name, employee ID, and job title.
- The specific information assets or systems to which access is requested.
- The type of access required (e.g., read-only, read-write).
- The business justification for the requested access.
- The requester's manager's approval.

1.3 For new employees, access requests shall be initiated as part of the onboarding process.

2 Access Approval:

2.1 All access requests shall be reviewed and approved by the appropriate data owner or system administrator, in accordance with the principle of least privilege.

2.2 Approval workflows shall be defined and documented, specifying the roles and responsibilities involved.

2.3 For sensitive information or systems, a higher level of approval (e.g., department head, CISO) may be required.

2.4 Approved access requests shall be documented and retained for audit purposes.

3 Access Granting:

3.1 System administrators shall grant access rights based on the approved access request.

3.2 Access rights shall be assigned using appropriate access control mechanisms (e.g., user accounts, roles, permissions).

3.3 The granting of access rights shall be documented, including the date, time, and the individual who granted access.

3.4 Users shall be notified when their access rights have been granted and provided with any necessary login credentials or access instructions.

4 Access Modification:

4.1 Requests for changes to existing access rights (e.g., adding or removing access) shall follow the same process as new access requests.

4.2 Changes in job roles or responsibilities shall trigger a review of access rights.

4.3 Access modifications shall be documented and approved.

5 Access Revocation:

5.1 Access rights shall be revoked promptly upon termination of employment, transfer to a different department, or change in job duties.

5.2 Managers are responsible for notifying the IT department or system administrators of any changes that require access revocation.

5.3 A formal offboarding process shall include procedures for revoking access to all relevant systems and information assets.

5.4 Revocation of access rights shall be documented.

6 Temporary Access:

6.1 Temporary access for vendors, contractors, or other third parties shall be granted only for a specified period and for a specific purpose.

6.2 Temporary access requests shall be clearly documented, justified, and approved by the appropriate data owner or system administrator.

6.3 Temporary access shall be automatically revoked upon the expiration of the specified period.

7 Emergency Access

7.1 In emergency situations, access may need to be granted quickly, bypassing the standard procedure.

7.2 A process for emergency access must be defined, documented, and approved by the CISO.

7.3 All emergency access must be logged and reviewed as soon as possible after the emergency.

ANNEX B: USER ACCOUNT MANAGEMENT PROCEDURE

This procedure outlines the process for managing user accounts on StyleTrendz's systems and applications.

1 **Unique User Identification:**
   - 1.1 All users shall be assigned a unique identifier (User ID) for accessing StyleTrendz's systems and applications.
   - 1.2 Generic or shared accounts shall be prohibited, except in exceptional circumstances with explicit approval from the CISO.

2 **Account Creation:**
   - 2.1 User accounts shall be created using a standardized naming convention.
   - 2.2 The creation of user accounts shall be documented, including the user's name, job title, department, and assigned access rights.

3 **Account Maintenance:**
   - 3.1 User account information (e.g., name, department) shall be kept up-to-date.
   - 3.2 Changes to user account information shall be documented and approved.

4 **Account Deactivation/Deletion:**
   - 4.1 User accounts shall be deactivated or deleted when access rights are revoked.
   - 4.2 Deactivated accounts shall be retained for a specified period (e.g., 90 days) before deletion, to allow for account reinstatement if necessary.
   - 4.3 The deactivation or deletion of user accounts shall be documented.

5 **Account Monitoring**
   - 5.1 User accounts should be regularly monitored for suspicious activity
   - 5.2 Any suspicious activity should be investigated.

ANNEX C: PASSWORD MANAGEMENT PROCEDURE

This procedure outlines the requirements and guidelines for managing passwords on StyleTrendz's systems and applications.

1 **Password Creation:**
   1.1 Users shall be required to create strong passwords that meet the requirements outlined in the **Access Control Policy**.
   1.2 New users shall be prompted to change their default password upon initial login.
   1.3 Users shall be provided with guidance on creating strong passwords.

2 Password Changes:
   2.1 Users shall be required to change their passwords regularly, in accordance with the Access Control Policy.
   2.2 The system shall enforce password history, preventing users from reusing previous passwords.
   2.3 Users shall be notified of upcoming password expiration dates.

3 Password Storage:
   3.1 Passwords shall be stored using a strong encryption algorithm (e.g., AES-256) with salting.
   3.2 Passwords shall never be stored in plain text or transmitted over insecure channels.

4 Password Recovery:
   4.1 A secure password recovery process shall be implemented, such as using security questions, email verification, or SMS verification.
   4.2 The password recovery process shall not reveal the user's actual password.

5 Password Policy Enforcement
   5.1 The password policy defined in the Access Control Policy shall be enforced by the systems.
   5.2 Users who violate the password policy shall be required to change their password.

ANNEX D: ACCESS RIGHTS REVIEW PROCEDURE

This procedure outlines the process for reviewing user access rights to ensure they remain appropriate and in accordance with the principle of least privilege.

1 **Review Frequency:**

1.1 User access rights shall be reviewed at least annually, or more frequently for systems containing sensitive information.

1.2 Access rights shall also be reviewed when job roles change or upon termination of employment.

2. **Review Process:**

2.1 Data owners or system administrators shall review the access rights of users within their respective areas of responsibility.

2.2 The review shall verify that users have the appropriate level of access based on the principles of the least privilege and need-to-know.

2.3 The review shall identify any unnecessary or excessive access rights.

3. **Documentation:**

3.1 Access reviews shall be documented, including the date of the review, the individuals involved, and the findings.

3.2 Any changes to access rights resulting from the review shall be documented and implemented promptly.

4. **Automated Tools**

1.1 Automated tools should be used to facilitate the access rights review process.

ANNEX E: SYSTEM AND APPLICATION ACCESS CONTROL PROCEDURE

This procedure outlines the process for managing access to StyleTrendz's systems and applications.

2 **Role-Based Access Control (RBAC):**

1.1 Access to systems and applications shall be managed using RBAC, where appropriate.
1.2 User roles shall be defined based on job functions and responsibilities.
1.3 Access rights shall be assigned to roles, rather than to individual users.
1.4 Role definitions and access rights shall be documented and regularly reviewed.

2. **Application-Specific Access Controls:**

2.1 Applications shall implement access control mechanisms to restrict access to specific functions and data.
2.2 Application access controls shall be configured to enforce the principles of least privilege and need-to-know.

3. **Default Password Changes:**

3.1 Default passwords for systems and applications shall be changed immediately upon installation.
3.2 A process shall be in place to ensure that default passwords are changed and documented.

4. **System Administration Access:**

4.1 Access to system administration functions shall be restricted to authorized personnel only.
4.2 A list of authorized system administrators shall be maintained and regularly reviewed.
4.3 System administration activities shall be logged and audited.

5. **Remote Access**

5.1 All remote access to StyleTrendz systems must be through a VPN
5.2 The VPN must use strong authentication.
5.3 Remote access must be logged and audited.

ANNEX F: NETWORK ACCESS CONTROL PROCEDURE

This procedure outlines the process for managing access to StyleTrendz's networks.

1 **Network Segmentation:**
   1.1 StyleTrendz's networks shall be segmented to isolate sensitive systems and data.
   1.2 Network segmentation shall be implemented using firewalls, VLANs, or other network access control mechanisms.

2 Firewall Management:
   2.1 Firewall rules shall be established to control network traffic based on the principle of least privilege.
   2.2 Firewall rules shall be regularly reviewed and updated.
   2.3 Changes to firewall rules shall be documented and approved.

3 Intrusion Detection/Prevention:
   3.1 Intrusion detection and prevention systems (IDS/IPS) shall be implemented to monitor network traffic for malicious activity.
   3.2 IDS/IPS alerts shall be investigated and responded to promptly.

4 Wireless Access Control:
   4.1 Wireless network access shall be secured using strong encryption (e.g., WPA3) and authentication (e.g., 802.1X).
   4.2 Guest wireless network access shall be segregated from the corporate network.

5 Access to Network Devices
   5.1 Access to routers, switches and other network devices shall be strictly controlled
   5.2 All access must be logged and audited
   5.3 Default passwords must be changed.

ANNEX G: PHYSICAL ACCESS CONTROL PROCEDURE

This procedure outlines the process for managing physical access to StyleTrendz's facilities and sensitive areas.

1 **Access to Facilities:**
   - 1.1 Physical access to StyleTrendz's facilities shall be controlled using access control mechanisms such as door locks, access cards, and keypads.
   - 1.2 Access to sensitive areas, such as server rooms and data centers, shall be restricted to authorized personnel only.

2 Visitor Management:
   - 2.1 Visitors shall be required to register at the reception desk and provide identification.
   - 2.2 Visitors shall be escorted by authorized personnel while on StyleTrendz's premises.
   - 2.3 A log of all visitors shall be maintained.

3 Security Monitoring:
   - 3.1 Surveillance systems (e.g., CCTV) shall be used to monitor physical access to StyleTrendz's facilities.
   - 3.2 Surveillance footage shall be retained for a specified period.

4 Access Logs
   - 4.1 All physical access to sensitive areas must be logged.
   - 4.2 Access logs must be regularly reviewed.

ANNEX H: MOBILE DEVICE ACCESS CONTROL PROCEDURE

This procedure outlines the process for managing access to StyleTrendz's information assets from mobile devices.

1 **Enrollment:**
   1.1 Employees using mobile devices (company-owned or personal) to access StyleTrendz resources must enroll the device with the designated mobile device management (MDM) solution, if applicable.
2 **Configuration:**
   2.1 Devices must be configured to comply with StyleTrendz's security requirements, including:
      - Strong authentication (e.g., biometric or passcode)
      - Device encryption
      - Automatic screen lock
      - Installation of approved security software
3 **Approved Apps:**
   3.1 Only approved applications may be installed and used
4 **Data Access:**
   4.1 Access to sensitive company data on personal devices may be restricted or prohibited.
5 **Lost or Stolen Devices:**
   5.1 Procedures for reporting lost or stolen devices must be established and communicated to all users.
   5.2 Remote wipe capability must be used to erase data on lost or stolen devices.

ANNEX I: INCIDENT REPORTING PROCEDURE

This procedure outlines the process for reporting security incidents related to access control.

1 **Reporting Security Incidents:**
   1.1 All users shall be required to report any suspected or actual security incidents, including unauthorized access attempts, to the IT department or the CISO.
   1.2 A clear and easy-to-use incident reporting mechanism (e.g., email, hotline) shall be provided.
2 **Incident Response:**
   2.1 Security incidents shall be investigated and responded to in accordance with the StyleTrendz Incident Response Plan.
   2.2 Incident response activities shall be documented.

ANNEX J: COMPLIANCE MONITORING PROCEDURE

This procedure outlines the process for monitoring compliance with the Access Control Policy and its associated procedures.

1 Policy Compliance:

1.1 Compliance with this Access Control Policy and its associated procedures shall be monitored by the CISO and the IT department.

1.2 Regular audits shall be conducted to assess the effectiveness of access controls and identify any non-compliance.

2 Audit Trails:

2.1 Audit trails shall be maintained for all access control-related activities, including user logins, access requests, access grants, and access revocations.

2.2 Audit logs shall be regularly reviewed for suspicious activity.

About Cyberatos

Cyberatos is a professional services company that helps organizations in different industries to be ready for the next cyber-attack. We offer many different business services, including cybersecurity Strategy and Policy planning, cybersecurity assessment, cybersecurity GAP recommendations, reports and policy and procedure templates, mentoring with high-level executives, and many more. Do you have a specific need that's not mentioned on our website? Contact us today with your details and we'll match you up with one of our highly trained and experienced professional consultants. If you wish to reach out, please visit us at https://cyberatos.com

Disclaimer:

This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors. This document refers to marks owned by third parties. All such third-party marks are the property of their respective owners. No sponsorship, endorsement or approval of this content by the owners of such marks is intended, expressed or implied.