**Security Policy & Operations - Project #2**

Coleton Sanheim & Rhean Propp

Table of Contents

[**Data Access**](#_jpknqov7c41z) **3**

[Identification](#_pnhc3yt3aum7) 3

[User Identification](#_scxczm28sbmp) 3

[Guidelines](#_3tieehbte86e) 4

[Authentication](#_w44w4ghj4krc) 4

[Password Complexity](#_cwo6dru1dvhq) 4

[Two-Factor Authentication](#_vpuq0o8bp95d) 5

[Accountability](#_x7q6ruumg04a) 5

[Desktop Session Controls](#_zpwtdw9rvwa) 5

[Auditing Plan](#_rtg4f0zcminb) 5

[**VPN Remote Access With Multi-Factor Authentication**](#_t5relgp7t7ep) **6**

# Data Access

Access to internal systems will only be provided to users based on requirements and responsibilities to function within their job. All modifications to system data must be approved by authorized management personnel. Account modification must also be approved by appropriate management personnel. Security audits will be performed on a regular basis. User and administrator accounts will be investigated. If any incidents or suspicious behavior is uncovered, disciplinary action can and will be administered.

## Identification

The IT department is responsible for adhering to the following procedures:

Directory Service

The selected directory service that will be used is LDAP in conjunction with Microsoft’s Active Directory.

### User Identification

**Requirements**

1. Ensure that user identification is unique.
2. Ensure that non-descriptive user identifications are used to hide job functions.
3. Ensure a separate channel is used when issuing a password for user identification.
4. Ensure administrative accounts are not used for daily operation
5. Ensure special user accounts are given elevated privileges to administer computer systems to allow for target obfuscation.
6. Ensure account IDs are random and do not have any descriptive properties such as “jake\_admin” or “jake”.
7. Ensure all employees have a physical access ID card. The ID card must provide the employees full name, photograph, access level and job title.
8. Ensure physical access ID cards are worn at all times. Any employee caught without an ID card will receive disciplinary action.
9. Ensure physical access ID cards are used to access different parts of the building. Different sections of the building require different levels of security clearance.

### **Guidelines**

1. Employees should receive regular security training. Common phishing practices and social engineering tactics should be reviewed. An action plan for responding to such events must be provided.
2. It is advised that appropriate work attire is enforced to identify persons that should be where they are designated to be.
3. Anyone caught abusing or disregarding security policy should be reprimanded and receive disciplinary action.

## Authentication

### Password Complexity

1. Ensure user passwords are at least 8 characters long, contain combinations of lowercase characters, uppercase characters, numbers, and special characters. This protects against brute force attacks and password guessing.
2. Ensure passwords do not contain any personal information such as names, dates, pets or anything identifiable to the person.
3. Ensure passwords are not written in plain text documents.
4. Ensure passwords are not written on sticky notes or any nearby physical object.
5. Ensure administrator passwords are at least 10 characters long, contain combinations of lowercase characters, uppercase characters, numbers and special characters.
6. Ensure administrator passwords contain alt-characters (e.g. Alt + 1 + 2 + 7 = ⌂). These characters are often not included in brute force attacks, increasing the difficulty of password cracking.

### 

### Two-Factor Authentication

1. Ensure multi factor authentication is enabled for both admin and non-special access users. User ID and password are required for account access. Once entered, an authentication app on the user’s phone must be used to verify the identity of the user. A 5-10 digit code that is renewed every 60 seconds must be entered within 30 seconds of attempted account access. If entered correctly, the user will gain access.

## Accountability

### Desktop Session Controls

1. Ensure computers log the user out after 5 minutes of machine inactivity.
2. Ensure screen savers do not display sensitive information.
3. Ensure a screen guard is enabled on all machines to discourage and mitigate shoulder surfing.
4. Ensure there is a limit to how many active sessions a user can log into.
5. Ensure high value systems are inaccessible after hours.
6. Ensure there is a logging system to see who logged in to which systems at which date and time.

### Auditing Plan

1. Ensure security audits are performed annually. This will ensure that auditing will be done regularly while not being disruptive to business activities.
2. Ensure security audits are performed on all necessary departments of the company.
3. Ensure security audits are performed by authenticated and verified security personnel that are a part of the Information Security Team.
4. Ensure any security issues are properly documented and investigated thoroughly should they arise.
5. Ensure security threats are reported to the Chief Information Security officer.
6. Ensure security training is required and regularly administered to all company staff.

# VPN Remote Access With Multi-Factor Authentication

