NCS lab 1

Information Security Policies

Danil Usmanov
Egor Osokin
Olga Chernukhina
BS-18-SB-01

Critique report on **Logical Access Control** section

5 Logical Access Control	
Chapter citation	**Comment**
5.1 Introduction	
5.1.1. The purpose of logical access control is to manage access to information in a way that: a) System is protected from unauthorized access b) Accidental damage from authorized user is minimized c) All Users have access to appropriate resources.	5.1.1. The goal is clearly defined, containing confidentiality, authentication, authorisation, identification in it.
5.1.2. This section addresses the logical access control requirements for All Users, and network devices such as router, switches, and computers.	5.1.2. The goal to include routers and switches in the following section is very obscure. Moreover, this is the only subpoint, where routers and switches are mentioned.
5.1.3. Audit requirements are also addressed in this section.	5.1.3. The motivation behind including audit requirements in the chapter named Logical Access Control is not clear
5.2 Authentication and Password (5.2 There is no information concerning password, so the section is better be renamed to "Authentication and User ID")	
(Restructuring) 5.9.2 All Users shall have a unique User ID such that activities can be traced to responsible user.	
5.2.1. All Users shall be held accountable for every action carried out by his/her User ID.	5.2.1. Non-repudiation is mentioned
5.2.2. All Users shall be uniquely identified and authenticated on the system before access to the system is granted.	5.2.2. While there is a requirement for identification and authentication, there is no mention on anti-spoofing measures such as 2FA
5.2.3. User ID should be suspended if one of the following conditions applies: a) The User ID has not been used for a defined period b) Staff is on long leave (e.g. sabbatical or extended leave)	5.2.3. The "defined period" should be properly defined in a number of days. The same for the "long leave".

c) Staff is on overseas assignment of duration longer than 6 months.	
5.2.4. User ID should be deleted on the following condition: a) Access rights removed b) Termination of employment c) Retirement d) Deceased.	5.2.4. An additional condition should be added for the cases of compromised User IDs
5.3 User Access Profiles	
5.3.1. Every application shall have a User Access Profile. Business Owners are responsible to authorize access to applications that they are responsible for.	
5.3.2. Business Owners shall maintain a formal record of all registered users and their access rights.	5.3.2 It is better to clarify the form of the record - is it electronic or is it on paper
5.3.3. Non-standard access may be granted in exceptional circumstances that shall be subjected to special authorization and controlled and applied only for a limited time.	5.3.3. The definition of “exceptional circumstances” should be set, or the employee title who is responsible for the final decision should be mentioned
5.3.4. Business Owners shall conduct review at regular intervals to review user access rights.	5.3.4. The recommendation on the intervals’ duration should be added
5.4 User Access Control	
5.4.1. For access to ABC systems that contain personal user data, All Users shall sign the confidentiality agreement to abide by the Data Protection Policy before they are registered.	5.4.1 Indeed it is a good practice to sign the agreement that has juridical power before having any access to sensitive and nonsensitive information
5.4.2. All Users shall have their personal User ID and password pair for the system. User ID and password shall not be shared.	
5.4.3. Group ID should only be used with approval from Director of Information Technology.	5.4.3 This is the only place in the Policy Group ID is mentioned at. It is better to define it in the same way as User ID was defined in 5.2 (or give a reference to the official document stating Group ID)
5.4.4. Whenever Generic ID is re-assigned, the password shall be changed.	5.4.4 This is the only place in the Policy Generic ID is mentioned at. It is better to define it in the same way as User ID was

5.4.5. There shall be a formal user registration and de-registration process for creation of user accounts.	defined in 5.2 (or give a reference to the official document stating Generic ID)
5.5 Password	
5.5.1. The use of logon passwords for authentication shall be implemented.	
5.5.2. Password should be at least 6 characters long if it is alphanumeric and case sensitive. If it is not case sensitive, it should be at least 8 characters long.	5.5.2 It is better to prohibit case-insensitive passwords and make a strong password generation program to generate a long and random password for the user.
5.5.3. All passwords to be distributed should be in sealed envelopes and delivered personally to the person concerned (if applicable). If the password is being distributed electronically, it should be sent in an encrypted manner.	5.5.3 All envelopes should have a single-use tear-off tape, and there should be an opaque layer inside them to prevent data leakage without opening the envelope.
5.5.4. All Users shall ensure password confidentiality and prevent disclosure and compromise at all times.	
5.5.5. Password file on system shall always be encrypted in storage.	
5.5.6. All Users should follow good security practices in the selection and use of password.	5.5.6 “Good security practices” are not defined.
5.5.7. All passwords should be changed periodically every 100 days. System administrator's passwords should be changed every 90 days.	5.5.7 Periodically changing passwords is important and is a good practice if done correctly. However, NIST stated that regularly changing passwords does not result in more secure passwords if the user is forced to enter a new password by hand. In this case, strong password generators and storage are preferred.
5.6 User Activities Monitoring	
5.6.1 ABC reserves the right to monitor computer facilities, systems, files, etc., for	

any suspected abuse, unauthorized or illegal activities.	
5.6.2 All user activities may be monitored at the system and at the network level depending on the access rights granted and the system and network services to be accessed.	
5.6.3 A Warning Banner should be displayed during logon for critical and sensitive systems to deter unauthorized access and to explicitly state that the usage of the system is subject to monitoring.	
5.7 Monitoring and Audit Log	
5.7.1 Audit logs should be retained to enable investigation to be carried out when necessary.	5.7.1 It makes sense to combine this with 5.7.8 since they are 2 aspects of the same issue or replace 5.7.8 to be 5.7.2
(Restructuring) 5.7.8 Application and System audit logs should be retained for a specified retention period defined by the Business Owners.	
5.7.2 Audit logs should be protected against unauthorized access and corruption.	
5.7.3 For systems and network managed by service provider, the auditing requirements shall be clearly defined and agreed.	5.7.3 Nothing is said about backing up logs to individual machines.
5.7.4 All computer clocks shall be synchronized on a regular basis. This is to ensure the accuracy of the audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.	5.7.4 Clock synchronization is an important aspect when working with audit logs from multiple machines.
5.7.5 Audit logs of critical systems shall be regularly reviewed, on a sampling basis, at least monthly. Suspicious activities shall be reported directly to SIRO. This should be done by a designated staff.	5.7.5 It is better to track logs automatically in real time, rather than monthly.
5.7.6 The following information should be captured in audit logs and monitored accordingly:	

a) Successful and unsuccessful logon event b) Security profile changes c) All activities related to privileged levels of access. 5.7.7 For financial and online transaction systems, transaction events and file modification activities (such as file delete, file edit) should also be captured in the audit logs. 5.7.8 Application and system audit logs should be retained for a specified retention period defined by the Business Owners.	5.7.7 All user actions, security, and transactions must be saved. You can also add system logs, such as boot and shutdown times.
5.8 Application Access Control	
5.8.1 Access to application shall be granted in accordance to the access rules set by the Business Owners. 5.8.2 Access rights should be reviewed periodically and excess rights removed.	5.8.2 It is indeed necessary to review access rights, though it is worth to specify the period and the responsible position
5.9 Operating System Access Control	
5.9.1 Access to operating system services shall be restricted to Administrator account. 5.9.2 All Users shall have a unique User ID such that activities can be traced to responsible user. 5.9.3 Periodically, it is necessary to change the Operating System (including upgrade to newer version). When such changes occur the security of the system should be reviewed to ensure that it does not introduced any vulnerability.	5.9.2 It is kind of a replication of 5.2.1 (and logically the fact that all Users should have a unique User ID should precede 5.2.1) 5.9.3 Software updates must be handled with precision to reduce the risk of avoiding the risk of compromising the system.
5.10 Mobile Computing Devices	
5.10.1 All Users are responsible for the	

security of Mobile Computing Devices (MCD) such as notebook/laptop/PDA etc. assigned, and to ensure that the business information stored is backed up regularly.	
5.10.2 When working from home, All Users shall use the company assigned MCDs for official work purpose only.	
5.10.3 When connected to internal ABC network, MCDs should not be connected to any other network or sites.	5.10.3 It may not be possible, but a VPN connection gives you another layer of data privacy.
5.10.4 For MCDs holding confidential information, implement encryption and anti-virus controls to protect the information.	
5.10.5 On a periodic basis, all assigned MCDs should be reviewed to ensure that appropriate security measures (such as anti-virus software) are maintained and updated.	5.10.5 It is better to prevent users from installing any software on the MCD.

Password standard

Inspired by University of Georgia Password Standard.

1.0 Password Construction

1.0.1 Minimum Password Length

Passwords shall have a minimum of 8 characters consisting of alphanumeric and special characters. At least one upper letter character and a special symbol shall be presented.

1.0.2 Password Composition

Passwords shall not consist of the publicly known weak passwords. The password shall not contain username.

1.1 Password Management

1.1.1 Password Storage

The password shall be memorized or saved in the password manager apps approved by the Security Department. The best recommended choice is 1Password at https://1password.com/.

1.1.2 Password History and Reuse

Users will be prohibited from re-using any previously used passwords in order to motivate the usage of automatically generated random passwords

1.2 Recommendations for the System and Database administrators, and Application developers

1.2.1 Storage

The raw password shall never be saved in the database or in any file. Only the SHA-256 hash of password shall be stored. The data inside the database should be encrypted with AES.

1.3 Emergency case

In the case of emergency, the employee is obligated to notify the Security department by any means of communication

Password management guidelines

Purpose

The purpose of this Guideline is to educate ABC Corporation (ABC) faculty and staff on the characteristics of a Strong Password as well as to provide recommendations on how to securely maintain and manage passwords.

Applies To

This Guidelines applies to all staff that have a password to at least one system or application, independent of whether he/she is an end user or a system administrator for that system or application.

Definitions

A *Strong Password* is defined as a password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.

Guidelines

The following are general **recommendations for creating** a Strong Password:

A Strong Password **should**

- Be at least 8 characters in length
- Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
- Have at least one numeric character (e.g. 0-9)
- Have at least one special character (e.g. ~!@#$%^&*()_-+=)

A Strong Password **should not**

- Spell a word or series of words that can be found in a standard dictionary
- Spell a word with a number added to the beginning and the end
- Be based on any personal information such as User ID, family name, pet, birthday, etc.

The following are several **recommendations for maintaining** a Strong Password:

- Do not share your password with anyone for any reason

- Change your password upon indication of compromise

  After resetting your password, report the incident to your local departmental administrator and/or the Information Security Office at information_security_office@abc.inc

- Avoid reusing a password

- Avoid using the same password for multiple accounts

The following are several **recommendations for recovering** a password:

- Request the new password from the Information Security Office with the means of physical presence in the office.

Additional Information

If you have any questions or comments related to this Guideline, please send email to the Information Security Office at information_security_office@abc.inc

Password change procedure

This document was inspired by link.

Introduction

This document describes the process of changing the user password.

This procedure has been created to ensure that staff is aware of the steps required to adequately protect company's data and that all users of the company IT systems are aware of their responsibilities with regard to effective password management.

Prerequisites

The Password management procedure is designed to ensure all users of the company IT systems have the tools and processes available to them in order to effectively protect their identity and data/systems belonging to the Company. All users of company systems must follow the Company Password Management Procedure. This procedure outlines the responsibilities of both system users and Information Services.

You must have an account in the company to verify your identity. If you do not have an account, please refer to the IT department.

You must have access to your account. If you lose your credentials, contact the IT department.

You must be connected to the internal VSC network. Please refer to the document "Internal Network Access".

Step-by-step example of user password change

1. Go to the private account on the company's website and click on the button "change password".
2. Verify your identity by answering several secret questions or using 2FA.
3. Create a new password with rules according to "password management guideline". You can use this service to create new strong password.
4. Verify procedure by the link that will send you on your restore email.