MULTIMEDIA UNIVERSITY

CCS 6214 – Cybersecurity Fundamentals

Name: Youssef Fathy ID: 1221302092

TUTORIAL ASSIGNMENT 04

Marks are allocated based on the rubrics below. Each question is allocated 1 mark, total marks will be normalized to 4 marks.

Please make sure that your solution is properly cited and referenced, where applicable. Failing to do so, your solution will not be graded.

Please fill up and submit this document in PDF format to Microsoft Teams. Late submissions will not be accepted and graded. Please take note of the deadline and the deadline follows **Microsoft Teams system's time, not your PC's time. Do submit early and don't take the risk of being cut off from the submission.**

Rubrics:

No evidence/wrong solution/no citation or references 0 mark	Average 0.5 mark	Good 1 mark
No evidence of solution; or wrong solution; or **no citations and references.**	Partially correct or incomplete solution.	Correct and complete solution.

1. As part of a system administration team for MMU, create a step-by-step IT security policy for implementing a new user account for an incoming student. The policy should define what resources the student has access to, what she does not have access to, and for how long access is granted. State any assumptions that you may have.

    1. Overview

    This policy establishes the procedures and guidelines for creating and managing new user accounts for incoming students at Multimedia University (MMU). The goal is to ensure the secure and efficient allocation of IT resources while safeguarding university data and systems.

    2. Purpose

    The purpose of this policy is to provide a clear framework for the provisioning, management, and security of student accounts. It ensures that students have the necessary access to academic resources while protecting university assets from unauthorized access and misuse.

3. Scope

This policy applies to all incoming students at MMU requiring access to university IT resources, including email, learning management systems (LMS), library databases, and campus network services. It defines the roles and responsibilities of students, IT staff, and university administrators.

4. Policy

4.1 -Account Creation and Authorization

Eligibility: All registered incoming students are eligible for a user account. The Registrar's Office will provide the IT department with a list of eligible students.

Authorization: Verification of student registration status by the IT department is required before account creation.

4.2 - Account Provisioning

User ID and Email: Each student receives a unique user ID and an MMU email address, formatted as [firstname.lastname@student.mmu.edu].

Initial Password: An initial password is sent to the student's personal email, which must be changed upon first login.

4.3 -Resource Access

Granted Access: Students have access to email services, LMS (e.g., Moodle), library resources, campus Wi-Fi, and other essential academic tools.

Restricted Access: Access to administrative systems, faculty-only resources, and confidential university data is prohibited.

Duration of Access: Access is granted for the duration of the student's enrollment. Accounts are deactivated 90 days post-graduation or withdrawal.

4.4- Security Measures

Password Management: Adherence to the university's password policy, including regular password changes and the use of strong passwords, is mandatory.

Multi-Factor Authentication (MFA): MFA is implemented where applicable to enhance security.

Monitoring and Reporting: Account activities are monitored for unusual behavior. Suspicious activities must be reported to the IT helpdesk immediately.

4.5- Compliance and Responsibilities

User Responsibility: Students must comply with the university's Acceptable Use Policy and are responsible for securing their accounts.

IT Department Responsibility: The IT department is responsible for maintaining IT infrastructure security, managing user accounts, and providing support to students.

4.6- Termination of Access

Account Deactivation: Accounts are deactivated 90 days after graduation or withdrawal. Extensions may be granted for ongoing university projects upon request.

Data Retention: Email and file storage data are retained for 90 days post-deactivation before permanent deletion.

5- Assumptions

All students have a personal email address on file with the Registrar's Office.

The IT department has the necessary tools to implement MFA and monitor account activities.

Refrances :
1-https://kb.itd.commonwealthu.edu/books/user-accounts/page/student-user-accounts
2-https://oit.princeton.edu/policies/information-security
3- Free and Downloadable Account Management Policy Template [2024] (heimdalsecurity.com)
4- IT Security Standard: Managing Computer Accounts - Information Security - Cal Poly, San Luis Obispo
5- Sample Account Management Policy Template (purplesec.us)

2. Examine the following web resources that discuss security policies:
   SANS Institute policies:
   www.sans.org/resources/policies/

   a. Choose 5 policies and summarize the main theme of these policy recommendations.

1. Acceptable Use Policy

Defines acceptable and unacceptable uses of organizational IT resources. Emphasizes responsible use, protection of sensitive information, and consequences for violations.

2. Password Protection Policy

Provides guidelines for creating, managing, and protecting passwords. Highlights the importance of strong passwords and regular updates.

3. Data Protection Policy

Outlines measures to safeguard sensitive data. Includes data encryption, access control, and data breach response procedures.

4. Incident Response Policy

Establishes procedures for identifying, managing, and responding to security incidents. Focuses on minimizing damage and recovery steps.

5. Remote Access Policy

Specifies requirements for secure remote access to the organization's network. Includes the use of VPNs, authentication, and monitoring.

b. Choose which policy out of the 5 recommendation you believe is the most secure and state the reasons for your choice.

The Most Secure Policy and Reasons
Incident Response Policy is considered the most secure because it ensures a structured approach to managing and mitigating security incidents, minimizing damage, and facilitating a swift recovery. It encompasses preparedness, detection, containment, eradication, recovery, and lessons learned, providing a comprehensive framework for handling threats effectively.