Harris McCall
CSIA300
Matt Boehnke
Lab 5

XYZ Corp Identity & Access Management Policy
Version *1.12* (prev. *1.11*)

Approved: 6/10/2023
Effective: 6/11/2023

Purpose:

This Identity & Access Management (IAM) policy for XYZ Corp establishes the requirements for managing user identities, authorizing user permissions, authenticating user access, and auditing access activities across organization systems and resources. The policy's purpose is to ensure the confidentiality, integrity, and availability (CIA) of XYZ Corp's data and resources, as well as ensuring that company resources are used in compliance with security, business, and legal requirements.

Scope:

This policy applies to all employees, contractors, partners, and any other users who access XYZ Corp's systems, networks, or data resources. It covers all user accounts and access points within the organization's environment.

Responsibilities:

- The *Chief Information Security Officer* (CISO) is responsible for overseeing the enforcement of this IAM policy.
- The IT department is responsible for implementing and maintaining IAM processes and controls.
- All employees, contractors, and users are responsible for adhering to the IAM policy when accessing XYZ Corp resources.

Policy:

1. User Identification:

- All users must be uniquely identified within the XYZ Corp systems based on a combination of factors, including usernames, email addresses, or employee IDs following organization naming conventions.

2. Authorization:

- Access permissions are based on the principle of least privilege (PoLP). Users are only granted access to resources necessary for their roles.
- Access control lists (ACLs) and role-based access control (RBAC) will be used to manage permissions.
- Regular access reviews will be conducted to ensure ongoing compliance.

3. Authentication:

- Users must authenticate using secure and approved methods, such as passwords, biometrics, or multi-factor authentication (MFA).
- Passwords must adhere to the following complexity and expiration policy:
    - Min length = 8 characters
    - Minimum 1 lower and 1 uppercase letter, 1 number, and 1 special character
    - Expiry = 90 days
    - Lockout policy = Locked for 30 minutes after 3 failed attempts
- MFA is required for access to sensitive systems and data.

4. Auditing:

- XYZ Corp will maintain comprehensive audit logs for all access and activities on its systems, and regular reviews of audit logs will be performed to identify and respond to security incidents.
- Audit logs will include:
    - user actions (write, execute, delete, etc.)
    - access attempts (failed login attempts)
    - security-related events (account creation/deletion, password changes, etc.)

Compliance:

Refusing or inability to comply with this IAM policy could result in disciplinary action, including but not limited to access restriction, suspension, termination, or legal actions in the case of data breaches or misuse.

Review:

This policy will be reviewed semi-annually or as needed to appropriately align with changing business requirements and regulatory standards. All updates will be proposed and reviewed by the CISO and IT department, and any necessary changes will be communicated to all relevant stakeholders.

XYZ Corp is committed to safeguarding its information and assets through effective Identity & Access Management. By accepting this policy, all users acknowledge their responsibility to comply with its guidelines.

Print Name: _____ Department: _____

Signature: _____ Date: _____