Identity and Access Management Security Policy

Last Update Status: *Updated March 2023*

1. Overview

This written document is a security policy on the importance of identity and access management and how to protect our company from identity theft and its consequences. Identity and access management allows our company to quickly and accurately verify an employee's identity and provide necessary permissions for their resources as soon as possible. This policy will also address the threats of identity theft and fraud within our company's assets as rates have increased. All employees of our company must always be aware of these policies.

2. Purpose of Policy

The purpose of this policy is to protect our company from the increasing risk rates of identity theft, fraud, and unauthorized access via employee credentials, accounts, and access while providing access to our organization's resources (files, apps, data, etc.). These policies are set in place to protect employees and the company. Weak credentials, irresponsible privacy of personal information, and lack of updated methods to secure employee sensitive information increases the risk of compromised accounts, identity theft, identity fraud, misuse of accounts, and prohibited access to personal and work accounts.

3. Scope

This policy applies to employees, consultants, temporary staff, remote workers, contractors, and individuals who have authorized access and relations with this company. These principles should be applied to all accounts related to company materials, systems, and applications. This includes: work email accounts, work portal accounts, accounts for work applications financial/payment accounts, personal accounts, and devices that have access to our network.
Company Data we protect:

a. Employee Personal Data
b. Employee Work-Related Data
c. Human Resources Data
d. Company Databases
e. Company Applications
f. Company Resources (files, and file permissions)

4. Policy

4.1. Every employee must have a complex password with a minimum of 10 characters.

4.2 Sharing your personal sensitive information publicly such as: work email, password, username, security question credentials, biometric information, exact building/home location and address while working is strongly discouraged.

4.3. Sharing sensitive information publicly related to the company and fellow employees such as their credentials, biometric information, and work email addresses is prohibited.

4.4 Do not provide personal information to requesting parties who are unfamiliar, unauthorized, unaccredited, and/or not part of our company.

4.5 Do not grant access to any work-related account to other employees, family members, friends, or outside sources.

4.7 Do not click or reply on suspicious emails, text messages, phone calls, or direct messaging on social media sites, applications, and platforms from sources you do not know or trust.

4.8 Do not edit/modify user or group permissions to files that have been predetermined by our IAM management/administration. If you have a concern, question, or adjustment please contact them as soon as possible to make reasonable changes.

4.9 Every employee will have single sign-on enabled and multi-factor authentication to ensure an additional layer of security for all work-related accounts.

4.10 Unless authorized, do not access or download work-related applications, accounts, files from personal computers, wearables, mobile devices.

5. Policy Compliance

5.1 Compliance

The business and its employees should be able to follow this security policy and implement it in order to reduce the risk of its employees being targeted and becoming a victim of identity theft, fraud, or unwanted access/control of work/personal accounts. This policy should be reviewed at least once a year and reviewed if important updates are made.

5.2 Non-Compliance

If the business and/or its employees fail to comply with this security policy, not only will all within our company become more vulnerable to identity theft and access attacks, disciplinary action will take place. Termination of employment may occur if a security breach or incident occurs in the absence of a security policy implementation.

6. Audits

Audits will be performed quarterly throughout user accounts to ensure the policy is being followed and the employees are only accessing necessary permitted accounts and resources. Passwords will be asked to be renewed 2-4 times a year depending on the employee’s necessary exposure to company content. This ensures the biggest employee data risks are identified, analyzed, and protected.

7. Revision History

Date of Change: 3/12/2023 | Responsible: Liela Pressley | Summary of Change: Created New Policy

References

Brooks, C. (2023, March 6). *Cybersecurity Trends & Statistics For 2023: More Treachery And Risk Ahead As Attack Surface And Hacker Capabilities Grow*. Forbes. https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=f269ebc19dba

Ciampa, M. (2021). *EBook: CompTIA security+ guide to network security fundamentals*. (pp. 353-377, 389-397)Cengage.

What is Identity Access Management (IAM)? | Microsoft Security. (n.d.). https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam