**Access Control Policy:**

**Document History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Summary of Changes** |
| **1.0** | **10/01/2023** | **Document creation and  approval** |

**Review Distribution**

|  |  |
| --- | --- |
| **Name** | **Job Title** |
| **Sabrina Senat** | **CEO** |
| **Paul Evans** | **President** |
| **Sally McCarty** | **Vice-President** |
| **William Clay** | **IT Team Supervisor** |
| **Tony Roch** | **Printing Manager** |
| **Jack Johns** | **HR Manager** |
| **Maria Garcia** | **Financial Manager** |

**Document Approval**

|  |  |  |
| --- | --- | --- |
| **Version** | **Organisation** | **Position Date** |
| **1.0** | **IT Team** |  |

**Purpose:** The purpose of this policy is to establish guidelines for the management of access to ABC Technologies resources, including the processes, procedures, and records related to access control.

**Scope:** This policy applies to all access to ABC Technologies resources, including but not limited to physical and digital assets, systems, networks, and data.

**Introduction:**

An access control policy is a set of guidelines that outlines how a company will manage and control access to its systems, resources, and data. The goal of an access control policy is to ensure that access to these assets is granted only to authorised individuals, and that unauthorised access is prevented or detected. By implementing an access control policy, a company can help to protect the security and integrity of its systems and data, and ensure that they are used in a responsible and accountable manner (ISO, 2013).

**Principles:**

* ABC Technologies will establish and maintain a centralised system for managing access to its resources, including the assignment of roles and permissions.
* Access to ABC Technologies resources will be granted on a need-to-know basis, based on an individual's job responsibilities and authorised access levels.
* ABC Technologies will establish and follow a formal process for requesting, approving, and revoking access to its resources. This process will include the following steps:
* An individual submits a request for access to the appropriate IT or security personnel.
* The IT or security personnel review the request to determine if the individual has a legitimate business need for the requested access.
* If the request is approved, the IT or security personnel assign the appropriate roles and permissions to the individual.
* If the request is denied, the IT or security personnel inform the individual of the decision and provide an explanation for the denial.
* ABC Technologies will establish and follow procedures for enforcing access controls and for monitoring and auditing access to its resources. These procedures may include, but are not limited to, authentication, access controls, encryption, and log review.
* ABC Technologies will maintain records of all access requests, approvals, and revocations, including the date of the request, the individual requesting access, the resource being accessed, and the reason for the request.
* ABC Technologies will regularly review and update its access control policies and procedures to ensure that they are effective and aligned with the organisation's security needs.

(Williams, 2016)

**Disciplinary Consequences:**

* Any suspected or actual breach of this policy needs to be reported to vice-president, president or CEO of ABC Technologies through a suitable channel. Appropriate action must then be taken by the vice president, president or CEO where they will take appropriate action and involve any relevant external and internal authorities.
* Compliance of this policy must be followed else disciplinary action will be taken in accordance with relevant process.

(Buckinghamshire New University, 2015).

**Responsibilities:**

**ABC Technologies responsibilities:**

* Providing training and resources to employees to help them understand the importance of access control and how to use the organization's access control systems and devices.

**IT team responsibilities:**

* Identify and classify the organization's sensitive data, resources, and systems and implementing appropriate levels of access controls to protect them.
* Establish procedures for granting, modifying, and revoking access to the organization's resources and systems, based on the principle of least privilege.
* Establish procedures for maintaining the security of access control systems and devices, such as firewalls, intrusion detection systems, and access control servers.
* Establish guidelines for the use of access control systems and devices, and communicating them to employees.
* Regular monitoring and reviewing access control systems and devices to ensure they are functioning properly and effectively.
* Regular reviewing and updating the access control policy to ensure it remains effective and relevant.
* Ensure compliance with relevant laws, regulations, standards, and best practices related to access control.
* Regular testing and reviewing the access control to identify vulnerabilities and address potential threats.

(Buckinghamshire New University, 2015).

**Third-party:**

* Ensuring compliance with relevant laws, regulations, standards, and best practices related to access control.
* Regular testing and reviewing the access control to identify vulnerabilities and address potential threats.

(Kobayashi et al., 2019)

**Contractors and Voluntary Staff:**

* Keeping accurate records of access control activities, such as login attempts and user access, to aid in incident response and investigations.

**Key Outcomes:**

* **Enhanced security and protection of company systems and data:** Implementing appropriate safeguards and controls, ABC Technologies can help to prevent unauthorised access or misuse of its systems and data, which can protect the security and integrity of these assets.
* **Improved compliance with relevant laws and regulations:** Access control policy can help a company ensure that it is in compliance with any relevant laws and regulations, such as data protection and privacy laws.
* **Greater transparency and accountability in the use of company systems and data:** Controlling and monitoring access to these assets, ABC Technologies can ensure that they are used in a responsible and accountable manner, which can improve trust and confidence among stakeholders.
* **Improved efficiency and productivity:** By enabling authorised users to access the resources they need in a timely and convenient manner, a company can help to improve the efficiency and productivity of its employees and partners.
* **Improved reputation and image:** A company that is seen as a responsible and trustworthy steward of its systems and data is likely to have a more positive reputation and image in the eyes of its stakeholders.

(Calder, 2017)

**Related policies:**

* **Password policy:** This policy outlines the requirements for creating and using secure passwords, as well as procedures for changing or resetting passwords.
* **Device security policy:** This policy outlines the measures that a company will take to protect its devices from unauthorised access or misuse, such as installing antivirus software and configuring firewalls.
* **Network security policy:** This policy outlines the measures that a company will take to protect its networks from unauthorised access or misuse, such as implementing VPNs and firewalls.
* **Mobile device management policy:** This policy outlines the procedures for managing and securing company-owned mobile devices, such as smartphones and tablets, when they are being used to access company resources.
* **Remote access policy:** This policy outlines the procedures for accessing company resources remotely, including the use of secure connections and authentication methods.