Guest Access Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Computer accounts are the means used to grant access to ABC Company information resources. These accounts provide a means of providing accountability, a key to any computer security program, for information resources usage and restrictions. Specific circumstances may require guests (non ABC Company Staff) to have access to ABC Company Information Resources.

# II. Purpose

This policy establishes the rules for the creation, monitoring, control, and removal of guest user accounts.

# III. Scope

This policy applies to all individuals who have access to ABC Company’s Information Resources.

# IV. Policy

Access to ABC Company Information Resources by a guest shall be coordinated through a sponsor. The sponsor will typically have some relationship with the guest. The sponsor will take responsibility for the actions of the guest while they are utilizing ABC Company Information Resources.

Members of the Board of Directors or advisory group members shall be eligible for guest access for the duration of their term. ABC Company Executive Management is allowed to sponsor a guest up to 90 days. Department Heads are allowed to sponsor a guest up to 7 days. The following categories of guests are eligible to be sponsored:

* New Staff waiting for their permanent logon credentials.
* Staff attending orientation or educational events.
* Commercial vendors or suppliers invited to demonstrate their equipment.
* Media such as television, radio, newspapers, and magazines.
* Conference and meeting presenters attending an event sponsored by an ABC Company Department. Participants are eligible for sponsorship only if they are actively participating in the event and not just a member of the audience.

Guest access to Information Resources shall be permitted only after approval from the appropriate sponsor. Guests are allowed to access the Internet, selected printers, and basic Microsoft Office programs. Guests shall not have the ability to:

* Download files from the Internet.
* Modify or install programs or utilities.
* Save files to hard drives.

Guests are subject to the same procedures and security controls used for ABC Company Staff. Sponsors are responsible for ensuring that guests know the procedures and security controls governing access to Information Resources. The IT Department is responsible for assigning temporary IDs to the guest and making records available for audit. It is the responsibility of service providers to determine to what extent guests are eligible to use their services and to authorize service usage as needed.

The IT Department shall implement a wireless network to support wireless access for guests. Procedures shall be established to ensure the guest wireless network cannot connect to ABC Company’s in-house network or access company data. The guest wireless network shall meet the security requirements specified in the Wireless Access Policy.

The Chief Security Officer shall ensure:

* The organization has implemented procedures for terminating access when the guest leaves or the time period has expired.
* Procedures assign responsibility for removing IT and/or physical access. Procedures include timely communication of termination actions to ensure that the procedures are appropriately followed.
* Procedures are based upon initial access authorization and subsequent modification of a guest’s access to Information Resources.
* Procedures are in place for establishing and modifying guest access to Information Resources. Such procedures shall be formally documented and updated regularly.
* An annual, or more frequent, review of the procedure to grant, modify, and terminate guest access to Information Resources.
* The organization assigns a unique name and/or number for identifying and tracking user identity. Procedures require the user ID to be in a specific format and specify the format to be used. Procedures specify that the unique user ID be used to track guest activity.
* Authentication procedures verify a person or entity seeking access to Information Resources is the one claimed. Policies specify the types of approved authentication mechanisms that are reasonable and appropriate.

All guest accounts created must have an associated request and approval that is appropriate for the ABC Company system or service. All accounts must be uniquely identifiable using the assigned user name.

All default passwords for accounts must be constructed in accordance with the ABC Company Password Policy. All accounts must have a password expiration that complies with the guest sponsor time period and Password Policy.

System Administrators or other designated staff:

* Are responsible for granting, modifying and removing guest accounts when they reach the end of their sponsor period.
* Must have a documented process to modify a user account to accommodate situations such as name changes and permission changes.
* Must have a documented process for periodically reviewing existing accounts for validity and ensuring that guest accounts are removed in a timely manner.
* Are subject to independent audit review.
* Must provide a list of accounts for the systems they administer when requested by authorized ABC Company management.
* Must cooperate with authorized ABC Company management investigating security incidents.

# V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all Staff members with access to ABC Company’s Information Resources.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO01.02, APO01.11, APO14.10, BAI09.03-04, DSS01.05

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 64.308(a)(4)(ii)(B), 164.310(a)(2)(ii), 164.310(a)(2)(iii)

ISO 27001 8.2-3, A.7, A.8.3.3, A.9, A.11

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 AT-3, PS-1, PS-3, PS-7

NIST Cybersecurity Framework ID.RA-6, ID.RM-1, PR.AC-1-2, PR.AC-7, DE.CM-2-3

PCI 6.1, 7.1-3, 8.1, 8.6, 9.1-4, 9.10