Admin Special 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

Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

# II. Purpose

The purpose of this policy is to establish the rules for creating, using, monitoring, controlling, and removing accounts with special access privileges.

# III. Scope

This policy applies to all Staff that have, or may require, special access privilege to any ABC Company Information Resources.

# IV. Policy

ABC Company departments must submit to the IT Department a list of administrative contacts for their systems that are connected to the ABC Company network.

All users must sign the ABC Company non-disclosure agreement before access is given to an account.

All users of Administrative/Special access accounts must have account management instructions, documentation, training, and authorization. Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the IT Director.

Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (e.g. user account vs. administrator account). Users with administrative account access shall use a dedicated or secondary account for elevated activities. This account shall only be used for administrative activities and not Internet browsing, e-mail, or similar activities.

Each account used for administrative/special access must comply with ABC Company’s Password Policy. The password for a shared administrator/special access account must change when an individual with the password leaves the department or ABC Company, or upon a change in the vendor personnel assigned to the ABC Company contract.

In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.

When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:

* Must be authorized
* Must be created with a specific expiration date
* Must be removed when work is complete

# V. Enforcement

Any Staff member 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 IT system administrators and security personnel.

**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, DSS05.02, DSS05.07

GDPR Article 32

HIPAA 164.312(a)(2)(i)

ISO 27001 A.7.2.1, A.12.4.3

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 AC-2, AC-5, AC-6, AT-3

NIST Cybersecurity Framework PR.AC, PR.AT-2, DE.DP-2, RS.RP-1

PCI 2.2.4.a-c, 6.4.2, 7.1.1-2