Change Management 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

ABC Company’s Information Resources are continuously becoming more complex with a dependency between resources. From time to time each Information Resource requires an outage for planned upgrades, maintenance, or fine-tuning. In addition, unplanned outages may occur that require upgrades, maintenance, or fine-tuning. Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure.

# II. Purpose

The purpose of this policy is to manage changes in a planned and predictable manner so that Staff can plan accordingly. Changes require planning, monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of ABC Company’s Information Resources.

# III. Scope

This policy applies to all Staff that installs, operates, or maintains Information Resources.

# IV. Policy

Every change to an Information Resource (e.g. operating system, computing hardware, networks, applications, data centers) is subject to this policy and must follow appropriate change management procedures.

All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with appropriate department head.

A Change Management Committee, appointed by department heads, shall meet on a regular basis to review change requests and to ensure that change reviews and communications are satisfactorily performed.

A formal written change request must be submitted for all changes, both scheduled and unscheduled. All scheduled change requests must be submitted in accordance with change management procedures so that the Change Management Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.

Each scheduled change request must receive formal Change Management Committee approval before proceeding with the change. The appointed leader of the Change Management Committee may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate backout plans, security implications, the timing of the change will negatively impact a key business process such as year-end accounting, or adequate resources cannot be readily available (e.g. weekends, holidays, or during special events).

Resource owners shall be notified for each scheduled or unscheduled change. A change review must be completed for each change, whether scheduled or unscheduled, and whether successful or unsuccessful. A Change Management Log Form shall be maintained for all changes. This log must contain, but is not limited to:

* Date of submission and date of change
* Owner and custodian contact information
* Nature of the change
* Indication of success or failure

Change management procedures shall:

* Ensure that production data is not unnecessarily replicated or used in non-production environments.
* Device configuration is backed up prior to implementing the change.

# 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 ABC Company Department Heads and those responsible for information system security.

**Policy History**

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

**References:**

COBIT APO05.03, APO05.05, APO11.09-10, BAI06.02, BAI06.05-06, BAI07.06, BAI10.07

GDPR Article 25

HIPAA 164.308(a)(4)(ii)(C), 164.308(a)(8), 164.316(a)

ISO 27001 A.12.1.2, A.14.2.2

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 CM-3, CM-5, CM-9, SA-10

NIST Cybersecurity Framework ID.RA-2, ID.RA-6, ID.RM-1, PR.IP-3, DE.DP-2

PCI 6.4