Problem 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

This Policy provides direction and guidance on managing problems that can disrupt ABC Company’s operations and/or adversely affect our image and reputation.

# II. Purpose

This Policy is established to prevent and detect problems and incidents. Where incidents cannot be prevented, this Policy identifies processes to address the problems and minimize the impact on our organization.

# III. Scope

This Policy applies to all individuals who manage and are responsible for ABC Company’s Information Resources.

# IV. Policy

The Chief Security Officer (CSO) shall ensure:

* Help desk or other teams are assembled to receive notice of problems and manage the process of investigating, responding to, and reporting of problems.
* Procedures and processes identify and respond to suspected or known problems, mitigate them to the extent practicable, measure harmful effects of known problems, document problems and their outcomes, collect evidence, and provide appropriate reporting to ABC Company management.
* Response procedures list examples of problems and the appropriate responses for each.

A. Background

The primary objective of problem management is to prevent issues and incidents, reduce the likelihood of incidents, and minimize the impact of an incident. Problem management includes diagnosis of a problem to identify the root cause of an incident and determine the resolution.

Major problem management steps include:

* Problem detection – Help Desk captures relevant information such as person/system reporting the issue, date/time, systems involved, actions taken, etc.
* Problem analysis – determine the underlying issue, impact on the organization, and possible resolution. Document activities planned and taken.
* Problem logging – details of the problem are recorded so that a record and audit trail exists.
* Problem prioritization – problems are prioritized according to their impact on our organization. The problem frequency, likelihood, workarounds, extent, resources required, cost, and other factors help determine priority.
* Problem investigation and diagnosis – appropriate Staff investigate and diagnose the problem to assist in identifying relevant issues. Important steps include preparing a chronological list of events that triggered the problem, identifying the target/size (number of systems, departments, etc.) impacted, location(s), and possible and true cause(s).
* Problem History Data Base – the event is logged in a Problem History Data Base (Data Base). The Data Base is used to identify and reduce the likelihood of future similar events and to quickly resolve similar issues.
* Problem communications – Help Desk keeps all relevant parties updated on the status of the problem and expected resolution dates. Relevant parties include, but not limited to, the individual that reported the problem as well as the CSO and upper management (if the issue has a major impact on the organization).
* Problem review – the CSO ensures a periodic review of the Problem History Data Base is performed. Such review identifies opportunities to minimize future incidents and their impact on our organization.

B. Preventive Controls

The CSO shall identify preventive controls that help prevent problems and incidents. When problems occur, preventive controls help contain and minimize the impact on business operations. Examples of preventive controls are listed below.

Only users with special training or a need for additional access shall be allowed to change system settings and install programs that are not operating system programs. For more information see the User Privilege Policy.

Network documentation helps ABC Company adhere to industry best practices, reduce downtime and makes the troubleshooting process more efficient when problems arise. For more information see the Network Documentation Policy.

Before approving updates, System Administrators shall understand the addressed vulnerability, previous patches or system update required, programs affected by the change, and problems that may result as a result of the change. For more information see the System Update Policy.

Periodic backup copies of software and data shall be made, tested, and stored securely. The physical security of the removable media must be maintained with plans to allow recovery from unexpected problems. For more information see the Security Policy.

Hard drives that are not fully encrypted (e.g., have encrypted partitions, virtual disks, or are unencrypted) that connect to unencrypted (e.g. USB drives) may be vulnerable to information spillage from the encrypted region into the unencrypted region. The hard drive’s unencrypted auto-recovery folder may retain files that have been saved to the encrypted portion of the disk or USB. Full disk encryption shall be implemented to avoid this problem. For more information see the Encryption Policy.

Vendors play an important role in the support of ABC Company hardware, software, and operations. Vendors can monitor and fine tune system performance, monitor hardware performance and errors, modify environmental systems, and reset alarm thresholds. For more information see the Vendor Access Policy.

Processes shall be in place to install and test all new/replacement software and hardware. Supervise all problem solving. Problem solving shall be supervised and documented. For more information see the Business Continuity Disaster Recovery Plan.

Staff shall follow approved procedures when dealing with copyright, trademark, and trade secrets. For more information see the Acceptable Use Policy.

C. Detective Controls

The CSO shall identify detective controls that detect problems and incidents. When problems occur, early detection can help contain and minimize the impact on business operations. Examples of detective controls are listed below.

Compliance tracking shall be used to map programs and activities to standards established by the CSO. Reports shall be generated and used to identify gaps or problems so that the appropriate corrective action can be taken. For more information see the Security Awareness and Training Plan.

Application logs help identify security incidents, establish baselines, provide information about problems and unusual conditions, assist with incident investigation, and help detect attacks. The CSO shall identify application events and activities to monitored and logged. For more information see the Logging Policy.

The IT Department shall be responsible for establishing, communicating and enforcing department level practices and procedures that promote security. Account auditing shall identify accounts that no longer have authorized access to ABC Company's Information Resources. The IT Department shall identify and correct problems caused on any network or system under their control. For more information see the IT Management Policy.

Resource monitoring and problem identification processes shall use audit trails to detect disk failures, over utilization of system resources, network outages, and similar events. Auditing systems shall consist of logging (collecting and recording events) and reporting (data analysis and reporting). For more information see the Audit Trails Policy.

Testing provides assurance that backups are complete and error free. Backups shall be tested to identify problems and issues related to the inability to restore from media. Such problems may include older media, poor quality, not properly stored, current backup software cannot read old backups, applications or data were not stored on original backups, encryption or key management issues (can’t read encrypted backups), etc. For more information see the Backup Plan.

The Emergency Action Applications Team shall participate in preparing and conducting tests at the Contingency Site. If a problem exists on how an application will operate at the Contingency Site, the Emergency Action Applications Team must prepare and document solutions for the problem. For more information see the Business Continuity Disaster Recovery Plan.

Effective privacy protection shall include robust mechanisms for assuring compliance with privacy principles and recourse for individuals who are affected by non-compliance with privacy principles. Processes shall include obligations to remedy problems arising out of failure to comply with privacy principles. For more information see the EU Privacy and Data Protection Policy.

D. Corrective Controls

The CSO shall identify corrective controls that mitigate problems and restore operations. When problems occur, early correction can help contain minimize the impact on business operations. Examples of corrective controls are listed below.

The appropriate system-level or application-level administrator should review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem. For more information see the Audit Trails Policy.

Software manufacturers frequently provide bug fixes and software patches for known problems. In-house change control procedures shall developed to provide for adequate testing before making changes and for backing out the changes if problems are detected. Should bug fixes or software patches cause a failure of software or network services, the Contingency Site Coordinator shall take the appropriate action to correct the problem either by authorizing a manufacturer-provided "fix" or by designating that the software be returned to the version prior to loading the changes. Some of ABC Company’s applications packages were acquired from third-party sources and are maintained by those companies. These vendors can assist in correcting application problems. For more information see the Business Continuity Disaster Recovery Plan.

If a severe incident occurs, the Emergency Coordinator shall determine the severity of the problem and decide on the appropriate action. All recovery teams will be asked if they are aware of other information or circumstances that need to be considered. The teams should collectively discuss all of the basic aspects of the situation, and considerations of problems due to the processing schedule or anything else, before proceeding to carry out their individual team functions. This is important to ensure that all teams understand the key issues which will result in better coordination. The final activity of the recovery process will be a meeting and debriefing of the Readiness Team, all Coordinators, and Emergency Action Team Leaders concerning the activities of the recovery. The Emergency Coordinator is responsible to ensure that events, problems, solutions, etc., are documented. For more information see the Business Continuity Disaster Recovery Plan and Business Continuity Business Resumption Plan.

E. Training

The CSO is responsible for ensuring that IT Department Staff have the proper training and appropriate problem management policies, procedures, plans and related documents. No less than annually, awareness and refresher training shall be provided to maintain problem management readiness and competency. The CSO may also arrange problem management exercises to test and evaluate Staff, related procedures, and the ability to respond to problems in a timely and effective manner.

# 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 the Chief Security Officer, Company Management, Director of IT, Help Desk, and Security Staff.

**Policy History**

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

**References:**

COBIT EDM01.03, EDM02.03, EDM03.07, EDM05.10, BAI09.04, DSS01.05, DSS03.05

GDPR Article 30, 32

HIPAA 1164.308(a)(1)(ii)(D), 164.308(a)(6)(ii), 164.312(b), 164.312(e)(2)(i), 164.312(e)(2)(ii)

ISO 27001:2013 6.2, 7.5, A.16

NIST SP 800-37 3.1, 3.2, 3.3, 3.4, 3.7

NIST SP 800-53 AU-2, CP-2, IR-8, PL-2, PM-1, RA-3, SA-8

NIST Cybersecurity Framework ID.AM-5, ID.BE-4, ID.RA-1, ID.RA-6, PR.PT-1, DE.AE-2

PCI 1.1.1, 8.4, 10.8.1, A3.3.1.1