Capacity and Utilization 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

Capacity and utilization safeguards are part of ABC Company’s risk management process to mitigate and reduce risks that can impact business operations and Information Resource availability.

# II. Purpose

Capacity planning and utilization helps ABC Company obtain maximum value from its Information Resources. In addition, planning ensures Information Resources meet current and projected needs.

# III. Scope

This Policy applies to the Chief Security Officer, IT Director, and IT Operations Manager.

# IV. Policy

For the purposes of this Policy, capacity and resource utilization is the extent to which ABC Company uses its Information Resources. It is the relationship between output actually produced and the potential output that could be produced if Information Systems were fully used.

ABC Company’s Chief Security Officer (CSO) is responsible for ensuring that security controls and safeguards are appropriate, sufficient, and effective at treating risks. The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance. The CSO shall:

* Resources – identify important resources that should be monitored and measured.
* Requirements – prepare a list of capacity constraints that are relevant to important resources.
* Monitoring – describe the required resource monitoring, alerts to be issued, and actions to be taken.

The CSO shall consider the following when determining the types of monitoring to be used:

* Automated tools – automated tools may be used to monitor capacity and utilization.
* Safeguards – review and evaluate policies, procedures, training plans and related controls and safeguards.
* Testing – testing may be used to identify system capacities and constraints.
* Monitoring logs – logs shall be controlled and restricted to prevent possible misuse or compromise of Information Resources and log data.

The CSO shall rely on the IT Department to review and document utilization statistics on data center equipment. Inefficient use of server resources shall be brought to the attention of the IT Director. See the Green Computing Policy for more information.

* The IT Department shall measure current capacity and performance on important resources identified by the CSO. Measurements may be achieved through analysis of reports as well as statistical information produced by servers, firewalls, and related equipment. In addition, performance may also be measured using monitoring equipment.
* Resource monitoring and problem identification may use audit trails to detect disk failures, over utilization of system resources, network outages, and similar events. See the Audit Trails Policy for more information.
* The IT Operations Department is responsible for developing and maintaining backup procedures. Such procedures include notifying the System Administrator of any issues that require attention (e.g. failed backups, capacity issues, time to backup files, etc.). Since backups run unattended without operators present, sufficient storage capacity needs to be allocated for backups/media. See the Backup Plan for more information.
* The IT Department shall establish monitoring systems that can detect new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include audit compliance, service level monitoring, performance measuring, and capacity planning. See the Security Monitoring Policy for more information.

The CSO shall provide necessary capacity and utilization reporting to ABC Company Executive Management on an as needed basis.

# 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 the CSO, IT Director, and IT Operations Manager.

**Policy History**

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

**References:**

COBIT EDM03.02, APO09.05, BAI04.05, BAI04.07, DSS01.05, DSS03.05, MEA01.05

GDPR Article 25, 32

HIPAA 164.308(a)(7)(ii)(E), 164.308(a)(8)

ISO 27001 A.12.1.3

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 AU-4, AU-5(1), CP-2(2), SC-5(2)

NIST Cybersecurity Framework PR.DS-4, DE.DP-2

PCI 1.1.2, 1.1.5, 1.1.6, 1.2.1, 2.2