Availability Policy

ACME Evil Anvil Corporation

March 2019

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	A1.1, CC9.1

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. The purpose of this policy is to define requirements for proper controls to protect the availability of the organization's information systems.

b. This policy applies to all users of information systems within the organization. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information controlled by the organization (hereinafter referred to as "users"). This policy must be made readily available to all users.

2 Background

a. The intent of this policy is to minimize the amount of unexpected or unplanned downtime (also known as outages) of information systems under the organization's control. This policy prescribes specific measures for the organization that will increase system redundancy, introduce failover mechanisms, and implement monitoring such that outages are prevented as much as possible. Where they cannot be prevented, outages will be quickly detected and remediated.

b. Within this policy, an availability is defined as a characteristic of information or information systems in which such information or systems can be accessed by authorized entities whenever needed.

3 References

a. Risk Assessment Policy

4 Policy

a. Information systems must be consistently available to conduct and support business operations.

b. Information systems must have a defined availability classification, with appropriate controls enabled and incorporated into development and production processes based on this classification.

c. System and network failures must be reported promptly to the organization's lead for Information Technology (IT) or designated IT operations manager.

d. Users must be notified of scheduled outages (e.g., system maintenance) that require periods of downtime. This notification must specify the date and time of the system maintenance, expected duration, and anticipated system or service resumption time.

e. Prior to production use, each new or significantly modified application must have a completed risk assessment that includes availability risks. Risk assessments must be completed in accordance with the Risk Assessment Policy (reference (a)).

f. Capacity management and load balancing techniques must be used, as deemed necessary, to help minimize the risk and impact of system failures.

g. Information systems must have an appropriate data backup plan that ensures:

    i. All sensitive data can be restored within a reasonable time period.

    ii. Full backups of critical resources are performed on at least a weekly basis.

    iii. Incremental backups for critical resources are performed on at least a daily basis.

    iv. Backups and associated media are maintained for a minimum of thirty (30) days and retained for at least one (1) year, or in accordance with legal and regulatory requirements.

    v. Backups are stored off-site with multiple points of redundancy and protected using encryption and key management.

    vi. Tests of backup data must be conducted once per quarter. Tests of configurations must be conducted twice per year.

h. Information systems must have an appropriate redundancy and failover plan that meets the following criteria:

    i. Network infrastructure that supports critical resources must have system-level redundancy (including but not limited to a secondary power supply, backup disk-array, and secondary computing system). Critical core components (including but not limited to routers, switches, and other devices linked to Service Level Agreements (SLAs)) must have an actively maintained spare. SLAs must require parts replacement within twenty-four (24) hours.

    ii. Servers that support critical resources must have redundant power supplies and network interface cards. All servers must have an actively maintained spare. SLAs must require parts replacement within twenty-four (24) hours.

    iii. Servers classified as high availability must use disk mirroring.

i. Information systems must have an appropriate business continuity plan that meets the following criteria:
    i. Recovery time and data loss limits are defined in Table 3.
    ii. Recovery time requirements and data loss limits must be adhered to with specific documentation in the plan.
    iii. Company and/or external critical resources, personnel, and necessary corrective actions must be specifically identified.
    iv. Specific responsibilities and tasks for responding to emergencies and resuming business operations must be included in the plan.
    v. All applicable legal and regulatory requirements must be satisfied.

Availability Classification	**Availability Requirements**	**Scheduled Outage**	**Recovery Time Requirements**	**Data Loss or Impact Loss**
High	High to Continuous	30 minutes	1 hour	Minimal
Medium	Standard Availability	2 hours	4 hours	Some data loss is tolerated if it results in quicker restoration
Low	Limited Availability	4 hours	Next business day	Some data loss is tolerated if it results in quicker restoration

Table 3: Recovery Time and Data Loss Limits