Data Retention Policy

ACME Evil Anvil Corporation

January 2019

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC1.2, CC6.5, P4.2

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

#Appendices Appendix A: Retention Periods

1 Purpose and Scope

a. This data retention policy defines the objectives and requirements for data retention within the organization.

b. This policy covers all data within the organization's custody or control, irregardless of the medium the data is stored in (electronic form, paper form, etc.) Within this policy, the medium which holds data is referred to as information, no matter what form it is in.

c. 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 the organization owns or controls (hereinafter referred to as "users"). This policy must be made readily available to all users.

2 Background

a. The organization is bound by multiple legal, regulatory and contractual obligations with regard to the data it retains. These obligations stipulate how long data can be retained, and how data must be destroyed. Examples of legal, regulatory and contractual obligations include laws and regulations in the local jurisdiction where the organization conducts business, and contracts made with employees, customers, service providers, partners and others.

b. The organization may also be involved in events such as litigation or disaster recovery scenarios that require it to have access to original information in order to protect the organization's interests or those of its employees, customers, service providers, partners and others. As a result, the organization may need to archive and store information for longer that it may be needed for day-to-day operations.

3 Policy

a. *Information Retention*

   i. Retention is defined as the maintenance of information in a production or live environment which can be accessed by an authorized user in the ordinary course of business.

   ii. Information used in the development, staging, and testing of systems shall not be retained beyond their active use period nor copied into production or live environments.

   iii. By default, the retention period of information shall be an active use period of exactly two years from its creation unless an exception is obtained permitting a longer or shorter retention period. The business unit responsible for the information must request the exception.

   iv. After the active use period of information is over in accordance with this policy and approved exceptions, information must be archived for a defined period. Once the defined archive period is over, the information must be destroyed.

   v. Each business unit is responsible for the information it creates, uses, stores, processes and destroys, according to the requirements of this policy. The responsible business unit is considered to be the information owner.

   vi. The organization's legal counsel may issue a litigation hold to request that information relating to potential or actual litigation, arbitration or other claims, demands, disputes or regulatory action be retained in accordance with instructions from the legal counsel.

   vii. Each employee and contractor affiliated with the company must return information in their possession or control to the organization upon separation and/or retirement.

   viii. Information owners must enforce the retention, archiving and destruction of information, and communicate these periods to relevant parties.

b. *Information Archiving*

   i. Archiving is defined as secured storage of information such that the information is rendered inaccessible by authorized users in the ordinary course of business but can be retrieved by an administrator designated by company management.

      1. Physical (e.g., paper) records must be archived in secured storage (onsite or offsite) and clearly labeled in archive boxes naming the information owner.

2. Electronic records must be archived with strict access controls set by the information owner and appropriate to secure the confidentiality, integrity and accessibility of the information.

ii. The default archiving period of information shall be 7 years unless an approved exception permits a longer or shorter period. Exceptions must be requested by the information owner.

1. As a guideline, an archiving period of more than 7 years may be granted for information with a vital historical purpose such as corporate records, contracts, and technical/trade secrets.

2. As a guideline, an archiving period of less than 7 years may be granted for information with a limited business purpose such as email, travel itineraries, pre-trip advisories, or to comply with specific legal, contractual and/or regulatory requirements (e.g., PCI DSS, GDPR, etc.)

iii. Information must be destroyed (defined below) at the end of the elapsed archiving period.

c. *Information Destruction*

i. Destruction is defined as the physical or technical destruction sufficient to render the information contained in the document irretrievable by ordinary commercially-available means.

ii. The organization must maintain and enforce a detailed list of approved destruction methods appropriate for each type of information archived, whether in physical storage media such as CD-ROMs, DVDs, backup tapes, hard drives, mobile devices, portable drives or in database records or backup files. Physical information in paper form must be shredded using an authorized shredding device; waste must be periodically removed by approved personnel.

d. Retention and archival periods for information that is created, processed, stored and used by the organization is defined in Appendix A, “Retention Periods.”

4 Appendix A: Retention Periods

Information Type	Information Owner	Storage Location	Retention Period	Archival Period