Data Classification Policy

ACME Evil Anvil Corporation

January 2019

Contents

1 Appendices **2**

2 Purpose and Scope **2**

3 Background **2**

4 References **2**

5 Policy **2**

6 Appendix A: Handling of Classified Information **6**

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Appendices

Appendix A: Handling of Classified Information

Appendix B: Form - Confidentiality Statement

2 Purpose and Scope

a. This data classification policy defines the requirements to ensure that information within the organization is protected at an appropriate level.

b. This document applies to the entire scope of the organization's information security program. It includes all types of information, regardless of its form, such as paper or electronic documents, applications and databases, and knowledge or information that is not written.

c. This policy applies to all individuals and systems that have access to information kept by the organization.

3 Background

a. This policy defines the high level objectives and implementation instructions for the organization's data classification scheme. This includes data classification levels, as well as procedures for the classification, labeling and handling of data within the organization. Confidentiality and non-disclosure agreements maintained by the organization must reference this policy.

4 References

a. Risk Assessment Policy

b. Security Incident Management Policy

5 Policy

a. If classified information is received from outside the organization, the person who receives the information must classify it in accordance with the rules prescribed in this policy. The person thereby will become the owner of the information.

b. If classified information is received from outside the organization and handled as part of business operations activities (e.g., customer data on provided cloud services), the information classification, as well as the owner of such information, must be made in accordance with the specifications of the respective customer service agreement and other legal requirements.

c. When classifying information, the level of confidentiality is determined by:

   i. The value of the information, based on impacts identified during the risk assessment process. More information on risk assessments is defined in the Risk Assessment Policy (reference (a)).

   ii. Sensitivity and criticality of the information, based on the highest risk calculated for each information item during the risk assessment.

   iii. Legal, regulatory and contractual obligations.

Confidentiality Level	**Label**	**Classification Criteria**	**Access Restrictions**
Public	For Public Release	Making the information public will not harm the organization in any way.	Information is available to the public.
Internal Use	Internal Use	Unauthorized access may cause minor damage and/or inconvenience to the organization.	Information is available to all employees and authorized third parties.
Restricted	Restricted	Unauthorized access to information may cause considerable damage to the business and/or the organization's reputation.	Information is available to a specific group of employees and authhorized third parties.
Confidential	Confidential	Unauthorized access to information may cause catastrophic damage to business and/or the organization's reputation.	Information is available only to specific indivi- duals in the organization.

Table 3: Information Confidentiality Levels

d. Information must be classified based on confidentiality levels as defined in Table 3.

e. Information and information system owners should try to use the lowest confidentiality level that ensures an adequate level of protection, thereby avoiding unnecessary production costs.

f. Information classified as “Restricted” or “Confidential” must be accompanied by a list of authorized persons in which the information owner specifies the names or job functions of persons who have the right to access that information.

g. Information classified as “Internal Use” must be accompanied by a list of authorized persons only if individuals outside the organization will have access to the document.

h. Information and information system owners must review the confidentiality level of their information assets every five years and assess whether the confidentiality level should be changed. Wherever possible, confidentiality levels should be lowered.

i. For cloud-based software services provided to customers, system owners under the company’s control must also review the confidentiality level of their information systems after service agreement changes or after a customer’s formal notification. Where allowed by service agreements, confidentiality levels should be lowered.

j. Information must be labeled according to the following:

    i. Paper documents: the confidentiality level is indicated on the top and bottom of each document page; it is also indicated on the front of the cover or envelope carrying such a document as well as on the filing folder in which the document is stored. If a document is not labeled, its default classification is Internal Use.

    ii. Electronic documents: the confidentiality level is indicated on the top and bottom of each document page. If a document is not labeled, its default classification is Internal Use.

    iii. Information systems: the confidentiality level in applications and databases must be indicated on the system access screen, as well as on the screen when displaying such information.

    iv. Electronic mail: the confidentiality level is indicated in the first line of the email body. If it is not labeled, its default classification is “Internal Use”.

v. Electronic storage media (disks, memory cards, etc.): the confidentiality level must be indicated on the top surface of the media. If it is not labeled, its default classification is "Internal Use".

vi. Information transmitted orally: the confidentiality level should be mentioned before discussing information during face-to-face communication, by telephone, or any other means of oral communication.

k. All persons accessing classified information must follow the guidelines listed in Appendix A, "Handling of Classified Information."

l. All persons accessing classified information must complete and submit a Confidentiality Statement to their immediate supervisor or company point-of-contact. A sample Confidentiality Statement is in Appendix B.

m. Incidents related to the improper handling of classified information must be reported in accordance with the Security Incident Management Policy (reference (b)).

6 Appendix A: Handling of Classified Information

Information and information systems must be handled according to the following guidelines*:

a. Paper Documents
    i. Internal Use
        1. Only authorized persons may have access.
        2. If sent outside the organization, the document must be sent as registered mail.
        3. Documents may only be kept in rooms without public access.
        4. Documents must be removed expeditiously from printers and fax machines.
    ii. Restricted
        1. The document must be stored in a locked cabinet.
        2. Documents may be transferred within and outside the organization only in a closed envelope.
        3. If sent outside the organization, the document must be mailed with a return receipt service.
        4. Documents must immediately be removed from printers and fax machines.
        5. Only the document owner may copy the document.
        6. Only the document owner may destroy the document.
    iii. Confidential
        1. The document must be stored in a safe.
        2. The document may be transferred within and outside the organization only by a trustworthy person in a closed and sealed envelope.
        3. Faxing the document is not permitted.
        4. The document may be printed only if the authorized person is standing next to the printer.

b. Electronic Documents
    i. Internal Use
        1. Only authorized persons may have access.

2. When documents are exchanged via unencrypted file sharing services such as FTP, they must be password protected.
3. Access to the information system where the document is stored must be protected by a strong password.
4. The screen on which the document is displayed must be automatically locked after 10 minutes of inactivity.

ii. Restricted

1. Only persons with authorization for this document may access the part of the information system where this document is stored.
2. When documents are exchanged via file sharing services of any type, they must be encrypted.
3. Only the document owner may erase the document.

iii. Confidential

1. The document must be stored in encrypted form.
2. The document may be stored only on servers which are controlled by the organization.
3. The document may only be shared via file sharing services that are encrypted such as HTTPS and SSH. Further, the document must be encrypted and protected with a string password when transferred.

c. Information Systems

i. Internal Use

1. Only authorized persons may have access.
2. Access to the information system must be protected by a strong password.
3. The screen must be automatically locked after 10 minutes of inactivity.
4. The information system may be only located in rooms with controlled physical access.

ii. Restricted

1. Users must log out of the information system if they have temporarily or permanently left the workplace.
2. Data must be erased only with an algorithm that ensures secure deletion.

iii. Confidential

1. Access to the information system must be controlled through multi-factor authentication (MFA).
2. The information system may only be installed on servers controlled by the organization.
3. The information system may only be located in rooms with controlled physical access and identity control of people accessing the room.

d. Electronic Mail

   i. Internal Use

      1. Only authorized persons may have access.
      2. The sender must carefully check the recipient.
      3. All rules stated under “information systems” apply.

   ii. Restricted

      1. Email must be encrypted if sent outside the organization.

   iii. Confidential

      1. Email must be encrypted.

e. Electronic Storage Media

   i. Internal Use

      1. Only authorized persons may have access.
      2. Media or files must be password protected.
      3. If sent outside the organization, the medium must be sent as registered mail.
      4. The medium may only be kept in rooms with controlled physical access.

   ii. Restricted

      1. Media and files must be encrypted.
      2. Media must be stored in a locked cabinet.
      3. If sent outside the organization, the medium must be mailed with a return receipt service.
      4. Only the medium owner may erase or destroy the medium.

   iii. Confidential

      1. Media must be stored in a safe.

2. Media may be transferred within and outside the organization only by a trustworthy person and in a closed and sealed envelope.

f. Information Transmitted Orally

i. Internal Use

1. Only authorized persons may have access to information.

2. Unauthorized persons must not be present in the room when the information is communicated.

ii. Restricted

1. The room must be sound-proof.

2. The conversation must not be recorded.

iii. Confidential

1. Conversation conducted through electronic means must be encrypted.

2. No transcript of the conversation may be kept.

In this document, controls are implemented cumulatively, meaning that controls for any confidentiality level imply the implementation of controls defined for lower confidentiality levels - if stricted controls are prescribed for a higher confidentiality level, then only such controls are implemented.