DATA CLASSIFICATION

THE DATA CLASSIFICATION IS A PART OF THE PPHS CYBERSECURITY STANDARD FOR SMALL AND MEDIUM-SIZED ENTERPRISES AND PUBLIC INSTITUTION DEVELOPED BY THE POLISH PLATFORM FOR HOMELAND SECURITY.

TABLE OF CONTENTS

03

WHAT IS THE CLASSIFICATION OF INFORMATION AND WHAT IS IT FOR?

- Classification of information is the grouping of information resources/assets according to criteria depending on their importance to the organization and environment.

- It allows to identify and mark the most important resources/assets and thus, ensure effective protection. This is due to the fact that safeguards and basic methods are defined for each category.

- A well executed classification of resources/assets allows all employees (and external stakeholders) to handle information properly - including the implementation of adequate protection measures.

- A well executed classification of information also allows for a better risk assessment process.

04

GUIDELINES FOR PREPARING THE CLASSIFICATION

- There is no one universal method to develop a classification of information that fits all types of entities.

- Taking into account the specific considerations of each organization, each entity should create its own classification system or adapt existing models.

NOTE

There are regulations that impose rules for the classification of information assets/resources and indicate very specific security mechanisms. An example is the protection of confidential information. Naturally, in this case, the organization is required to follow those legal guidelines. Therefore, only the assets/resources that are not covered by the regulations which specify particular security activities, should be classified. The classification should complement (and not replace) the legally required security mechanisms.

05

GUIDELINES FOR PREPARING THE CLASSIFICATION

- A particular nomenclature used while designing the classification system, should not be misleading - e.g. 'top secret' should not be used (used in the protection system of classified information) when the organization does not process legally protected classified information.

- Apart from taking into account the requirements resulting from common legal regulations, when building the classification, the organization should take into account other requirements resulting from e.g. contractual obligations concerning protection of information according to the specifications of the client or a business partner.

- The classification must be understandable for all users, not too complicated, so that all employees can easily apply it. At the same time, it should not be too general.

- The creation of a classification system is a continuous process that should be improved over time.

- Classification should be formulated considering three main security attributes:

    - Confidentiality - protection of information assets/resources from entities that should not have access to them.
    - Integrity - protection of information assets/resources against unauthorized or random changes and damage.
    - Accessibility - ensure that an authorized person can have access to the information asset/resource whenever it is needed.

06

WHAT STEPS SHOULD BE TAKEN TO CREATE A CLASSIFICATION

STEP 1

USE THE REGISTER OF INVENTORY ASSETS / INFORMATION RESOURCES
(STAGE 1 PPHS STANDARD)

STEP 2

DEFINE CATEGORIES FOR GROUPS OF ASSETS / INFORMATION RESOURCES IN THE ORGANIZATION

STEP 3

DEFINE SAFETY MEASURES AND WAYS OF HANDLING ASSETS / RESOURCES ASSIGNED FOR EACH CATEGORY

STEP 4

ASSIGN CATEGORIES TO PREVIOUSLY IDENTIFIED RESOURCES
(MARK THEM)

07 EXEMPLIFICATORY CLASSIFICATION

An example of a three-tier classification of information with an illustration of which resource/asset could be included in each category, can be found bellow.

The classification also includes examples of requirements regarding security handling.

CATEGORY: SENSITIVE INFORMATION

DESCRIPTION/EXPLANATION

Unauthorized access to information assets/ resources in this category (especially by external entities), lack of access when it is needed (e.g. due to damage), unauthorized change of them could have a very negative impact on the organization and/or its collaborators (e.g. customers, business partners).

Those very negative consequences may include e.g. significant financial losses, tarnishing the brand image, or even a threat to the safety of some people.

A breach of information asset/resources security may constitute a breach of legal requirements or contractual obligations.

EXAMPLE

Security related data (e.g. login data, passwords, configuration data, incident information).

Special categories of personal data (e.g. health, individual financial situation, biometric data).

Business and financial data:
(e.g. negotiation strategies, secret project plans, credit card data, accounting data e.g. salaries, tax returns, data related to tenders).

Confidential agreements and terms of cooperation with clients and contractors.

PROTECTION

Access: only persons (may be categories of persons/functions) with written authorization from the Board of Management

Authentication: two-stage user verification

Transmission: only to persons or entities on a list approved by the Board of Management

Encryption: information may only be transmitted using encrypted transmission channels

Backup: every day

Destruction: in a way that makes recovery impossible

08

EXEMPLIFICATORY CLASSIFICATION

CATEGORY: INFORMATION FOR INTERNAL USE ONLY

DESCRIPTION/EXPLANATION

The information assets/ resources should only be used for the organization's internal use and needs.

These are not critical resources/assets related to the day-to-day operation of the organization, but at the same time, they should be protected with a chosen method.

Confidentiality, availability and integrity issues could impede the effective functioning of the organization.

They should not be disclosed to anyone outside the organization without permission.

EXAMPLE

- Personal data (except special categories of personal data)
- Internal regulations and internal policies
- Memos
- Procedures
- Contract templates
- Customer databases
- Task management tools

PROTECTION

Access: access for a person (may be categories of persons/functions) approved by the owner of the resource.

Authentication: two-stage user verification

Transmission: only to persons or entities on a list approved by the owner of the resource.

Encryption: required for transmission to external entities.

Backup: every week.

Destruction: in a way that makes recovery impossible

09

EXEMPLIFICATORY CLASSIFICATION

CATEGORY: PUBLIC INFORMATION

DESCRIPTION/EXPLANATION

Information assets/ resources that can (or in some cases should) be made publicly available and distributed without restriction.

EXAMPLE

- Advertising.
- Company promotion information.
- Official price lists.
- Website.

PROTECTION

Access: unlimited.

Authentication: none

Transmission: discretionary

Encryption: none

Backup: once a month

Destruction: no special requirements

10

MORE INFORMATION ON THE CLASSIFICATION:

S. Fowler, Information Classification -Who, Why and How, SANS Institute, 2019.

ISO27k Forum at www.ISO27001security.com.

POLISH PLATFORM
FOR HOMELAND SECURITY

Polish Platform for Homeland Security

ul. Slowackiego 17/11
60-822 Poznań
www.ppbw.pl/en
tel.: +48 (61) 663 02 21
e-mail: standard-cyber@ppbw.pl

European Funds Smart Growth

Republic of Poland

European Union
European Regional Development Fund

The project "Cybersecurity – PPHS Standard for SME and public institutions" was financed by the European Regional Development Fund.