Data Classification Policy

Beyond

August 2023

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
Aug 14 2023	Initial document
Aug 18 2023	Initial review

1 Appendices

Appendix A: Handling of Classified Information

2 Purpose and Scope

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

b. This document applies to the entire scope of Beyond's information security program. It includes all types of information, regardless of its form, such as 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 Beyond.

3 Background

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

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

Table 3: Information Confidentiality Levels

a. Information must be classified based on confidentiality levels as defined in Table 3. Classification must be made available and kept up-to-date by the owner in the Data Classification Matrix. *Internal access only*

b. 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.

c. Information classified as "Internal" or "Restricted" must be accompanied by a list of authorized roles or individuals in which the information owner specifies the names or job functions of persons who have the right to access that information.

d. 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.

e. 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.

f. Information must be labeled according to the following:

   i. Paper documents: Printing of "Internal" and "Restricted" information is considered unacceptable 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 within the Data Classification Matrix. *Internal access only*

   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 video conference, or any other means of oral communication.

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

h. All third parties accessing "Internal" or "Restricted" information must be governed under a Beyond vetted Non Disclosure Agreement.

i. All persons accessing classified information must complete and submit a Confidentiality Statement to their immediate supervisor or company point-of-contact.

j. 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 and Restricted
        1. Printing of “Internal” and “Restricted” information is considered unacceptable use.

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 15 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.

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 15 minutes of inactivity.
    ii. Restricted
        1. Data must be erased only with an algorithm that ensures secure deletion.

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.
4. Email system must warn the user when sharing documents if sent outside Beyond.

ii. Restricted

1. Email must be encrypted if sent outside Beyond.

e. Electronic Storage Media

i. Internal Use

1. Only authorized persons may have access.
2. If sent outside Beyond, the medium must be sent as registered mail.

ii. Restricted

1. Media and files must be encrypted.
2. Media or files must be password protected.
3. If sent outside Beyond, the medium must be mailed with a return receipt service.
4. Only the medium owner may erase or destroy the medium.

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.

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.