Standard
Mandatory
General Use
June 2018

St

Nestlé
Good Food, Good Life

Information Classification Standard

Standard
Mandatory
General Use
June 2018

St

Issuing department
Group Legal / Group Compliance

Target audience
All Employees

Approver
Executive Board Nestlé S.A

Repository
All Nestlé Principles and Policies, Standards and Guidelines can be found in *NestleDocs*, on the Nest

Design
Nestec Ltd., Corporate Identity & Design,
Vevey, Switzerland

Introduction

The efficient use and appropriate safeguarding of an ever-increasing amount of information are important for the success of our Company. The degree to which information needs to be protected varies and depends mostly on the sensitivity of its content. This Standard describes the different Information Classification levels that are to be used at Nestlé.

This Standard applies to Information Assets created after the date of approval of the Standard. Information Assets created before the date of this Standard will continue under the regulation of the previous Standard. It is not necessary to revise their classification unless they are otherwise updated or modified.

Guidelines will be developed to facilitate implementation of this Standard. Tools will be provided to ensure easy and efficient classification, labelling and protection of information.

Scope

All Nestlé Information is subject to classification, irrespective of format. Documents or Information Assets that are not otherwise classified will be considered General Use.

Markets may deviate from this Standard if advised to do so by the Legal function due to local legal requirements.

Employees are permitted to have non-business information on Company devices for personal use only. Unless applicable local laws and regulations specify otherwise, non-business documents and Information are not exempt from investigations or legal searches.

In parallel to this Information Classification Standard, other criteria may apply to the labeling of documents. For example, in some countries the notion of "legal privilege" applies to communications with the legal function. In these cases, the required label should be added, upon the request of a Nestlé lawyer, along with the Information Classification category that applies to the document. In these cases, the document will be identifiable as either "Legally Privileged and Confidential" or "Legally Privileged and Highly Confidential".

Employees or contractors who come across Information Assets classified as Confidential or Highly Confidential (e.g. orphaned document at a printer, forgotten in a conference room, stored on an unprotected folder, etc.) must raise an Information Security Incident immediately.

Classification Levels

All Information Assets should be assigned to one of the following classification levels:

- Public
- General Use
- Confidential
- Highly Confidential

Public

Information Assets are classified "Public" if Nestlé makes the explicit decision to share them with the public. This classification may only be applied by business units that are authorized to do so.

General Use

This category applies to the majority of the Information Nestlé manages; this is Information required and created as part of our day-to-day activities.

General Use Information may be shared with Nestlé employees and contractors and with third parties external to Nestlé. However, when we share information or communicate with third parties outside Nestlé, it always important to consider the possible consequences or repercussions for Nestlé. It is our obligation to protect Nestlé Information and Nestlé corporate reputation.

Confidential

This category covers Sensitive Information that **could** cause damage if shared with unauthorized people. Information Assets that contain Personal Data should be classified as Confidential – Personal Data.

Confidential Information may be shared with (i) Nestlé employees and contractors; and (ii) third parties external to Nestlé that have signed a non-disclosure agreement.

The owner and the recipients of "Confidential" Information Assets distributed in paper assume responsibility for limiting the distribution on a "Need to know basis". In electronic form, "Confidential" Information must be subject to technical controls, when available, ensuring that the owner controls who has access to the Information.

Highly Confidential

This covers very Sensitive Information that would cause damage if shared with unauthorized people. It is recommended to consult legal before classifying an Information Asset as Highly Confidential. Information Assets that contain Sensitive Personal Data should be classified as Highly Confidential – Sensitive Personal Data.

Highly Confidential Information Assets may be shared with (i) Nestlé employees and contractors; and (ii) third parties external to Nestlé that have signed a non-disclosure agreement approved by the legal function.

Highly Confidential Information Assets in electronic form must be subject to additional technical controls, when available, ensuring that only pre-defined individuals can access the Information.

Highly Confidential Information Assets in paper form must be shared only with a pre-defined group of individuals.

Appendix - Definitions

Data – Raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized.

Information – The knowledge obtained from Data. Data carries Information, so when Data is processed, organized, structured or presented in a given context as to make it useful, it is called Information.

Information Assets – All documents and files created by or on behalf of Nestlé, irrespective of whether they are in electronic or paper form.

Information Classification – Assignment of a classification level to an Information Asset based on the Sensitivity of the Information carried by the Information Asset.

Personal Data – Information concerning an individual as an identified or identifiable person (e.g. name, address, telephone number, e-mail address, etc.). For clarification, this does not include the name, email address and contact information of the sender or recipients of the Information Asset.

Sensitive Information – Data or in most cases, Information which if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause financial and reputational harm to the organization. Note that the notion of Data sensitivity is not absolute but is time-dependent. As an example, Global Sales Data are very sensitive the day before publication of our annual results and therefore must be protected accordingly. The next day, this Information is public and not sensitive. Sensitive Information should be marked as either "Confidential" or "Highly Confidential" in accordance with the Classification Levels described in this Standard.

Sensitive Personal Data – Personal Data relating to the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, data concerning physical or mental health or sex life, or sexual orientation, the commission or alleged commission of any offense and any related proceedings and outcome thereof.