# Policy - Information Classification, Labeling and Handling

## Introduction

### 1. Scope

Information assets owned by GlobalLogic are classified, taking into account their legality, value, sensitivity and criticality to GlobalLogic.

### 2. Responsibilities

2.1 The owner of each asset is responsible for its classification, for ensuring it is correctly labelled and for its correct handling in line with its classification.

2.2 The intended recipient of any information assets sent from outside GlobalLogic becomes the owner of that asset.

2.3 System/Service/Application Owner is responsible for the technical labelling mechanisms of corporate systems and applications.

2.4 All users of organizational information assets have specific responsibilities identified in the **Policy - Acceptable Use**.

2.5 Asset owners are responsible for ensuring that mail/postal services, voicemail and voice communication, photocopiers, couriers, and sensitive documents are handled in line with information security policies, procedures and specific work instructions.

## Abbreviations and Definitions

| Abbreviation | Description |
|---|---|
| Service\System\Application Owner | The individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system. The owner is a key contributor in developing system design specifications to ensure the security and user operational needs are documented, tested, and implemented. |
| Personal Data | Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Information that could be reasonably used to identify an individual data subject, includes among others names, addresses, email addresses, telephone numbers, Social Security numbers, government identification numbers, IP or personal addresses, health data, or any other personally identifiable information which may enable to identify a person, individually or by |

combination and copies of such information, and materials derived from such information, and any other information associated with or linked to such information. Also described as “Personally Identifiable Information”.

# Description

## 3. Classification

3.1 GlobalLogic classifies information into four levels of classification (**public, confidential, restricted, secret**)

3.2 The classification level of an information asset is defined by originator/owner by placing a label on the asset.

3.3 The classification label included in the document footer at least, which is set to appear on all pages of the document.

3.4 Information received from outside of GlobalLogic is re-classified by its recipient (if he/she becomes its owner) so that, within GlobalLogic, it complies with this procedure.

3.5 The classifications of information assets are reviewed regularly by their owners and if the classification level can be reduced, it will be. The asset owner is responsible for declassifying information.

3.6 **Secret:** this classification applies to information that is specifically restricted to the Board of Directors, specific professional advisers and particular group of people.

3.6.1 Information that falls into this category must be marked ‘**GL Secret**’, and its circulation is kept to a minimum.

3.6.2 Examples of secret information might include information about potential acquisitions or corporate strategy, security information, including passwords and biometric data, know-hows, or about key organizational personnel, such as the Chief Executive Officer (CEO).

3.6.3 Secret information must be shared only to individuals known to be allowed to receive such information.

3.6.4 Secret information sent by e-mail must be approved by its owner, and sent only to the email box of the identified recipient.

3.6.5 Secret information can only be processed or stored on facilities which have been assessed as providing adequate security for such information.

3.6.6 The amount of information that falls into this category should be carefully limited; the cost and operational inconvenience of protecting it properly is such that it needs only to be information whose release can significantly damage GlobalLogic.

3.7 **Restricted:** information of this category is restricted to employees/consultants particular department, project, group, process.

3.7.1 Information that falls into this category must be marked ‘**GL Restricted**’

3.7.2 Examples of restricted information include technical, business, financial information, designs, specifications, drawings, reports, diagrams, production statistics and Personal Data.

3.7.3 Restricted information must be shared only to individuals known to be allowed to receive such information.

3.7.4 Restricted information sent by email must be approved by its owner, and sent only to the email box of the identified recipient.

3.7.5 Restricted information can only be processed or stored on facilities which have been assessed as providing adequate security for such information.

3.7.6 For the information restricted to the project/account, Project Manager/Project Director is responsible to translate the client's information classifications into this one and ensure appropriate handling of this information according to the client requirements (e.g. information encryption requirements, retention etc.)

3.8 **Confidential (Internal Information):** this classification covers all information assets that have value but which do not need to fall within either of the other categories. Information that is hosted on all GlobalLogic internal resources and available to employees/consultants, including Personal Data of GlobalLogic employees/consultants also falls into this category.

3.8.1 Information that falls into this category must be marked '**GL Confidential**'

3.8.2 Every employee/consultant of GlobalLogic is entitled to access information with this classification.

3.8.3 Confidential information must be shared only to individuals known to be allowed to receive such information.

3.9 **Public:** this is information which is authorized to be released outside GlobalLogic (including information deemed public by legislation or through a policy of routine disclosure) and its unauthorized disclosure would not cause any damage to the GlobalLogic, its employees/consultants and partners.

3.10 Access to secret, restricted and confidential (internal) information is granted to employees/consultants and non-employees, related parties with signed non-disclosure agreements who have a business need to know according to the established access control procedures.

## 4. Labeling

4.1 Documents are labelled as set out above, in the document footers or headers.

4.2 Electronic documents and information assets are labelled by the owner. Labeling mark has to be placed in such a way so that it is viewable and clearly shows the category of the information: included on every page of a document; included into a subject of an email, etc.

4.3 Some types of information (processed through information systems, databases, etc.) are non-markable and must be communicated as restricted or confidential in another appropriate way (through the applicable policies, instructions, emails, verbal communication etc.).

4.4 If GL logo is clearly presented in document or other information medium, "GL" letters from label may be neglected.

4.5 If information within databases and systems falls under different classifications levels, each type of information is classified separately by its owner and the level of its sensitivity is communicated to users.

4.6 Country level documents especially of legal matters (local agreements and its attachments, native language notes, instructions, training materials, any document in native language etc.) may contain labels made in native/local language only or bilingual labels.

4.7 All e-mails have a standard disclaimer on the footer to the effect that the views expressed in the email are those of the sender alone and do not reflect the views of GlobalLogic.

4.8 The details of how to label and use information are described in the **How To – Label and Use Information**.

## 5. Handling

5.1 Information assets can only be handled by individuals that have appropriate authorizations.

5.2 The requirements for transmission, receipt, storage and declassification of classified and restricted information are described above. Destruction of information media can only be carried out by someone who has an appropriate level of authorization and in line with the requirements of **Policy - Hardware Asset Management**.

5.3 Methods of handling portable and storage media for each project are determined individually in accordance with the customer requirements.

5.4 Project Manager/Project Director is responsible to translate the client's information classifications into this one and ensure appropriate handling of this information according to the client requirements (e.g. information encryption requirements, retention etc.).

# Change History

| Revision | Change Description | Valid Date | Approver |
|---|---|---|---|
| 1.0 | Initial issue (ISMS documentation structure review) | 06/22/2017 | Cristian Rojas |
| 2.0 | The item 4.7 was added | 09/06/2018 | Alok Malik, CISO |
| 2.1 | The item 4.4 was added. Minor text changes | 07/17/2019 | Alok Malik, CISO |
| 2.2 | Personal Data is added to section 3.7 and 3.8 | 01/10/2020 | Alok Malik, CISO |
| 2.3 | Item 3.7.6 was added | 08/25/2020 | Alok Malik, CISO |
| 3.0 | Guideline - Information Classification Labeling and Handling was changed to Policy - Information Classification Labeling and Handling in terms of documents restructure project. | 01/27/2021 | Alok Malik, CISO |
| 3.0 | Annual review - no changes | 23/03/2022 | Alok Malik, CISO |
| 3.1 | Date Format of Valid Date was corrected | 03/23/2022 | Alok Malik, CISO |

| | | | |
|---|---|---|---|
| 3.1 | Annual review - no changes | 03/15/2023 | Denys Kudriavchenko, Head of Security Risk & Compliance |
| 3.2 | Updated link and name for Policy - Asset Management | 09/19/2023 | Denys Kudriavchenko, Head of Security Risk & Compliance |