Information Classification and Handling Procedure

KG Invicta Services (KGiS)

[Ref: ISM-PLC-DOC-01]
[Ver: 0.1]
[05th April 2023]
[Classification: Internal]

+91 422 4419999

KGiS
o 365, KG Invicta Services Private Limited KGiSL Campus, Thudiyalur Road, Saravanampatti, Coimbatore - 641035, India

www.kginvicta.com

Statement of Confidentiality

This document contains confidential and proprietary information of KG Invicta Services Private Limited (KGiS). It is furnished for KGiS internal use and purpose only. Except with a prior written permission of KGiS, this document and the information contained herein may not be published, disclosed, or used for any other purpose. This document is reviewed at least annually.

a. © KG Invicta Services Private Limited, 2022

Copyright and Intellectual Property

b. KGiS logo are registered marks of KG Invicta Services Private Limited.

c. Copyright © 2022 KG Invicta Services Private Limited. All rights reserved.

Table of Contents

1 Document Control

1.1 Document Owner and Approval

KGiS's Information Security Office (ISO) is the accountable owner of this procedure. The ISO is responsible for ensuring that this document is reviewed periodically by the relevant stakeholders in line with the review requirements of the Information Security Management System (ISMS).

A current version of this document is available to all KGiS members at the corporate Intranet and is published on 05th April 2023.

This procedure document was approved by the Head of ICT on 05th April 2023 and met the required Documentation Quality Standard and is issued on a version-controlled basis under the signature.

Name: Shanmugam C

Designation: GM - ICT

Signature: Date:

1.2 Amendment History Record

Version	Description of Change / Action	Resource	Date
1.a	New draft baseline of ISMS procedure	Harikrishnan P	04th-April-2023
1.0	Verified and Approved By	Shanmugam Chinnasamy	05th-April-2023

1.3 Cross References

All reference documents available in – Shared Folder
ISO 27001– Information technology – Security Techniques – Information security – Requirements
ISO 27002 – Information technology – Security techniques – Code of practice

1.4 Document Sign off and Distribution

Name	Designation	Signature	Version	Date
Shanmugam Chinnasamy	GM- ICT		1.0	05th May 2023

Document Distributed for Internal Approval.

Stakeholder	Date
All Head of Departments and Departments	

2 Definitions & Glossary

Term	Definition
Division – Department	The business unit / team who is responsible for the data collected or created
Business Process	Business processes handled within the Division - Department
Data Set / Document Name	Data Set is the document or file name of the data
Description of Data	A short description about the identified data
Data Category	Data category denotes the type of data which has been identified, whether the data is Personal, Technical, Legal or Business data etc.,
Data Owner	Data owner is the absolute legal person or entity who holds rights on the data and is the authority. Data owners are expected to classify data based on the sensitivity and level of assurance to protect security of data.
Data Custodian	Data may be held by another entity or a group or a person who is authorized by the legal owner to operate and process the data. Custodians are expected to be compliant to the Data handling practices as prescribed by the legal owner.
Data Format	Data format represents the type of data identified. The data format has been categorized into the following. Structured – data which has been collected or generated from the application Unstructured – data which has been created or collected manually Semi structured – data which has manual intervention and collected through an application
Data type	Data type denotes whether the data is in a Physical or Digital format or it could be in both medium
Confidentiality	To ensure that data/ information is not made available or disclosed to unauthorized individuals, entities
Integrity	To ensure accuracy and completeness of the data/ information is maintained. Modifications to the information is made only by authorized individuals
Availability	To ensure that data/ information is made available, accessible and usable for authorized personnel

Classification Taxonomy	Data taxonomy is the classification of data into categories and sub-categories. It provides a unified view of the data and introduces common terminologies and semantics across multiple systems
Risk	The situation with undesired outcome of an event or an occurrence
Impact	The resulting effect upon occurrence of a Risk
Legal /Regulatory Impact	The resulting effect on the organization upon violation of Legal, regulatory or contractual obligations leading to notices, legal suite/ charges, including Financial Penalties
Financial Impact	The resulting effect on the organization that lead to loss of revenue, or profitability upon violation of Legal or contractual obligations
Reputational Impact	The resulting effect on the organization that lead to loss of brand image, reputation and negative publicity
Operational Impact	The resulting effect on the organization that lead to loss of productivity, inconvenience to Business operations

3 About the Document

3.1 Introduction

Data classification (or information classification) is a process of organising data into categories for its most effective, efficient and secure use. Data classification involves the categorisation and labelling of data according to its level of sensitivity, such as data that must be safeguarded for **Confidentiality**, **Integrity**, and **Availability**.

Data classification and handling is primarily concerned with the management of information to ensure that it is handled well with respect to the threats it poses to the organization. It also factors in how this information is being used and structured to allow authorized personnel to get the right pieces of information at the right time, while aiding in ensuring that only those who are authorized can view or access information.

This procedure, in concurrence with Information Security Policy sets the foundation to drive **acceptable data handling practices and legitimate use of data** in the context of KGiS. This procedure also documents the data lifecycle, data management principles and role & responsibilities towards classification and handling of information.

3.2 Objective

The objective of this procedure is to outline and establish a process in KGiS's environment to identify, classify and handle data within the organization, and help the business to identify the data owner and custodian respectively to maintain and protect the data.

3.3 Purpose

This procedure sets forth the directions on data classification and handling guidelines for data owners, champions and end users by prescribing principles and methodology to classify data in hard copy and digital format.

3.4 Scope

This procedure is applicable to all business teams within KGiS, who handle or are authorized to have access to the information within KGiS' s environment.

The scope of this procedure covers all types of data present within KGiS, which includes but not limited to the following:

a. Personal data
b. Employee data
c. Financial data
d. Health data
e. Business data
f. Customers data
g. Legal & Contractual data
h. Technical data
i. Compliance data

The scope of this procedure also covers all information assets owned by KGiS, which includes but not limited to the following data generated and/or stored within:

a. Applications and Databases
b. End user devices i.e. desktops, laptops, tablets and smartphones
c. Removable media storage i.e. tapes, authorized USB drives
d. Hard copy documents

3.5 Data Classification Principles

a. Data classification is necessary to define acceptable use and handling of data throughout its life cycle.

b. Classification taxonomies assist in labeling that are important to induce good security practices.

c. All data created or received by KGiS requires to be classified.

d. All unclassified information shall be deemed to be the highest classification. Unclassified information shall be classified in consultation with the data owner.

e. Data must be classified considering the key expectations from the data owner on security attributes such as confidentiality, integrity and availability.

f. A data set that contains sensitive information shall receive a higher classification.

g. All types of data require formal handling mechanism involving storage, transfer, processing, retention, and disposal.

h. Data must be reclassified (increasing the sensitivity) in the event the information handling is redefined for a specific data type.

i. Data must be declassified (lowering the sensitivity) to suit the business needs to facilitate sharing and collaboration with customers and business partners. A justification shall be provided by the authorized user for declassifying the data.

4 Data Management – Life Cycle, Classification and Handling

The key to data management is identification, categorization and segregation of data based on the importance of data to business process and the business objectives of the organization. Data Management focuses on Confidentiality, Integrity and continued Availability of data for authorized personnel, to comply with obligations such as legal, regulatory and contractual requirements and KGiS's management objectives. Data represented in meaningful form becomes information. The sensitivity increases due to the data presented in digital formats across the ecosystem of the technology and business process environment.

Data handling encompasses areas such as identification, storage, processing, transfers, retention and disposal. KGiS is responsible for data handling to commensurate with risks and impacts based on the data security requirements of the organization or respective data owners.

Data Handling involves:

a. Labelling – information based on its sensitivity
b. Storage of data with proper access control
c. Legitimate use of data for processing
d. Need based transfers to internal and external entities
e. Retention of data to meet with requirements of law, contracts and statutes
f. Secure methods of disposal of data

4.1 Data Life Cycle and Classification

Data classification is performed based on sensitivity and criticality of the data. This helps the data owner to implement appropriate data security controls. The sensitivity of data is bound to change over time and shall need to be reclassified at various stages in the data cycle.

Data life cycle involves processes such as create or collect, store, use / process, transfer /share, retain and dispose.

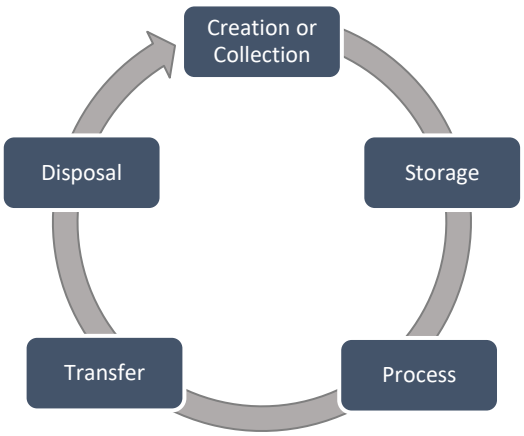


Figure 1 Data Lifecycle

Collection or Creation: In this first stage of data life cycle, the data is created or collected by the respective business team/owners within KGiS.

Storage: The data is stored and accessed by authorized data owner and custodian within the designated storage area in KGiS's environment.

Process: This is the state where the data created or collected will be processed by the data user within the business team as per the process defined by the business owner.

Transfer: Data transfer within and outside KGiS by the authorized personnel.

Disposal: Upon end of life of the data, the data shall be disposed i.e. delete permanently from KGiS's environment by authorized personnel.

4.2 Roles and Responsibilities

a. **Data Owner** – Data owners are individuals or groups who create data and make decisions on who are authorized to access, privileged to edit data and advise on how the data should be used. Owners may not be working with their data on a day to day, however they are accountable for overseeing & ensuring protection of data under their ownership.

   Data owners are also responsible to make decisions and advise information security team on the classification/reclassification/ declassification of data.

b. **Data Custodian** – Data custodians are responsible for the safe custody, transport, storage of the data and implementation of certain business rules. Data custodians are responsible to ensure compliance and satisfy the requirements of the data owner on ensuring confidentiality, integrity and availability.

c. **Data User** – Data users are personnel who are authorized and have the legitimate business need to access and process the data. Users are responsible and should adhere to the principles and guidelines set by the data owner and custodian.

4.3 Data Format

Data formats may be unstructured, structured or semi-structured, and these are bound to change from structured to unstructured and vice versa depending on the changes to the business process/environment. However, irrespective of the format the data classification becomes a fundamental requirement.

a. **Unstructured** – Data that is present in the form of individual files that contain information in a discrete form e.g. word processor documents, spreadsheets that contain discrete forms of information or any other file type that is transportable to another place as a file object.

b. **Structured** – Data that has a mix of discrete information like an email - that has text, numbers, and/or tabular data forms with predetermined data fields e.g. application form that contains - instructions in text, and tables for filling up standard information.

c. **Semi Structured** – Data that is present in the form of individual files that contain information in a discrete form e.g. word processor documents, spreadsheets and it is transportable to another place as a file object.

4.4 Roles and Responsibilities Matrix

Roles/ Responsibilities	Data owner	Data Custodians	Information Security	Data User
Identify unclassified data	A, R	C, I	C	I
Identify custodian/ data type/ category	A, R	C, I	C	I
Identify data security requirements	A	C, I	R	I
Identify data formats	A	R	C	I
Identify data profile – storage, processing, transmission, retention requirements	A, R	C, I	C	I
Identify & select potential impacts	A, R	C, I	C	I
Derive classification taxonomy	R	C, I	A	I
Adopt Data Handling on Storage, Processing, Transmissions, Retention	A	R	C	I
Re-classify data	A, R	C, I	C	I
De-classify data	A, R	C, I	C	I

R Responsibility – The personnel who is responsible for performing the task

A Accountability – The personnel who is accountable for the process or data

C Consulted – The personnel who provide opinions or suggestions

I Informed – The personnel who should be informed with the progress and updates

5 Data Classification Process

Classification of data becomes equally important when data is created within or received from outside the organization. Data may be received with or without a classification, but respective data owners are accountable to ensure any data within KGiS are classified with appropriate labels. It is recommended that data custodians' approach and consult the data owner requesting them to classify the data. The data is treated as sensitive by KGiS in case the data is not being classified.

Data classification & handling process the following as described in this section here.

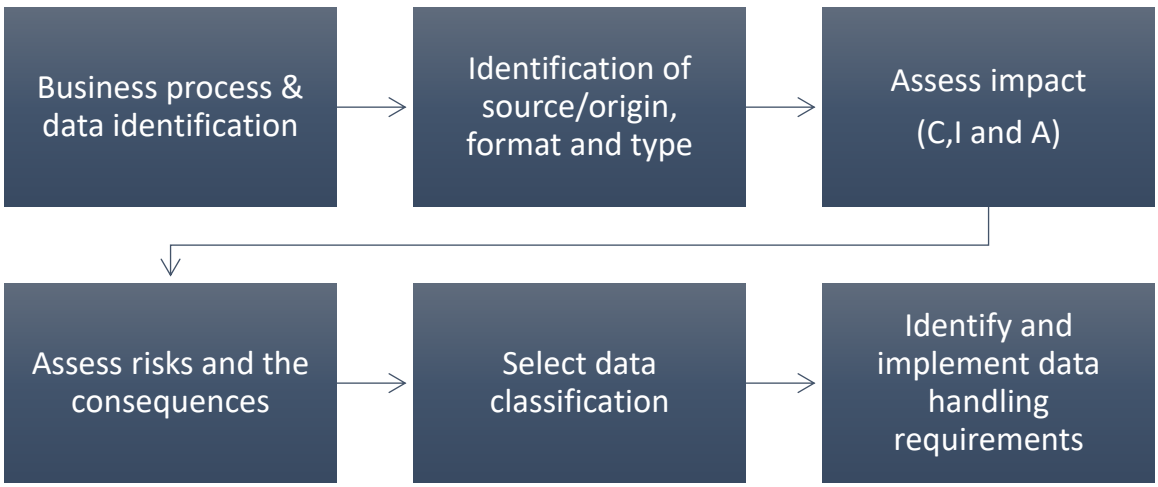


Figure 2 Data Classification Process

5.1 Identification of Business Process & Data

Identify data that is created or processed by the department. Such data may include data received created/transformed/processed by the department or received from the group companies, stakeholders, clients, vendors and suppliers.

a. **Personal Data** – Data that belong to individuals and may pertain to personal identifiers such as citizenship information, government identification details, heath and family details, medical insurance and claims etc.

b. **Employee Data** – This is personal data that is sensitive in the context of an individual's employment or association with KGiS such as employee salary details.

c. **Financial Data** – Data that belong to KGiS or its customers or vendors or service providers that is business critical.

d. **Business Data** – Data that belong to KGiS or its customer or vendors or service providers that is sensitive to respective businesses that may be proprietary information.

e. **Customer Data** – Data belonging to KGiS customers. (KGiS plays role of data custodian in this case).

f. **Legal & Contractual Data** – Third party contract (client, vendor, supplier, etc.) and related documents.

g. **Technical Data** – Data pertaining to KGiS's technological environment. For example: IT infrastructure architecture, device configuration, etc.

h. **Compliance Data** – Data related to KGiS's applicable statutory and regulatory compliance.

Above is an indicative list, more categories may evolve depending on the usage and type of data Example: business-financial data, business & technical data or personal health data.

5.2 Identification of Source of Data/ information

5.2.1 Identify Data source

Internal or external to company – identify the origination of the data which may be a customer, third party (e.g. vendor, service provider etc.), or an internal department assignment of data ownership

a. **Data Owner** – Identify the owner who is the data authority and the ultimate owner of the data. Data owners drive the information security requirements on confidentiality, processing integrity and availability.

b. **Data Custodian** – Identify custodians of data who may hold & process data within KGiS, and may be even external entities (such as authorized vendors or service providers or business partners)

5.2.2 Identification of Data Formats

a. Identify data formats such as structured, unstructured or semi structured.

5.2.3 Identification of Data Type

a. Identify data types –such as digital/physical, audio/video etc.

5.3 Assessment of Impact

In the event the data in subject is compromised on confidentiality and integrity or availability, potential impacts are computed using the scale as per the below table.

Impact rating - 0 being the lowest and 4 being the highest.

Impact Rating	Qualitative definition of Impact	Data Classification Taxonomy
4	Very High or Catastrophic	Sensitive
3	High	Confidential
2	Limited or Moderate	Restricted
1	Insignificant or low	Public

0	Not applicable or No impact	Public

Table 1 Data Classification Taxonomy

Note

- Not applicable is specific scenario – depends on type of data
- No impact is the negligible impact

Data Classification Taxonomy- Illustration

Impacts	Legal	Financial	Operational	Reputational	Data Classification Taxonomy
If	Very High or Catastrophic	High	High	Very High or Catastrophic	Sensitive
If	High	High	High - Moderate	High	Confidential
If	Limited - Moderate	Low or insignificant	Limited - Moderate	Moderate - Low	Restricted
If	Low or insignificant	Low or insignificant	Low or insignificant	Low or insignificant	Public

Table 2 Data Classification Illustration

Note: Highest degree of impact in any one category will override the other impacts.

Example:

If any of legal, financial, operational or reputational impact is **'Very High'** or **'Catastrophic'**, the resulting impact on the data is computer to be **'Very High'** or **'Catastrophic'** driving the data classification to **'Sensitive'**.

If any of legal, financial, operational or reputational impact is **'High' or 'High Moderate'**, the resulting impact on the data is computer to be **'High'** driving the data classification to **'Confidential'**.

5.4 Assessment of Security Risk and Consequence

The Table describes the nature and magnitude of impact that is used to derive data classification. The impact categories are

a. **Legal, Regulatory Impact** – This includes impact on contractual requirements with customers and business partners.
b. **Reputational Impact** – This includes media coverage, reputation etc.
c. **Financial Impacts** – This includes revenue loss, penalties, resulting incidental expenses on account of legal, regulatory actions.

Operational Impacts – This includes inconvenience and damage caused on business operations, resulting in productivity and business loss.

Information Classification Categories				
Criteria	**Legal / Regulatory Impact**	**Reputational Impact**	**Operational Impact**	**Financial Impact**
Very High Impact/ Catastrophic	Legal action against KGiS, violation of applicable regulation leading to legal & regulatory investigations and fines.	KGiS receives high negative media coverage resulting in large scale customer loss or significant impact on share prices.	Most of the customers impacted / complete IT systems outage, core functions and multiple mission critical functions are down.	Significant impact on financial flow, customer, relationship, contractual breaches resulting in penalties due to contractual obligations and the financial impact
High Impact/High Moderate	Warning from regulators and legal authorities.	Organization receives significant negative media coverage resulting in customer loss.	Some of the customers impacted, some IT systems are down, and some mission critical functions are down.	High impact on financial flow, customer relationship, contractual breaches resulting in penalties and the financial impact
Limited Impact/Moderate /Limited-Moderate/Moder ate-Low	No legal impact but potential legal impact is possible if it happens again.	Few customer complaints	Some of the customers impacted, non-mission critical system outage	Limited financial impact, customer, relationship, contractual breaches resulting in penalties due to contractual obligations and financial impact
Low/Insignificant	No legal actions	No media coverage/ customer complaints	No impact on operation / transaction	No financial loss. No impact on customer relationship, no contractual breaches
No impact	No legal impact/not applicable	No reputational impact/ not applicable	No operational impact/ not applicable	No financial impact/ not applicable

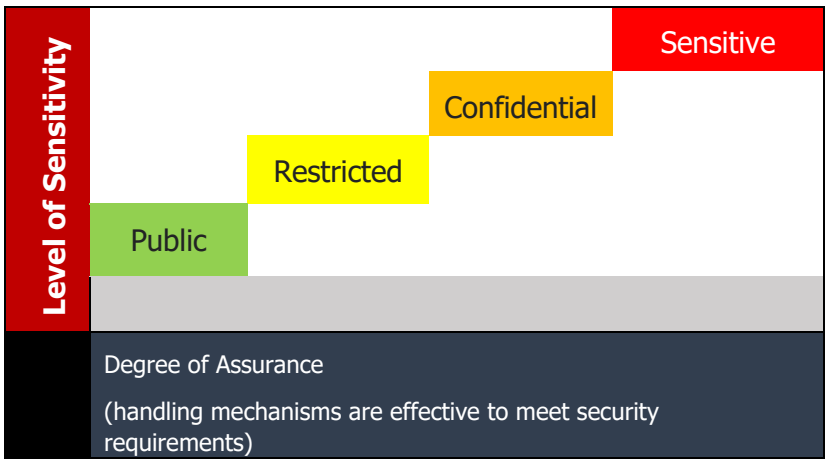
Table 3 Information Classification Categories

5.5 Data Classification Taxonomy

Data classification is a combination of two key attributes

a. Degree of assurance on security & protection
b. Level of sensitivity of data

Assurance is a requirement of the data owner, and Level of sensitivity is an outcome; Sensitivity level is directly proportional to the degree of assurance.



Classification taxonomies are derived basis the impact ratings for each type of data.

Data is classified as

a. **Sensitive –** If any of the impact categories are rated to be 'Very High' or 'Catastrophic'
b. **Confidential -** If any of the impact categories are rated to be 'High'. There can be further segregation of this category as Confidential- Internal and Confidential- External.
c. **Restricted** -If any of the impact categories are rated to be 'Limited' or 'Moderate'
d. **Public** -If any of the impact categories are rated to be 'Insignificant' or 'Low'

5.6 Identification of Rules Governing Data

Business rules or policies are most essential to achieve intended objectives on data management and security. Data handling rules prescribe acceptable practices to commensurate with the data classification:

a. **Storage**
b. **Processing**
c. **Transmissions**
d. **Retention and**
e. **Disposal**

5.7 Data handling

Following are the governance and security control measures to be considered for data handling:

Electronic						
Information Asset Classification	**Examples**	**Storage**	**Transfer**	**Disposal**	**Access Allowed**	**Access Approver**
Sensitive	Strategic documents, merger and acquisition plans etc.	Encrypted / password protected, copy & print restricted and access restriction	Encrypted / password protected, copy & print restricted and access restriction	Data eraser and wiping – DoD method Physical destruction	Department head Only, Author and CEO	CEO
Confidential - internal	Project documents, RFPs, IP addresses, network diagram, payroll data, passwords etc.	Limited access with strict access restriction	Encrypted only	Degaussing – hard disk drives (HDD) Shredding, grinding, pulverizing – solid state disk (SSD) Data eraser and wiping – DoD method	Department head, author and authorized internal stakeholders	Department head
Confidential - external	Client confidential data, vendor agreements, vendor SLAs, communication with regulatory authorities etc.	Limited access with strict access restriction	Encrypted and/or password protected	Degaussing – hard disk drives (HDD) Shredding, grinding, pulverizing – solid state disk (SSD) Data eraser and wiping – DoD method	Department head, author, internal and external stakeholders	Department head
Restricted	Internal policies and procedures, training material, forms, sops etc.	User access restriction	No control required	Secure formatting/ overwrite multiple times (minimum of 7 cycle)	All employees only	Author
Public	KGiS web site, external marketing material etc.	No control required	No control required	No control required	Anyone	Anyone

Table 4 Data Handling Procedures (Electronic)

Paper						
Information Asset Classification	**Examples**	**Storage**	**Transfer**	**Disposal**	**Access Allowed**	**Access Approver**
Sensitive	Strategic documents, merger and acquisition plans in print etc.	Fire and waterproof secure vault and access authorized by asset owner and data labels	Secure vault carried by authorized personnel	Shred	Department head Only, author and CEO	CEO
Confidential - Internal	Printed network diagrams, sales forecasts, invoices (in print) etc.	Fire and waterproof locked cabinet with restricted access and data labels	External: sealed envelope carried by authorized personnel Internal: carried by authorized person	Shred	Department head, author and authorized internal stakeholders	Department head
Confidential - External	Legal notices (in print), customer or vendor confidential material in print etc.	Fire and waterproof locked cabinet with restricted access and data labels	External: sealed envelope carried by authorized personnel Internal: carried by authorized person	Shred	Department head, author, internal and external stakeholders	Department head
Restricted	Training handouts, printed and posted process maps etc.	Locked cabinets	By Authorized person	Shred	All employees only	Author
Public	Marketing fliers in print.	No control required	No control required	No control required	Anyone	Anyone

Table 5 Data Handling Procedures (Paper)

5.7.1 Data transfer

a. Below media/mechanism are approved by information security team as official medium for data transfer. Any additional mechanism needs to explicitly be approved before using.

5.7.2 Approved mechanism for Internal transfer

a. Email
b. OneDrive for Business
c. MS Teams

5.7.3 Approved mechanism for External transfer

a. Email

5.7.4 Data Retention

Below data retention requirements have been established for various forms of data created/processed within KGiS

5.7.4.1 Permanent Retention

Unless otherwise specified all documents pertaining to the list below will be kept for an indefinite period:

a. Shareholder and board resolutions;
b. Organizational by-laws;
c. Articles of association; and
d. Annual reports.

5.7.4.2 General Retention

a. Most business documents - 7 years (unless specified otherwise by the owner)
b. Invoices and other financial data – 5 to 7 years
c. HR data of existing employees after offboarding - 7 years
d. HR data of un-hired staff – 3 years
e. Tax records VAT etc. – 4 years
f. Legal correspondence or data – Permanent

Any other data not specified in the above list shall be retained for 7 years.

6 Standard References

a. **ISO 27001:2013**
   - A.8.2.1 Classification of Information
   - A.8.2.2 Labeling of Information
   - A.8.2.3 Handling of Assets

7 Attachment

Information pertaining to Data handling within and outside KGiS's environment has been detailed in the following document. Kindly refer to the following template for more information.

Information Classification template

Information Classification Templat