DRPG

INFORMATION CLASSIFICATION GUIDELINES

Version:	7
Published:	01/07/2022
Created by:	James Hurley
Approved by:	Richard Parmenter
Confidentiality level:	Restricted

Contents

1 Purpose and scope

DRPG's information assets and services are classified, considering their legality, value, sensitivity and criticality to the organisation.

2 Responsibilities and applicability

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

The intended recipient of any information assets received from outside **DRPG** becomes the owner of that asset.

The Information Security Manager is responsible for maintaining the inventory of assets and services together with their classification levels.

All **DRPG** users of organisational information assets (including mobile phones, laptops and other peripherals) have specific responsibilities as identified in their acceptable use and user agreements.

Line managers and asset owners are responsible for ensuring that the correct transmission processes are followed for the classification of data.

The classifications of information assets should be reviewed annual by their owner and if the classification level can be reduced, it will be. The asset owner is responsible for de-classifying information.

3 Referenced documents

ISO27001:2013 Clause A.8.2.1, A.8.2.2, A.8.2.3

4 Introduction

DRPG is an agile, dynamic organisation with limited appetite or overhead for managing overly complex marking schemes. It does however recognise the importance of effective information classification to protect information and assets based on its value and importance.

We have conducted extensive risk assessment and consideration of assets as regards confidentiality, integrity and availability. We also take note of ISO 27002 guidelines on labelling "The procedures can define cases where labelling is omitted, e.g., labelling of nonconfidential information to reduce

workloads." in these instances we have looked at other means of designating the classification of information e.g., via procedures or meta-data.

To that end, organisation-controlled documents, digital content and physical drives (e.g., standalone back-up drives) holding files need to be classified or marked with one of the following:

5 Classification

To protect the confidentiality, integrity and availability of the information processed, stored or transmitted, all information will be classified in one of the following categories ‘confidential’, ‘restricted’, and ‘other’.

5.1 Confidential Information

For information where disclosure or loss has a serious impact on long term strategic objectives or puts the survival of the organisation at risk.

Information included in this category is:

- Any Personally Identifiable Information (PII), for example, personnel records, customer records (where individuals data resides), bank and financial records, NI, Tax or pension records.
- Any Personally Identifiable Information (PII) that fall under GDPR (General Data Protection Regulation), for example, health records, sexual orientation, ethnicity, criminal records, political or religious beliefs, memberships of trade unions, dietary requirements and biometric data.
- Company sensitive information about acquisitions or corporate strategy
- Any information covered by intellectual property rights (IPR) – e.g., developed code, research materials, copyrighted documentation etc.
- Any information considered infrastructure critical – e.g., Cryptographic keys, security configurations, log files, pen testing scopes and results etc
- Corporate financial or strategic information – e.g., un-released figures, details of business deals, performance figures etc.
- Note that whilst a system may be considered “Restricted” it may still hold “Confidential” information.

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

Access to ‘Confidential’ information will be subject to access controls.

Confidential information sent by e-mail must be encrypted (TLS (Transport Layer Security)) and digitally signed and sent only to the e-mail box of the identified recipient.

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 **DRPG** or an associated client.

5.2 Restricted

This is the default setting to be applied to all draft work, and for final versions that have business sensitive information that is generally targeted at discrete stakeholders on a need-to-know basis e.g., customers.

Most of the way the organisation works is digital, using technology, which makes explicit classification difficult especially when using online systems. It includes directly inputting data into web pages, structured fields, and storing records that cannot be easily classified, or would be costly to do so and unlikely to work in practice.

As such all content (beyond clearly marked documents) stored in our online systems and those that offer business support services from other technology and business service suppliers shall automatically be determined as “restricted”.

It is not necessary to specifically mark information as “restricted”.

The use of these digital systems is therefore “Restricted” by default unless or until something has been made Public e.g., by publishing to a public website, distributing collateral to a wider stakeholder group etc.

Information types included in this category are:

- Customer information technology systems details
- Commercial proposals
- Service delivery methodologies
- **DRPG** IP (Intellectual Property)
- Internal Forms

Restricted information must only be sent to the e-mail box of individuals known to be allowed to receive such information.

5.3 Public

The information which can be released and shared outside of **DRPG** with no limitations.

6 Labelling

Documents are labelled as set out below, ideally in the document footer, document title, watermark or by stick on label.

Public – Not labelled. Only "Public" if clearly for un-restricted release (e.g., marketing materials)

Restricted – Not labelled; and unlabelled information is treated as this level unless clearly for public release.

Confidential – Labelled where possible (e.g., physical documents, physical storage media)

Examples:

Emails – No classification label is applied, and e-mail is treated as if the default "restricted" classification.

Physical and paper documents – labelled as "Confidential" where applicable or left unlabelled and treated as "Restricted" unless clearly for external release (e.g., marketing materials)

Physical storage devices – electronic media, where used, are labelled as "Restricted" or "Confidential" (e.g., external hard drives).

7 Handling of assets

Wherever possible the organisation avoids the creation of paper-based information assets itself and attempts to produce only digital information. Customers and others who receive that can print and share as they see fit based on their policies and procedures in accordance with the classification and any controls we have applied to the information.

The purpose of this policy is to ensure the correct handling of classified information and to reduce the likelihood of unauthorised disclosure.

1. All information is to be handled in accordance with our:
   - Terms & conditions of employment (A.7.1.2);
   - Acceptable use of assets policy (A.8.1.3); and
   - **DRPG**'s Code of Conduct.
2. Information is also to be handled in accordance with the table below.
3. Where customer information must be handled in line with their requirements and/or classification scheme, those requirements will take precedence (e.g., for UK Government etc)

		Public	**Restricted**	**Confidential**
	Examples	Press releases Websites	Client IP DRPG IP (Forms, documents Proposals Photo's	Employment records Personnel records Tax, benefit, pension records PII (Information inc: National Insurance no., Ethnicity, Political or Religious belief, Sexual orientation, Criminal Record, Passport Number PCI (Payment Card Information)
Handling				
Storage	Removable Media	Removable media may be used to store or transfer this information, but it is strongly recommended that the media be erased once the task has been completed.	Information may be stored or transferred using removable media providing: The media is encrypted; and Appropriate permissions are granted from the information owner.	Information may be stored or transferred using removable media providing: The media is encrypted; and Appropriate permissions are granted from the information owner Storage or transfer of personally identifiable information (PII) using removable media must be avoided wherever possible. Wherever such use of removable media is required, advice must be sought from the Data Protection Officer to ensure compliance with the DPA (Data Protection Act) and GDPR.
	Hard copy		Hard copy is acceptable but is deemed "uncontrolled" and must be kept within the confines of the office as best practice. Personnel can take hard copy information outside of the premise if there is a clear business reason to do so but must return it for storage or secure destruction when finished with.	Printing of information must be avoided where possible. Where printing must occur, information must be recovered from the printer immediately. Hard copy must not be taken offsite unless express permission has been granted from the information owner. Hard copy must be stored in designated storage facilities (e.g., locked filing cabinets)

Transmission		DRPG has approved these prior to release and satisfied for the to me transmitted to unknown persons	Information can be passed on to third parties where: suitable NDAs are in place; sufficient checks are made for suitability of sending; and appropriate permissions are granted from the information owner.	This information may only be transferred between authorised persons.
	Email	TLS 1.2	TLS 1.2	Encrypted TLS 1.2
	Office 365 (OneDrive/SharePoint/Teams)	TLS 1.2	TLS 1.2	Encrypted TLS 1.2
	Post			Signed for and with tracking
	Web Browser	Ensure SSL (Secure Sockets Layer) on Browser or TLS 1.2	Ensure SSL on Browser or TLS 1.2	Ensure SSL on Browser or TLS 1.2
	File Transfer (WeTransfer/OneDrive)	Ensure SSL on Browser or TLS 1.2	Ensure SSL on Browser or TLS 1.2	Ensure SSL on Browser or TLS 1.2
Disposal	Hard copy	Paper copy must be shredded or put in the Confidential Waste bin	Paper copy must be shredded or put in the Confidential Waste bin	Paper copy must be shredded or put in the Confidential Waste bin
	Hard drives / removable media	Removable media must be formatted to DoD 5220.2M standard Media - HDD / CD / DVD or Flash drives must be shredded		
	Electronic files	Delete	Delete and empty recycle/trash	Delete and empty recycle/trash

8 Consequences of non-compliance with this policy

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational Disciplinary Process (A.7.2.3).

9 Document owner and validity

The Information Security Manager is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements of the ISMS.

This document is valid from 01/07/2022

Next review date 30/06/2023

10 Change Record

Issue	Description of change	Approved by	Date
1	Initial issue.	April Pearson-Myatt	21st February 2016
2	Updated branding and review of policy	James Hurley	16th January 2017
3	Annual review	James Hurley	24th February 2018
4	Policy review and rebrand	James Hurley	27th June 2019
5	Annual review	James Hurley	20th January 2020
6	Annual review	James Hurley	25th January 2021
7	Annual review including updated policy structure.	Richard Parmenter	01st July 2022