

Contact officer:

Name: Faizal Kassim

Function: Director

Information Security**Management System Policy****Issue date:**

January 2020

Latest review date:

December 2021 [V3.0]

New review date:

December 2022

GRI418: 103-1, 103-2, 103-3

Introduction

IPL Packaging International information security values are supported by three main principles: confidentiality, integrity and availability. IPL Packaging strives to ensure strong and rigid information security measures to protect its information and guarantee business continuity. One of the central topics within the following document is the protection of individual rights and freedoms. This is supported by our compliance with the General Data Protection Regulation as well as internal processes. We aim to protect all data within our operations and guarantee the highest information security standards.

Purpose

This policy addresses all our IT-related security objectives. These are supported by their corresponding measures. The document is a comprehensive guide for management and employees to understand our current information security measures as a whole. Its purpose is to inform about the current situation and oblige all individuals within the scope to comply to these standards. Within this document terms 'data' and 'information' will be used interchangeably. For definitions, please refer to Chapter 7.

Scope

The contents of this policy are intended for all employees, part time workers, interns, contractors of IPL Packaging its affiliates, and production sites.

What are your rights as a data subject?

Data subjects have the right to be informed of the existence and purpose of their personal data that is being processed. As a data subject, you are entitled to request details regarding your personal data. IPL Packaging will then notify you whether or not we are processing your personal data, and inform you about the purpose for which your personal data is being processed. If necessary, you can request rectification or ask IPL Packaging to delete your data. We will implement this request, unless there are compelling, e.g., legal, obstacles to doing so. IPL Packaging will inform you about whether

or not a rectification or data erasure has been made. You always have the right, due to your specific situation, to object to the processing and to request IPL Packaging to restrict or discontinue said processing. If there are no compelling obstacles, for example legal obstacles, we will honour your request and notify you of its completion.

Policy objectives

IPL Packaging aims to:

- > comply with the General Data Protection Regulation and any other applicable local and international laws and regulations that address information security;
- > implement a robust and safe framework for information security operations to reduce the risk of damage, misuse, theft, loss or abuse, based on ISO27001 standards;
- > educate employees regarding our current measures on information security and increase awareness regarding its importance;
- > ensure appropriate data retention and protection within the operations of IPL Packaging
- > protect all personal data and respond to incidents in a timely manner;

- > implement high standard software, which ensures information security and protection from external hazards;
- > ensure information is protected by physical controls;

- > have an 80% [or higher] rate of employees who have received training on information security awareness.
- > conduct a Security Audit to ensure all measures implemented are up-to-date and in accordance with the latest regulations and requirements.

Policy measures

IPL Packaging strives to achieve its information security objectives with the following measures. The measures are categorised under different themes for ease of comprehension.

General

IPL Packaging:

- > ensures structured data classification under different confidentiality levels to ensure it is protected from unauthorised access. Please refer to our Data Access Control Procedure for more details.
- > ensures its data protection by making use of anonymisation and pseudonymisation. This guarantees that only the necessary information is transferred to the recipient. Moreover, we have guidelines regarding the correct method of data disposal. Please refer to Data Anonymisation and Disposal Guidelines for more details.
- > has a Privacy Statement, which details our general processes with regard to personal data handling. This involves an explanation of the data we process and store of website visitors and for what purpose.
- > has a Disclaimer, Cookies & Privacy Policy, which outlines our procedures regarding privacy, intellectual property and cookies. It details personal rights and procedures with regards to personal data collected from website visitors.
- > supports its core production sites with an additional Information Technology Policy, which is written in the local language and helps all employees and management protect sensitive data.

GDPR Compliance

On May 25, 2018, GDPR [General Data Protection Regulation] entered into force, and is applicable throughout the European Union [EU]. GDPR regulates the protection of personal data in all EU - countries, and the same legal framework applies in each Member State.

IPL Packaging:

- > has a GDPR contact person and a GDPR team that can be contacted by anyone with questions about the policy and procedures;
- > has an overview of all parties that process personal data. This includes both internal and external parties [data processors];

- > ensures to have an overview of all personal data held by the company including but not limited to processing activity, purpose and category.
- > makes use of a processing register, which is kept up to date by the HR Manager.
- > has privacy statements made for employees, website visitors, and applicants which explains the data that we process and store of employees and for what purpose;
- > ensures that all data incidents are reported without undue delay and handled effectively in line with GDPR standards [Data Breach Procedure].

Data retention & access IPL packaging:

- > suppliers that require processing of our personal data to provide us their services, must gain our permission through a personal data processing agreement before processing any personal data;
- > employees provide consent to our processing of their data by signing the employment contract which includes the HR manual where information on what we process and why, is communicated;
- > has an overview of retention periods related to personal and business data. These retention periods are in line with the General Data Protection Regulation.
- > makes use of the Role System, which allows to assign different roles within the active directory to different employees. Consequently, employees are only able to access information related to their job position;
- > ensures efficient handling of personal data request in line with GDPR standards. We provide a form with which data subjects can request their information. More details: Subject Access Request Procedure;
- > supports its core production sites with additional Procedure for Document and Record Control, which ensures that documents remain legible and are retained for their purpose.

Information security awareness & best practices IPL Packaging:

- > has an IT handbook within its HR manual. It addresses the code of conduct related to computer, network, e-mail, social media and internet usage for IPL Packaging employees.

has created a training for its employees regarding information security, including information covered within the HR manual. It raises awareness of all current measures and highlights the importance of good IT practices;

- > ensures that individuals are aware of their rights to their personal data. The rights are explained in the HR Manual [employees] and in the Disclaimer, Cookies and Privacy Policy [website visitors];
- > educates its employees regarding password management within the organisation's operations.

Third-party management

IPL Packaging aims for all its data processors sign an agreement for processing data.

Information security software IPL packaging:

- > obliges its employees to use Microsoft Authenticator App. If they cannot use the app, a phone call or text message will be used as alternative. This ensures a two-step authentication for the linked account. It increases data protection and prevents incidents of undesired access;
- > makes use of FortiGate hardware. This cloud managed hardware solution consists of routers [MX] including firewall solutions, switches [MS] and access points [MR].
- > makes use of The FortiGate router, which has Firewall functionalities built into it. This is a cloud managed solution from SonicWall which has similar functionality as regular firewalls, only it has threat protection, advanced dash boarding and alerting included.
- > has installed on all LC Windows devices a virus scanner software, which guarantees end-point protection against malware, exploits and ransomware;
- > ensures that all Windows devices are scanned real time using the Windows Defender Antivirus software;
- > uses Windows 10 automatic monthly updates to make sure all Windows Devices are updated. For all programs within Windows the tool SCCM is used;
- > ensures data encryption with Microsoft Bit locker encryption on all Windows devices;
- > has an SLA with network service provider, Qdos (Pty) Ltd to ensure stability and security regarding the network.

Continuous controls

IPL Packaging:

- > conducts regular third-party information security audit controls;
- > conducts regular mystery hacks to check employee compliance with the information security standards;
- > makes use of internal communication platform when specific information security risks are observed such as occurrences of spam or phishing emails;
- > obliges its employees to reset their passwords on a bi-annual basis;
- > periodically checks its applications to prevent information security breaches.

Physical protection IPL Packaging:

- > stores employee personal data in the personnel file, categorised per topic. It is stored in the HR office, in four places:
 - Within Office365 mailbox
 - Within personal Google workspace
 - Paper personnel file in the filing cabinet;
 - Documentation folders in the wall cabinet.
- > relies on data retention of Google workspace
- > has a record of all its assets [physical and digital] managed by Silicon Overdrive (Pty) Ltd. This helps to create a comprehensive overview and allows efficient asset management.

Approval of policy

Name: Faizal Kassim

Date: 07/12/2021

Signature:

A handwritten signature in black ink, appearing to read 'Faizal', written in a cursive style.