Information Technology Data Governance Framework

Introduction

Purpose

The purpose of this document is to provide a confirmation to stakeholders of Nestlé Nigeria Plc. that it's Information Systems are designed and implemented to ensure the Integrity, Availability of services and confidentiality of data against potential breaches amidst the new digital reality.

Applicability

This document is applicable to all Nestle Nigeria Plc Information Systems and it's usage by Nestlé Employees, contractors and 3rd party staff.

It covers the following Nestlé information systems: all computers, networks, cloud services and mobile devices that are either Nestlé's property or that are used to access Nestlé proprietary information.

Local laws

This document will be used in conjunction with existing local laws regulating Information Security, such as the Nigeria Data Protection Regulation 2019.

RESPONSIBLE ADMINISTRATOR: INFORMATION TECHNOLOGY OPERATIONS LEAD

RESPONSIBLE OFFICE(S): INFORMATION TECHNOLOGY

ORIGINALLY ISSUED: DECEMBER 16, 2020

Information Technology Operations Lead

Finance & Control Director

REVISION DATE: Every Two (2) Years

Data Governance

ERP Systems Security

Nestlé Nigeria Plc. uses SAP as the internal ERP for processing financial and other data. The use of this ERP is governed through globally defined standards, security policies and by adequate Segregation of Duties (SoD) enforced by Internal Control practices during role requests. Accordingly, routine checks are performed on all controls to guarantee that all information systems are protected and are compliant to standards and policies.

Network Redundancy

To prevent transaction failures due to outages on our network, we have invested in and implemented a robust network structure that ensures near consistency to all Information Systems. Each of our locations – head office and factories have been designed to run as a separate network entity with redundancy built in. For assurances, these links are tested to ensure that they work as they are designed to do.

Data Backup & Restore

All our data are backed in line with the defined policies with frequency meeting business requirements. The backups are maintained and kept in safe environments to ensure data protection and robust recovery in event of failures of productive systems in compliance with the legal and regulatory requirements.

Periodic restore tests are performed to ensure the restore procedures are up to date and that data restoration is possible.

Policies guiding IT Operations

Nestlé IT Operations are governed through several internal policies to ensure consistent, robust and compliant operations. Some of these policies are:

- Nestlé Privacy Policy and Privacy Standard
- Information Classification Standard
- Record Retention Rules
- Reporting Information Security Breach Incidents.
- Identity & Access Management.
- Other applicable policies and standards.

These policies define the acceptable way to operate Information Systems at Nestlé.

Protection of Assets

Nestlé Nigeria Plc. provides devices (e.g. PCs, Laptops, Tablets, and Smartphones to our Users according to their needs. All IT equipment provided are protected through several tools and policies to ensure Data Protection on these devices all the times.

Nestlé Users are trained and made aware of their roles in Asset protection. Nestlé Mobile devices should contain minimum information and only what is required for current business activities when working off-line.

At Nestlé, steps have been taken to ensure that Data on all devices (and the devices themselves) are appropriately protected – using encryption of the device hard drives and the enrollment of Mobile devices to protect data on mobile devices where allowed.

Global security tools are used to enforce protection against malware infections and virus outbreaks in Nestlé and as such, all the necessary tools and preventive measures are in place to minimize the probability of such vulnerabilities. To maximize the Global data protection, online collaboration tools are implemented to eliminate the need for off-line data sharing across Nestlé.

Multi-factor Authentication (MFA) solutions have been put in place to prevent unauthorized access to our information systems where applicable which prevent unauthorized access from non-Nestlé systems.

Data Security & Compliance

As part of steps to ensure that our data is secure and in compliance with applicable laws and standards, we have adopted the International Standards Organization's Security Techniques through the Information Security Management Systems (ISO27001:2013) certification.

The Information Security Management System preserves the Confidentiality, Integrity and Availability of information systems by applying a risk management process that gives confidence to interested parties that risks are adequately defined, assessed, mitigating controls are defined and practices.

Nestlé Information Systems are audited to confirm adherence to the standard and policies by the group defined External Auditors and internal auditors on defined schedules which ensure continuous reviews and re-certifications every three (3) years.

IT Organization and Decision making

Information Technology (IT) is a global organization at Nestlé which ensures the Information Systems are designed, implemented and are operated in a consistent manner. Information Technology strategy is defined globally and is implemented through local IT teams in the countries Nestlé operates in. IT Strategy is periodically reviewed globally and approved by the executive board.

IT Organization is a 3-tiered organization at Nestlé

- Global Team is responsible for IT products strategy, roadmaps and products design in line with the functional needs of the different business units
- Regional IT team is responsible for supporting the implementation of the said IT Products in a defined geography e.g. Regional IT HUB based in Sydney is responsible to support the implementation of IT products in Asia, Oceania and Africa (including Nigeria).
- Local IT team is responsible for the management of Information Systems and IT Operations in each country and provides the on-field support to all business users e.g. Nestlé Nigeria IT Team which support all IT Operations in Nigeria

Change Management

To ensure rigor control and avoid business disruptions, all changes to be made on the Nestlé infrastructure must pass through a change advisory board (CAB) that evaluates the change, accesses the impact/risk and approval is given on whether to proceed with the change or not. The change management processes are in compliance with the Industry standard – Information Technology Infrastructure Library (ITIL) processes.

A global system is in place to ensure management of such changes for effective management and traceability.

Personal Responsibility

A global End User Policy defined the responsibility of each user at Nestlé. This Policy covers their responsibilities in detail on the use of Information Systems at all times.

It is the responsibility of all Nestlé Users to demonstrate and encourage the behaviour required to protect information and to protect the reputation of Nestlé, and to apply the principles of our various polices in their daily activities.