COURTEVILLE BUSINESS SOLUTIONS PLC
...enabling systems

EXTRACT OF CBS INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

1.0 INTRODUCTION

Information is a key asset of Courteville Business Solutions Plc (hereafter referred to as "**the Company", "CBS" or "Courteville"**) which must be used effectively and lawfully. The Information Security Incident Management Policy ("Policy"), and supporting documents within the Information Security Management Framework provide management direction to ensure that the Company's information and assets are appropriately managed. Compliance with this policy will help the Company to efficiently and effectively manage the risks from information security threats.

2.0 POLICY STATEMENT

CBS will ensure that it reacts appropriately to any actual or suspected incidents relating to information system and information within its control.

3.0 SCOPE

This policy applies to;

a. All information security incidents.
b. All information created or received by CBS in any format, whether used in the work place, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely.
c. All IT systems managed by, or on behalf of the company.
d. Any other IT systems on which CBS information is held or processed.
e. All users of CBS information. Users include all employees of CBS, all affiliates, contractors, suppliers and partners in any venture.
f. All locations from which CBS information is assessed.

4.0 PURPOSE

a. The intent of this policy is to provide a framework for managing and responding to information security incidents. Fostering a culture of proactive incident reporting and logging will help reduce the number of security incidents which go unreported and unnoticed, often without resolution.

b. This document provides guidance to the CBS Incidence Response Team and Crisis Management Team and associated stakeholders to better respond to information security events and incidents. It also provides a structured approach to;

- Detect, report and assess information security incidents.
- Respond to and manage information security incidents.
- Continuously improve incident response as a result of managing information.

5.0 DESCRIPTION OF INFORMATION INCIDENTS

An information security incident is defined as the exposure of sensitive personal data or confidential information to unacceptable risk. It may include any actual or potential breach of security which may compromise the confidentiality, integrity or availability of information stored, processed and communicated in relation to CBS business whether in hard copy or electronic format. Each potential incident will be risk assessed on a case by case basis.

6.0 PROCEDURES FOR INCIDENT MANAGEMENT

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed on time to identify if the event or series of events have escalated to an incident. It is important for the detectors to provide the Incidence Response Team with as much information as possible for investigation.

7.0 REPORTING INFORMATION SECURITY EVENTS

a. Incidents should be reported to the dedicated Help Desk platform set up by the IT Department. Information on the incident should include a description of the data lost or stolen, whether it was held in hard copy or portable media, the quantity (if known), where it was lost and the sensitivity of the data (if known).

b. In addition, all information incidents involving an IT security breach should be reported immediately to the IT Department for corrective action.

c. Security incidents involving sensitive data should be assessed based on the potential detriment to the individual and/or organisations affected, including possible distress and financial damage together with the volume of data involved.

d. Any IT incident occurring outside secure office premises should be reported immediately to the IT department.

8.0 PROCEDURE FOR REPORTING INFORMATION SECURITY WEAKNESSES

All information security events and weaknesses that concerns personal data relating to a member of staff, a service user or a member of the public, or it contains particularly sensitive or confidential information, then the incident should be reported directly to the Group Managing Director.

All IT-related events and weaknesses must be reported IMMEDIATELY to the IT Service Desk. If applicable, you must note the symptoms and any error messages on screen and await further instructions from a member of IT Department.

Information security events and weaknesses need to be reported at the earliest possible stage. It is vital that as much information is gained as possible to identify whether reported events or weaknesses are security incidents and to determine any further cause of action.

Security events and weaknesses that must be reported include;

i. Theft or loss of equipment, data or information (including removable media)
ii. Breaches of physical security arrangements
iii. Computer infected by a virus or other malware
iv. Receiving unsolicited mail of an offensive nature or requesting personal data
v. Unauthorised disclosure of information including information being faxed, e-mailed, posted or handed to an unintended recipient
vi. System malfunctions which may compromise security
vii. Inadequate disposal of confidential material
viii. Writing down passwords and leaving them on display or somewhere easy to find
ix. Non-compliance with policies or guidelines
x. Accessing a person's record inappropriately
xi. Receiving and forwarding chain letters – including virus warnings, scam warnings, and other emails which encourage the recipient to forward on to others.
xii. Accessing a computer database using someone else's authorisation (e.g. someone else's user ID and password).

Annex 1: Examples of Information Security Incidents and Categorisation

Incident Category	Description
Sensitive Personal Data	Risk of accidental or deliberate disclosure of sensitive personal data.
Business related confidential information	Risk of accidental or deliberate access of confidential information by an unauthorized person.
Passwords	An unauthorised person has gained access to your account or attempted to gain access using your password.
IT Security Breach	Degraded IT system integrity or loss of system availability posing threat to loss of information or disruption of activity.
Physical Security Breach	Unauthorised access to secure areas containing confidential information e.g. forced access to a locker containing information or sensitive personal data.
Theft or loss of portable media	Unencrypted laptops or other portable media containing confidential or sensitive personal data lost or stolen e.g. laptop stolen from car
Denial of Service (DOS)	An attack that successfully prevents or impairs the normal authorised functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim of, or participating in, a DOS.
Malicious Code	Successful installation of malicious software (e.g Virus, Worm, Trojan horse, or other code-based malicious entity) that infects the ICT services and systems.
Improper Usage	Actions involving IT services and systems that violate the Company's Information Security Management Policies. e.g

	a. Downloading and /or using unauthorised security tools. b. Use of Peer-to-Peer applications to acquire or distribute copyrighted material.

Annex 2: Incident Prioritisation Template

Priority	Factor	Examples of Incidents
Severe	An incident affecting the entire organisation	• Business disruptions resulting from malicious activity that results in > 50% degradation. • Any incident that impacts the availability of perimeter security infrastructure. • Exposure of unencrypted, unmasked or insufficiently masked CBS confidential or sensitive information into the public domain. • Damage to CBS reputation • Large number of people affected. • Serious breach of confidentiality or disclosure of sensitive personal data.
Major	An incident affecting multiple facilities, user groups, or networks	• Compromised privileged system credentials • Incident involving highly critical assets • > 10% of users dis-enabled • Potential for involvement of law enforcement • Active attack incidents that affect the servers. • Exposure of unencrypted, unmasked or insufficiently masked CBS confidential or sensitive information into the public domain. • Damage to an individuals reputation/ privacy. • Over 20 people affected and media not encrypted • Potentially serious breach
Moderate	An incident affecting a facility or network	• Malware incidents that do not fall in a higher severity • Data loss incidents not involving sensitive information

		• Confirmed phishing campaign that impacts more than a hundred users. • No material damage to the Reputation of the individual or organisation • Minor breach of confidentiality (up to 20 individuals)
Insignificant	Minor Incident	• Some localised inconvenience, but no impact to CBS.

CONTACT AND COMMUNICATION: If you require further information or a copy of the policy, you may contact IT, Legal or SCMU at our Head Office, 38, Commercial Avenue, Sabo, Yaba, Lagos.