INFORMATION TECHNOLOGY AUDIT REPORT

ON THE

DISPOSAL OF ICT EQUIPMENT

OF

SELECT PUBLIC ENTITIES

(MINISTRY OF SCIENCE, ENERGY AND TECHNOLOGY, eGOV JAMAICA LIMITED AND POST & TELECOMMUNICATIONS DEPARTMENT)

The Auditor General is appointed by the Governor General and is required by the Constitution, Financial Administration and Audit Act, other sundry acts and letters of engagement, to conduct audits at least once per year of the accounts, financial transactions, operations and financial statements of central government ministries and departments, local government agencies, statutory bodies and government companies.

The Department is headed by the Auditor General, Pamela Monroe Ellis, who submits her reports to the Speaker of the House of Representatives in accordance with Section 122 of the Constitution of Jamaica and Section 29 of the Financial Administration and Audit Act.

This report was prepared by the Auditor General's Department of Jamaica for presentation to the House of Representatives.

Auditor General of Jamaica
Auditor General's Department
40 Knutsford Boulevard
Kingston 5
Jamaica, W.I.
www.auditorgeneral.gov.jm

Our Vision :
A better country through effective audit scrutiny.

TABLE OF CONTENTS

AUDITOR GENERAL'S OVERVIEW 4

EXECUTIVE SUMMARY 6

WHAT WE FOUND 6

Inadequate Information Security Controls in the Disposal of ICT Equipment 7

Inadequate Access Controls 8

WHAT SHOULD BE DONE 9

PART ONE 10

AUDIT OBJECTIVE, SCOPE AND APPROACH 10

PART TWO 11

MINISTRY OF SCIENCE, ENERGY AND TECHNOLOGY (MSET) 11

BACKGROUND 11

INADEQUATE ACCESS CONTROLS 11

INADEQUATE INFORMATION SECURITY CONTROLS IN THE DISPOSAL OF ICT EQUIPMENT 12

PART THREE 13

EGOV JAMAICA LIMITED 13

BACKGROUND 13

INADEQUATE ACCESS CONTROLS 13

INADEQUATE INFORMATION SECURITY CONTROLS IN THE DISPOSAL OF ICT EQUIPMENT 13

PART FOUR 15

POST AND TELECOMMUNICATIONS DEPARTMENT (PTD) 15

BACKGROUND 15

INADEQUATE INFORMATION SECURITY CONTROLS IN THE DISPOSAL OF ICT EQUIPMENT 15

AUDITOR GENERAL'S OVERVIEW

Information and Communications Technology (ICT) equipment is increasingly being utilized by Ministries, Departments and Agencies (MDAs) in their daily operations resulting in an increasing build-up of inventory. Sensitive data stored on these devices must be appropriately secured or destroyed prior to their disposal. Despite this increased reliance on technology and the eventual disposal of ICT devices that have reached the end of their useful life, there is not yet any clear government policy regarding the secure disposal of ICT equipment to prevent the unauthorized disclosure of confidential information stored on these devices.

I commissioned an IT audit of three MDAs, namely the Ministry of Science, Energy and Technology (MSET), eGov Jamaica Limited (eGovJa) and the Post and Telecommunications Department (PTD) to determine whether the entities had implemented adequate controls to preserve the confidentiality of information prior to the disposal of ICT equipment and related storage media. The audit revealed that all three entities had a high risk of unauthorized disclosure of confidential information because their control systems were inadequate to ensure that sensitive information was safeguarded before the disposal of their ICT equipment. Steps need to be taken to strengthen their control systems to ensure that confidential information is preserved and proper records are maintained as evidence of the media sanitization undertaken.

This report is intended to assist all three entities to enhance their IT control systems in order to reduce the likelihood and or impact of IT security risks on their operations. It is therefore crucial that the management of MSET, eGovJa and PTD carefully review the recommendations contained in this report with a view to strengthening their control systems by adopting the measures outlined.

I wish to thank the management and staff of MSET, eGovJa and PTD for the courtesies extended to my staff during the audit.

Pamela Monroe Ellis, FCCA, FCA
Auditor General

This page was intentionally left blank.

EXECUTIVE SUMMARY

The National Development Plan, Vision 2030, identifies the Information and Communications Technology (ICT) industry as a key contributor to the nation's competitiveness and development and as such is linked to two National Outcomes, number 11 – "A Technology-Enabled Society" and number #12 "Internationally Competitive Industry Structures". It is envisaged that an advanced ICT industry will be developed to achieve sustained global competitiveness and enhance the productivity of our goods and service sectors. However, with the increased use and dependence on technology there are increased information security and environmental risks associated with the disposal of electronic waste (e-waste).

We undertook an IT audit of the Ministry of Science, Energy and Technology (MSET), Post and Telecommunications Department (PTD) and eGov Jamaica Limited (eGovJa) to determine whether they had implemented adequate controls to minimise the information security risks associated with the disposal of ICT equipment. The audit involved a review of each organization's general computer controls, systems and procedures in particular those relating to information security over the disposal of ICT equipment.

Key Audit Question

Was an effective information security management system in place to safeguard the confidentiality of information prior to the disposal of ICT equipment?

What we found

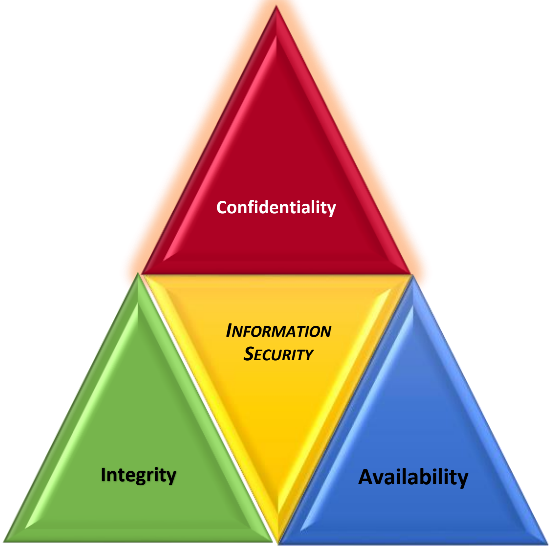
All three entities had a high risk of unauthorized disclosure of confidential information because their control systems were inadequate to provide reasonable assurance that sensitive information was safeguarded prior to the disposal of their ICT equipment.

Both MSET and eGov were vulnerable to information security threats due to inadequate access controls.

Inadequate Information Security Controls in the Disposal of ICT Equipment

1. Our review of the information security controls over the disposal of 479 ICT devices (laptops, desktops, servers and networking equipment) at MSET, eGovJa and PTD revealed that the entities did not maintain any record of the steps taken to secure confidential information stored on the devices prior to disposal for the period under review. The entities indicated that low level formatting was done on the devices, however, no record of this was maintained. There was also no evidence that every device was examined to determine if confidential residual data remained prior to disposal. Consequently, we were unable to determine whether the appropriate data sanitization and security procedures were conducted prior to the disposal of these ICT devices. An examination of 30 *Closed User Group (CUG)* mobile phones scheduled for disposal by MSET revealed that 15 phones were not subject to any sanitization procedures. Nine phones contained confidential information such as official emails, messages, contacts, images and videos, while six were locked by a third party application, which increased the risk of unauthorized disclosure of the Ministry's confidential information.

Figure 1: Key Concepts of Information Security



Source: Auditor General's Department

The entities subsequently indicated that the necessary steps will be taken to secure information on their ICT equipment, improve record keeping and documentation to provide assurance that confidential information is safeguarded prior to the disposal of ICT devices.

Inadequate Access Controls

2. We found that MSET had an increased risk of unauthorised access due to weaknesses in its password policy that allowed users to freely reuse old passwords and create weak passwords to authenticate their identity. The risk of IT security breaches going undetected was also high because the Ministry's network was not configured to identify and prompt for further review of unsuccessful log-on attempts.

The Ministry has since indicated that all matters concerning access controls will be investigated and its systems will be appropriately configured.

3. An examination of eGovJa's access controls revealed that there was a lack of compliance with its own information security policy in relation to password controls that could expose eGovJa to serious security breaches. We found that aspects of the company's Active Directory were not configured in accordance with its approved password policy. Additionally, the system's password complexity requirement was disabled and the minimum password length was less than the industry recommended best practice.

eGovJa has since indicated that the password structure for its Active Directory was reviewed and adjusted to ensure that it is in keeping with the company's password policy.

What should be done

MSET, PTD and eGovJa should strengthen their information security and related controls over the disposal of ICT equipment to preserve the confidentiality of the information stored on their devices. Further, to reduce the risk of unauthorised access and ensure the integrity and availability of their data and networks, MSET and eGovJa should take the necessary steps to improve their access controls.

PART ONE

Audit Objective, Scope and Approach

1.1 In keeping with my constitutional mandate, I commissioned an IT audit of the Ministry of Science, Energy and Technology (MSET), eGov Jamaica Limited (eGovJa) and the Post and Telecommunications Department (PTD) to determine whether the three entities had implemented adequate controls to preserve the confidentiality of information prior to the disposal of ICT equipment and related storage media.

1.2 The audit involved a review of each organization's general computer controls, systems and procedures in particular those relating to information security over the disposal of ICT equipment. Our audit was conducted in accordance with International Standards of Supreme Audit Institutions (ISSAIs).

1.3 Using a risk based audit approach we reviewed official documents, records and other related information, observed processes and conducted interviews with senior officers and staff of each entity. We also compared existing general computer controls against international benchmarks and widely accepted best practices within the ICT sector.

PART TWO

Ministry of Science, Energy and Technology (MSET)

Background

1.1 The mission of the Ministry is to develop science, energy and technology policies that fuel growth. Its aim is to transform Jamaica's science, energy and technology sectors to ensure energy security, improved quality, affordability and access to information, modernized ICT infrastructure and to facilitate the wide-spread application of science, technology and innovation towards sustained national development. The Ministry's vision is to create an environment, through policy development and a progressive legislative framework that facilitates investment, creates jobs and meaningfully improves the well-being of each Jamaican.

1.2 The Ministry, through its Information and Communications Technology (ICT) Division, is currently pursuing the ICT transformation of the Government, which is guided by the *Blueprint Report* prepared by Jamaica's Chief Information Officer (CIO). The Office of the CIO was established in April 2015 to provide the technology vision and leadership in the development and implementation of the Government of Jamaica (GoJ) ICT strategies, policies, initiatives, projects and programmes. In keeping with that mandate, the Blueprint report was prepared in August 2016 as a road map and five-year action plan to transform the organisation and management of ICT in the public sector. The transformation process will include the introduction of an ICT support process, ICT performance management, information management, e-government initiatives, enterprise content management and shared ICT services within the public service.

Inadequate Access Controls

1.3 Access controls provide the first line of defence against unauthorized users. Accordingly, best practice recommends that access control policies be developed based on the established levels of data sensitivity and used as a basis for assigning user privileges in keeping with employee job roles and functions. An examination of the Ministry's access controls revealed that its default password policy settings were not defined to enforce controls relating to password history, password length or complexity. Consequently, users were able to freely reuse old passwords and create weak passwords to authenticate their identity, resulting in an increased risk of unauthorised access. Additionally, 26 active domain users and three administrator accounts did not require periodic password change. We also found that the Ministry's network was not configured to identify and prompt for further review of unsuccessful log-on attempts in order to reduce the risk of IT security breaches going undetected.

1.4 The Ministry has since indicated that all matters concerning access controls will be investigated and the related systems appropriately configured.

Inadequate Information Security Controls in the Disposal of ICT Equipment

1.5 MSET should establish formal procedures for the appropriate disposal of all its ICT equipment in order to minimise the risk of unauthorized disclosure of confidential information. These procedures should be proportional to risks and take into consideration the removal of data, disposal of equipment based on their security classification, secure storage of devices prior to disposal and the maintenance of relevant disposal records as audit trail.

1.6 The Ministry's disposal document, though in draft specifies the policy and procedures for the disposal of computer equipment and peripheral devices (including personal computers, servers, hard drives, laptops, smart phones and handheld computers, printers, scanners, typewriters, compact discs). It stipulates that all data should be removed using a disk sanitizing software that cleans the media by overwriting each disk sector. It also states that the equipment should be labelled with a sticker indicating the date and initial of the officer who performed the disk wipe. However, despite developing a policy, MSET had no record of the steps taken to secure confidential information stored on 43 of its ICT devices *(laptops and desktops)* that were disposed of during the period under review. The Ministry indicated that low level formatting was done on the devices, however, no record of this was maintained. There was also no evidence that each device was examined to determine if confidential residual data remained on them prior to disposal. Additionally, we found that 15 of the 30 *Closed User Group (CUG)* mobile phones scheduled for disposal by the Ministry were not subject to any form of data sanitization to prevent the unauthorized disclosure of confidential information. We identified official emails, messages, contacts, images and videos on nine of the phones while the other six phones were locked by a third party application.

PART THREE

eGov Jamaica Limited

Background

3.1 eGov Jamaica Limited (eGovJa) is a government company that offers ICT services to Ministries, Departments and Agencies (MDAs). The company was incorporated under the Companies Act as a limited liability company on April 15, 1985 and was formerly known as Fiscal Services Limited (FSL). FSL was initially an agency of the Ministry of Finance with responsibility for the computerisation of the revenue departments and provision of ongoing technical support for the systems and services implemented. However, based on the Government's plan to transform ICT in the public sector, Cabinet approval was given in 2013 for the repositioning of Fiscal Services Limited (FSL) as the entity with responsibility for implementing ICT projects across the public sector. The revised mandate resulted in a change in the portfolio ministry and business name to reflect the expanding role of the organization.

Inadequate Access Controls

3.2 An examination of eGovJa's access controls revealed that there were deviations between its information security policy and some system configurations. For example, aspects of the company's Active Directory were not configured in accordance with its approved password policy. The policy required that the organisation's systems be configured to record previously used passwords, prevent the reuse of recent passwords[1] and include a maximum defined password age. However, our review of the system's password policy settings revealed that the number of previous passwords remembered by the system was less than the required number and the actual maximum password age was twice the period outlined in the organisation's policy. Additionally, the system's password complexity requirement was disabled and the minimum password length was less than the industry recommended best practice.

3.3 Lack of compliance with its own information security policy could expose eGovJa to serious security breaches leading to a compromise of its operations. eGovJa has since indicated that the password structure for its Active Directory was reviewed and adjusted to ensure that it is in keeping with the company's password policy.

Inadequate Information Security Controls in the Disposal of ICT Equipment

3.4 Despite having a policy in place to guide the secure disposal of ICT equipment, eGovJa had no record of the steps taken to secure confidential information that was stored on 265 of its ICT devices *(laptops, desktops, servers and networking equipment)* that were disposed of during the period under review. The company indicated that low level formatting was done on some

[1] *Specific number of recent passwords is not published for security reasons.*

of the devices while others were physically destroyed, however, no record of these activities was maintained. There was also no evidence that the devices were examined to determine whether l residual data remained on them prior to disposal. Consequently, there was no assurance that the appropriate data sanitization and security procedures were conducted prior to the disposal of the ICT equipment.

3.5 eGovJa acknowledged the shortcoming and indicated that the necessary steps will be taken to improve its record keeping and documentation to ensure compliance with its disposal policies and provide assurance that confidential information is secured prior to the disposal of its ICT equipment.

PART FOUR

Post and Telecommunications Department (PTD)

Background

4.1 The Post and Telecommunications Department (PTD) has responsibility for the postal services in Jamaica and is governed by the Post Office Act. The PTD is a Principal Receiver of Revenue responsible for the dissemination of letters and parcels within Jamaica and overseas in line with international standards established by the Universal Postal Union. PTD through partnerships with public and private sector entities also offers bill payment services, Smarter Card refills, phone cards sales, Internet Café services, PATH welfare and NIS payments at selected post offices island wide.

4.2 However, with the advancements in technology and increased competitiveness in the delivery industry, the PTD has sought to transform its operations by implementing a five step modernization plan focused on the rebranding and promotion of the zip mail service, introduction of mobile post offices and post shops; development of a model post office and the installation and deployment of IT infrastructure. Upgrades to the information technology infrastructure has allowed for improved communication between the locations and supported the automation of counter services, which has enhanced the efficiency of staff and reduced some operational cost.

Inadequate Information Security Controls in the Disposal of ICT Equipment

4.3 Our review of PTD's information security controls over the disposal of its ICT equipment revealed that PTD did not maintain any record of the steps taken to secure confidential information that was stored on 171 of its ICT devices that were disposed of during the period under review. The Department indicated that low level formatting was done on the devices, however, no record of this was maintained. There was also no evidence that independent verifications were conducted to determine if residual data remained on the devices prior to disposal. Additionally, PTD did not implement the policy and procedures to ensure that confidential information was removed from assigned mobile phones (CUGs) prior to their disposal. Consequently, there was no assurance that the appropriate data sanitization and security procedures were conducted prior to the disposal of the PTD's ICT equipment. This increased the risk of unauthorized disclosure of the Department's confidential information.

4.4 PTD subsequently indicated that the necessary steps will be taken to secure information on its ICT equipment and improve its recording keeping and documentation to provide assurance that confidential information is safeguarded prior to the disposal of its ICT equipment.