ANNEX B

POLICY: Information Technology Security

Effective Date: 27 October 2015

Version: 3

Revised: 29 October 2015

1.0 BACKGROUND

Information Technology Systems are critical to conducting business through out the Government. Therefore it is important to safe guard against security threats.

2.0 POLICY STATEMENT

It is the policy of the Bermuda Government to safeguard the integrity, sustain the availability and preserve the confidentiality of the Government's digital information and digital assets.

3.0 APPLICATION

The Bermuda Government Security Instructions state "Public Officers have a duty to protect all official documents and information whether security classified of not". Accordingly, this policy applies to Public Officers, that are supported by the Information Technology Office (ITO), or any other entity connected to or given authorized access the Government information technology (IT) systems.

This policy does not apply to Bermuda Hospital, Bermuda Police Department, Department of Education, Quangoes or entities not supported by ITO.

This policy:

(i) is the point of reference for all other policies, procedures and standards that address or impact security of the Bermuda Government IT Systems;

(ii) will apply in conjunction with the policies in (i) above and in the event of any conflict will take precedence, and in cases where Laws, regulations or other statues governing the security of information apply, those requirements will take precedence.

4.0 DEFINITIONS

4.1 **"Access"** – means to instruct, communicate with, cause input, cause

output, cause data processing, or otherwise make use of any resources of a Computer Device, Application or IT System. Use includes printing and viewing.

4.2 **"Application"** – means a computer program/software designed for a specific task or use.

4.3 "**Authorisation**" - means having the consent or permission of an owner, or of the person licensed or authorized by the owner to grant consent or permission to access a Computer Device, Application or IT System in a manner not exceeding the consent or permission.

4.4 **"Authorised Applications"** – means Applications necessary for business purposes and approved as such by the Director of the Information Technology Office (ITO).

4.5 **"Cloud"** – means system software, Applications or other computer services hosted on and accessed by the Internet.

4.6 **"Computer Device"** – means laptop computers, desktop computers, tablets, phones or printers.

4.7 **"Critical IT Systems"** – means the list of IT Systems and Applications approved by the Government as being the first systems to be restored in the event of a disaster.

4.8 **"Data"** – includes data and information required to carry out the business, services and mission of the Bermuda Government. Data may be stored on IT Systems, removable media, or computer devices.

4.9 **"Employee"** – any Public Officer who works for the Government of Bermuda on a full-time, part-time or casual basis, including any consultant, contractor, service technician, vendor or other similar person.

4.10 **"Externally Hosted"** – means the Application, Data and computer hardware and software are located where the ITO does not own or manage the physical location. Phyical custody is provided by a non-Bermuda Government entity.

4.11 **"Information Technology (IT) Systems"** – means the logical and/or physical computer network and any device that is owned by the Bermuda Government and/or used for government business whether or not it is physically connected to the government network.

4.12 **"Public Officer"** – means the holder of any public office and includes a person appointed to act in any public pubic as defined in Bermuda

Constitution Order 1968.

5.0 AUTHORITY

This policy is issued under the authority of the Government of Bemuda.

This policy replaces the Policy Statement, Computer Security Instructions Version 1.8 – 20 October 2006

6.0 REQUIREMENTS / STANDARDS

6.1 Responsibilities

6.1.1 The ITO is responsible for the promotion of IT Systems security throughout the Bermuda Government, including the review and approval of associated policies.

6.1.2 Applications and associated Data will be owned by an explicitly stated Department and the Department will be referred to as the "Application Owner". In the absence of such a Department then the ITO will by default become the Application Owner (e.g. e-mail).

6.1.3 The ITO is responsible for maintaining and publishing a list of business Applications and owners. Department Heads are responsible for ensuring that details of their Department's business Applications are provided to ITO for inclusion in this list.

6.1.4 Department Heads are responsible for reviewing the business Applications list annually and informing the Director of the ITO of any changes to be made to the Application list owned by their department.

6.1.5 The Bermuda Government Security Instructions state "the unauthorised disclosure of material from a Government computer system (even though the individual items of information may not be classified) can bring the security system into disrepute". Accordingly, Department Heads are responsible for working with the ITO Security Manager to ensure appropriate security controls have been established and implemented for Applications which their department is identified as the Application Owner.

6.1.6 Department Heads must ensure all Bermuda Government equipment is returned and Bermuda Government Applications and Data is removed from Employee owned devices before the final pay check is issued. The ITO will provide a means to remove Data from Employee owned devices.

6.1.7 Department Heads are responsible for ensuring compliance with this policy within their departments.

6.2 Access Control

6.2.1 The Director of ITO or an authorized designee is responsible for granting Employees authority to physical access to IT Systems.

6.2.2 The Director of ITO or an authorized designee is responsible for ensuring that access to Applications and Data is granted as authorised by the Application Owner.

6.2.3 The Department Head or an authorized designee are responsible for granting employees authority to Applications and Data for which their Department is the owner.

6.2.4 Employees must not disclose their passwords to anyone and are accountable for the negligent disclosure and unauthorized use.

6.2.5 Computer Devices that contain Bermuda Government Applications or Data must be protected by a 'password' or other user identify standards authorized by the Director of the ITO.

6.2.6 Computer Devices, whether mobile or not, should be locked by password protection when an Employee is visited by individuals who should not have access or when an Employee leaves the computer device unattended for any length of time (i.e. end of work day or longer than a fifteen minute duration).

6.2.7 The Bermuda Government reserves the right to inspect any computer device that is part of the Bermuda Government IT System for violations of this policy.

6.2.8 Bermuda Government owned Computer Devices must be returned to the ITO when they are retired from service. This will mitigate risk of unauthorized access to and/or accidental disclosure of Bermuda Government Data stored on these devices.

6.2.9 Access to Bermuda Government IT Systems must be terminated no later then the date and time when the Employees contract, service agreement, service order or employment with the Bermuda Government ends.

6.2.10 Applications and or Data must not be copied or stored on any removable media, Computer Device, Externally Hosted IT System or moved to the Cloud unless it has been preauthorized by the by the Application Owner.

If authorization has been given, the Applications and Data must be appropriately secured by a method approved by the ITO Security Manager.

6.2.11 Downloading, installing and use of programs that provide the ability to crack or steal passwords are prohibited unless prior written approval from the ITO Security Manager is obtained.

6.3 Restrictions on use

6.3.1 IT Systems, Applications and Data are to be used in compliance with the Computer Misuse Act 1996 and IT related polices referred to in Section 8 of this policy.

6.3.2 Access to IT Systems, Applications and Data is restricted to authorised Employees only.

6.3.3 Employees will only be authorised to access those IT Systems, Applications and Data that are necessary to fulfil their employment responsibilities.

6.3.4 Employees must not access or attempt to access IT Systems, Applications and/or data to which they are not authorised.

6.3.5 Employees must not connect personally owned Computer Devices to the Government IT Systems unless they have obtained prior authorization from their Department Head. Personally owned Computer Devices used for Government business must be registered with the ITO via the ITO Helpdesk.

6.3.6 Employees must not store Bermuda Government Applications or Data on employee owned devices unless prior authorization has been obtained from the Department Head. Upon termination of relationship with the Bermuda Government, any information must be returned and the information wiped from the non-Bermuda Government owned system. The Bermuda Government reserves the right to verify the information has been removed.

6.4 Changes to IT Systems

6.4.1 Critical IT Systems, Applications and Data must have back up and recovery procedures that are agreed with the Application Owner.

6.4.2 Only authorised Employees may install or remove IT Systems and Applications. The Director of ITO is responsible for granting authority to Employees to install or remove IT Systems and Applications. Only Authorised Applications may be installed and/or used on IT systems.

6.4.3 Changes (modifications) to IT Systems and production Applications require the authorization of the Director of the ITO. Changes are authorized by securing approval through the ITO "Request for Change (RFC) Process".

6.4.4 Software that can be used to assess, evaluate and compromise the security of the IT Systems, Applications and Data is prohibited from installation unless prior approval is received from the ITO Security Manager.

6.4.5 Copyright laws and IT System license agreements must be complied with.

6.5 Virus, Malware & Intrusion Prevention

6.5.1 Computer Devices and servers connecting to the Government IT System must have ITO approved and updated anti-virus and anti-malware systems installed.

6.5.2 Security patches for servers and Applications must be kept current.

6.5.3 Industry standard network perimeter security measures along with intrusion detection systems must be maintained.

6.5.4 Applications exposed to the Internet must subject to vulnerability testing at system setup time and on a routine basis thereafter.

6.6 Externally Hosted Systems

6.6.1 The Permanent Secretary, Department Head and the Director of ITO must approve the use of Applications that are Externally Hosted or accessed via the Cloud.

6.6.2 Applications and Data residing on the Cloud or Externally Hosted must meet security standards approved by the Director of the ITO acting in accordance with this policy.

6.6.3 Minimum security requirements must be included in Vendor contracts hosting Bermuda Government Information/Data. The minium standard must include a means of recovery of Data to the Bermuda Government or transfer to the new vendor when the contract ends.

6.6.4 To mitigate security risks, contracts for Externally Hosted or Cloud based IT Systems and Applications must be reviewed by the ITO Security Manager before contracts are signed.

6.7 Ownership & Disposal

6.7.1 When ending an agreement with vendor for Externally Hosted Systems then the Bermuda Government Data stored on and Externally Hosted system must be returned to the Bermuda Government and wiped from the Externally Hosted system in such a fashion that it cannot be recovered. Language stipulating this requirement must be built into contracts that provide these types of services.

6.7.2 Bermuda Government owned Computer Devices or Servers that are deposed of, must be sanitized (i.e. all Bermuda Government information wiped and not recoverable) before leaving the custody of the department that owns it. This includes, but is not limited to:

- Equipment to be destroyed (i.e. at the end of its useful life)
- Leased equipment being returned or replaced (i.e. photocopiers)
- Equipment sold to employees or the public.

6.8 Security Awareness

Employees must receive IT security awareness and protective measures information at least annually and when security threats to IT Systems, Applications or Data are discovered.

7.0 ENFORCEMENT

7.1 Contravention of the policy

7.1.1 Employee violation of these policies and procedures is subject to disciplinary action as set out in the Code of Conduct.

7.1.2 Displinary Action necessary as a consequence of violation of this policy will be the joint responsibility of the Department Head and the Director of the ITO. The Director of the ITO will make recommendations whether disciplinary action should be taken and to what extent and the Department Head will make final decision and take action in accordance with appropriate disciplinary procedures.

7.1.3 Vendor violation of this policy may lead to the termination of contracts or business transactions by the Government.

7.2 Reporting

7.2.1 Employees are responsible for reporting any suspected or confirmed violation of this policy to their Department Head and the Director of ITO. Failure to report a violation is in itself a violation of this policyand will be addressed in accordance with "Section 7 Enformenent" of this policy.

8.0 REFERENCES

Internet and E-mail Usage Policy	Final 3.5	28 August 2006
APO13 – Manage Security	COBIT Version 5	
DSS05 – Manage Security Services	COBIT Version 5	
Bermuda Government Security Instructions		Nov. 1990

9.0 CONTACTS FOR MORE INFORMATION

For more information regarding this polices contact

- The Director of the Information Technology Office
  - Telephone : (441) 297-7733 or ito@gov.bm
  - Intranet site "itoshare" on any browser connected to the Bda Government Network.