ICT Policy

GOVERNMENT COMPUTER SYSTEM USAGE POLICY

1.0   Title

Government Computer System Usage Policy

2.0   Effective Date:

7 November 2009

3.0   Introduction

3.1   The Government computer system is an effective tool provided to government officers for their daily work. Appropriate use of the Government computer system   shall ensure that government officers will provide effective and efficient services.

4.0   Definitions and Interpretations

4.1   As used in this these document, the following terms shall have the following meanings, except where the context otherwise requires:

4.1.1   Agency - Any Government ministry or department including educational institutions and statutory board.

4.1.2   Application Systems – From systems software that includes operating systems, compilers, and utilities for managing computer resources. To application software (end-user programs) which includes database programs, word processors, and spreadsheets.

4.1.3   Computer Systems - Desktop or Personal computers, notebooks, network computers, pocket PCs, mobile devices and personal digital assistants that are used to store, process or access Government Resources.

4.1.4   Government – The Government of His Majesty the Sultan and Yang Di-Pertuan of Brunei Darussalam

4.1.5   Government Resources - All Government data, hardware or software implemented for official use by the Government and its authorised personnel.

4.1.6   Head of Agency - The term refers to the Permanent Secretary of Government Ministry, Head of Government Department, and CEO of Statutory Board.

4.1.7 Official – This means any business related to the Government and/or agency.

4.1.8 User - The term encompasses full-time and part-time government employee, consultant, contractor, temporary, volunteer and any other worker at all levels within the government.

4.2 Abbreviations

4.2.1 EGLF - The E-Government Leadership Forum;

4.2.2 EGNC – The E-Government National Centre

4.2.3 EGTAB – The E-Government Technical Authority Body

5.0 Purpose

5.1 This policy establishes the principles and guidelines for the proper use of Government computer systems. These rules and guidelines aims to manage security risk exposure and misuse, and to protect the Users and the Government.

5.2 Access to computer systems owned or operated by the government imposes certain responsibilities and obligations and is granted subject to government policies and the security manual. Appropriate use of the Government computer system should always be legal, ethical, reflect honesty, reflect community standards, and show restraint in the consumption of shared resources. It should also demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individuals' rights to privacy and to freedom from intimidation, harassment, and unwarranted annoyance.

6.0 Scope

6.1 This policy applies to all Agencies and Users of the Government computer systems.

6.2 This policy covers all computer systems provided by the Government.

6.3 This policy covers any work related on the Government computer systems.

7.0 Reference

7.1 Laws of Brunei, Chapter 196, Electronics Transaction Act, 2008

7.2 Constitution of Brunei Darussalam Computer Misuse Order, 2000

7.3 Security Manual, Internal Security Department, Prime Minister's Office

7.4 Laws of Brunei, Chapter 116, Brunei National Archives Act, 1984

7.5 Laws of Brunei, Chapter 83, Public Officers (Conduct and Discipline) Regulations

7.6 Government Network Usage Policy (currently being developed)

8.0 Principles and Guidelines

8.1 The use of Government computer systems is not a right, and any inappropriate use will result in the cancellation of such use. The provision of the Government computer system is for official purposes only and only Government application systems shall be used.

8.2 Users shall not misuse the Government Computer Systems. Any misuse of the Government Computer Systems shall result in notification to the Head of Agency and revocation of the access. In addition, subject to disrepute under Regulation 29 of the Public Officers (Conduct and Discipline) Regulations and result in disciplinary actions, any unlawful violation may result in civil or criminal liability.

8.3 Personal use of the Government computer systems is permissible but must adhere to the following limitations:

8.3.1 It must be infrequent and brief, and not have any negative impact on the User's overall productivity;

8.3.2 It must not incur any additional expense to the user's agency or the Government;

8.3.3 It must not interfere with the normal operation of the user's agency or user's work; and

8.3.4 It must not compromise the user's agency or the Government in any way.

9.0 Guidelines on Policy and Procedure

9.1 General Policy and Procedure

Agencies shall put in place necessary policies and procedures to:

9.1.1 Safeguard the use of government resources;

9.1.2 Securely erase classified government data from storage media used on the computer systems;

9.1.3 Handle incident of loss or disclosure of government resources; and

9.1.4 Prevent unauthorised access to government resources.

9.2 Security procedures

Agencies shall develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional

information stored, and to impose appropriate penalties when privacy is purposely abridged. The security procedures should include the following:

9.2.1 Ensuring all desktop systems is installed with up-to-date anti-virus security software.

9.2.2 Scan computer systems for malicious codes prior to connecting to the government network.

9.2.3 Anti-malicious software must be enabled at all times.

9.2.4 Promptly update their computer systems with latest updates and/or patches.

9.2.5 Agencies shall immediately eradicate malicious code once discovered and prevent such codes entry to the government network.

9.2.6 Investigate point of entry and put in place policy and procedure to prevent similar incident in the future.

9.2.7 Report as required in the Security Manual, published by the Internal Security Department of the Prime Minister's Office.

9.2.8 And any other security measures in the Security Manual, published by the Internal Security Department of the Prime Minister's Office.

9.3 Connecting to Government Network

9.3.1 Only Government computer systems can be connected to the Government Network.

9.3.2 Any connections to the network must be scanned and clear of any malicious code before connecting.

9.3.3 A more comprehensive guideline on connecting to the Government Network is specified in the Government Network Usage Policy.

9.4 Anti-harassment procedures

Agencies shall develop, implement, maintain, and enforce appropriate procedures to discourage harassment through the use of government computer systems or networks and to impose appropriate penalties when such harassment occurs.

9.5 Upholding of copyrights and license provisions

Agencies shall ensure that its users will uphold copyright laws, laws governing access and use of information, and rules of organizations supplying

information resources to members of the community (e.g., acceptable use policies for use of Internet).

9.6   [intentionally left blank]

9.7   [intentionally left blank]

9.8   Agencies are responsible for the proper retention and deletion of documents in compliance with the Brunei National Archives Act.

9.9   End users shall:

9.9.1   adhere to the agency and government policy and procedure;

9.9.2   be accountable to confidential data residing in their computer systems;

9.9.3   report immediately any lost or stolen computer system to their CIO or appointed authority in their agency;

9.9.4   report to their agency (using the incident handling procedure) if their computer systems are being tampered with or infected by malicious codes;

9.9.5   be accountable for their password to their computer system which should not be disclosed to others.

10.0   [Intentionally left blank]

11.0   Ownership and Use of Computer Systems

11.1   All documents or files residing in the Government computer systems are the property of the Government of Brunei Darussalam. Agencies shall have the right to access and disclose any contents composed, sent or received using Government e-mail systems.

11.2   Agencies shall have an incident reporting framework to report misuse of computer and network systems.

11.3   Agencies shall appoint an approving authority for access and disclosure of contents when required.

12.0   Prohibited and Unacceptable Uses

12.1   Sharing of access

Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. Each User shall be responsible and accountable for any use of his or her account.

12.2 Unauthorised access

Users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users.

12.3 Use of privileged access

Special access to information or other special computing privileges are to be exercised in the performance of official duties only. Any information obtained through such special access or other special computing privileges shall be treated as private and confidential.

12.4 Libel, Slander and Harassment

12.4.1 Users shall not, under any circumstances, use government computer systems to libel, slander, or harass any other person.

12.4.2 Users shall not use the government computer systems to harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family.

12.4.3 Users shall not use the government computer systems to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection.)

12.4.4 Intentionally using the computer to disrupt administrative or related pursuits of another.

12.5 Game playing

Government computer systems are not to be used for recreational game playing.

12.6 Attempts to circumvent security

Users are prohibited from attempting to circumvent or subvert any system's security measures.

12.7 Decoding access control information

Users are prohibited from using any computer program or device to hack, intercept or decode passwords or similar access control information.

12.8   Denial of service

Deliberate attempts to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any government computer system are prohibited.

12.9   [intentionally left blank]

12.10 File sharing and P2P activities

Unauthorised file sharing and peer-to-peer (P2P) activities are not allowed on the government data network.

12.11 [intentionally left blank]

12.12 [intentionally left blank]

12.13 Use of copyrighted information and materials

Users are prohibited from using, inspecting, copying, disseminating, reproducing and storing copyrighted information and other material, without proper permission of the copyright owner.

12.14 Use of licensed software

Only Government approved software are to be installed on the computer systems.

12.15 [intentionally left blank]

12.16 Personal business

This policy restricts the use of government computer system for personal commercial gain or benefit.

12.17 Immoral Activities

It is forbidden to use the government computer system for immoral activities.

12.18 Damage to Computer Systems

Users may not damage Government Computer Systems.