Republic of Nauru

INFORMATION, COMMUNICATIONS & TECHNOLOGY POLICY

ICT ACCEPTABLE USE POLICY

MOANA-SHERNADE DAGEAGO – POLICY ANALYST & DRAFTING
DEPARTMENT OF INFORMATION, COMMUNICATIONS AND TECHNOLOGY
Government Building, Yaren District, Nauru

Table of Content

Purpose and Scope

“This policy defines end-user acceptable use of the Government’s IT resources. The policy applies to desktops, laptops, tablets, mobile phones, printers, networks and any other equipment provided by the Government for the purpose of creating, accessing, printing and modifying data.
Anyone that uses Government IT resources will be referred to as users which include staff (either temporary, trainee or permanent), consultants, contractors and visitors, must adhere to this policy. In addition, acceptable use applies to proper care and maintenance of equipment and following documented security policies relating to equipment use.”

User Responsibilities

All users shall use IT equipment responsibly and for official Government business purpose only.

For the purposes of this Policy:

I. Active desktops and laptops are not to be left unattended for prolonged periods of time. In addition, users should secure their workstations when leaving the workstation unattended.

II. Government information displayed on screens or reports shall be treated as confidential and private. Users must guard government information against unauthorized access or use. Any signed or implied confidentiality agreement shall fully apply to information accessed with government-owned IT equipment.

III. The respective Heads of Department are responsible for ensuring that their staff is adequately trained on the appropriate use of IT equipment and are adhering to this policy.

IV. Users shall not grant access to a non-employee, including vendors or contractors, without the approval of their respective Head of Department.

V. Users shall keep their equipment clean and free from dust. In addition, users shall maintain “breathing space” around equipment following equipment installation instructions.

VI. Users shall not eat or drink at their workstations especially near devices or Government Owned Equipment.

VII. This Policy applies equally to non-government-provided equipment if the equipment accesses government information or government network.

VIII. Users who have access to government information and computer systems from remote locations must adhere to this policy.

IX. The government-provided equipment shall be kept securely so that the staff household members and anyone else who is not authorized do not have access to the device when not in the office.

X. Users should not store approved critical government information or files locally on the hard drives except working documents only. The use of SharePoint or approved network drives for all government information is required.

XI. Users are responsible for backing up files stored on their desktop or laptop. The Department of ICT does not provide backups at the desktop level.

XII. Users are responsible for their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no circumstances should users share their password with another person.

XIII. Users should notify the Department of ICT helpdesk if they identify a possible security issue, which includes any attempt to gain unauthorized access to any system.

XIV. Users should notify the Department of ICT helpdesk if they receive any suspicious email. Users should not open email attachments from suspicious emails unless cleared by the Department of ICT.

XV. Users should always use email etiquette to write and respond to email messages.

Prohibited Practices

Any activity, action, or lack of action on the part of a user that causes or may cause damage or compromises security, or confidentiality is prohibited.

Prohibited practices include:

I. Installing new desktops and IT equipment without prior approval by the Department of ICT.

II. Upgrading equipment or adding peripheral equipment without the prior approval of the Department of ICT.

III. Downloading or installing programs that are not explicitly approved by the Department of ICT. Using unlicensed or pirated software is strictly prohibited. In addition, users may not copy and share software installed on their desktops or laptops with other users.

IV. Using programs or Internet websites that compromise the privacy of data.

V. Use of Government-provided internet (either through government network, mobile phone or portable MiFi)) for inappropriate use such as video streaming for entertainment purposes, playing games, social media browsing, providing a hotspot for others and other internet activities that may be classified as inappropriate depending on the nature of your job requirements.

VI. A user shall not attempt to gain unauthorized access to the Internet Service or to any other computer system through the Internet Service or go beyond his or her authorized access. This includes attempting to log in through another person's account or access another person's files.

VII. A user shall not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means.

VIII. Removing or compromising antivirus and other related device protection programs.

IX. Opening email attachments that are inappropriate or look suspicious. Guidance can be obtained from the Department of ICT on validating the authenticity of the emails.

X. Using Government-provided IT equipment and network for non-business reasons or for personal gain.

XI. Unauthorized attempts to break into any workstation.

XII. Unauthorized access to Government files, programs, databases or confidential information.

XIII. Sending or posting confidential files to unauthorized people.

XIV. Failing to fully cooperate with IT audits and IT security investigations.

XV. Allowing co-workers or other users to use devices without the approval of Director/Secretary or by the Department of ICT.

XVI. Sharing password information or displaying it in plain view on or around the desktop.

XVII. Users must secure their passwords and not reveal them to others.

Compliance

The Department of ICT will monitor and report violations of this Policy. This will be done through a combination of remote monitoring and on-site visits. Whenever any authorized IT professional is on-site at a location, he or she may test compliance levels at the individual desktop level.

In addition, the Department of ICT will also conduct quarterly IT Audits for inventory purposes and check compliance with this Policy.

Users who violate this Policy will have their network account suspended for a minimum of one week and/or referred to HR for further disciplinary actions. The Secretary for ICT will also be able to determine the penalty for violating this policy depending on nature and extent of violation.