Republic of Nauru

INFORMATION, COMMUNICATIONS & TECHNOLOGY POLICY

BRING YOUR OWN DEVICE (BYOD) 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 provides guidelines for the use of personally owned notebooks, smart phones, tablets and Laptops for government purposes. All staff who use or access Government's network technology equipment and/or services are bound by the conditions of this Policy.

Anyone that uses government IT resource from here on will be referred to as users include staff (either temporary, trainee or permanent), consultants, contractors, must adhere to this policy. In addition, this policy makes reference to other specific policies that require further elaboration.”

The purpose of this ICT policy as a whole is to:

- ensure that the ICT systems are used for its intended purposes
- define acceptable use of systems and use of government data
- follow government guidelines and applicable laws
- protect the government from any possible litigation
- establish processes for addressing policy violations and sanctions for violators

Mobile devices approved for Government Use

The following personally owned mobile devices are approved to be used for Government purposes:

I. **Notebooks and Laptops**

- May operate any operating system.
- It is mandatory to use a reputable anti-virus system into the device with up-to-date virus signatures.
- It is mandatory that the device is free from viruses.
- The device should not include any pirated software installations.
- Not all types of government services are suitable for all device types. The user must check with the Department of ICT and respective departments on compatibility.

II. Smart Phones and Tablets

- May operate any operating system.
- It is mandatory that the device is free from virus.
- The device should not include any pirated software installations.
- Not all types of government services are suitable for all device types. The user must check with the Department of ICT and respective departments on compatibility.

Registration of Personal Device

Employees when using personal devices for Government official business must register the device with the Department of ICT.

ICT will record the device and all applications used by the device.

This includes:

- Physical (MAC/IMEI) address of all network interfaces (Ethernet and Wifi)
- Operating System
- Registered User
- Details of hardware configuration
- Details of all installed software

An employee may only use his or her personal mobile device for the following purposes:

- Email access
- Government internet access for authorized work-related purposes only
- Government telephone calls

An employee who utilizes personal mobile devices agrees to:

- Not download or transfer government or personal sensitive information to the device.
- Not use the registered mobile device as the sole repository for government information. All government information stored on mobile devices should be backed up to government owned devices.
- The government will use MDM (mobile device management) to manage the device.

- make every reasonable effort to ensure that Department of ICT's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorized persons and all registered devices should be password protected

- ensure the device and all its software’s are up-to-date.

- Not share the device with other individuals ensuring to protect the government data access through the device

- abide by Department of ICT's internet policy for appropriate use and access of internet sites etc.

- notify Department of ICT immediately in the event of loss or theft of the registered device

- Not connect USB memory sticks from an untrusted or unknown source to avoid virus related issues.

All employees who have a registered personal device for Government use acknowledge that the Government:

- Owns all intellectual property created on the device

- Can access all data held on the device inclusive of work related data

- Will delete all data held on the device in the event of loss or theft of the device

- Has the right or option to buy the device where the employee wants to sell the device

- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data

- Has the right to deregister the device from government network at any time.

Keeping mobile devices secure

When handling mobile computing devices:

Mobile computer devices must always be kept securely and never be left:

- unattended in a public place,

- in an unlocked house,

- in a motor vehicle, even if it is locked.
- Mobile devices should be carried as hand luggage when travelling by aircraft

Compliance

The Department of ICT will monitor and report violations of all ICT Policies. 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 the policy.

Users who violate this policy will have their network account suspended for a minimum of one week and referred to HR for further disciplinary actions. If the matter is referred to the Human Resource Department for disciplinary process to commenced. The misconduct and the penalty will be in accordance with the Public Service (Disciplinary) Regulations 2020. The Secretary for ICT will also be able to determine the penalty for violating this policy depending on nature and extent of violation.