Republic of Nauru

INFORMATION, COMMUNICATIONS & TECHNOLOGY POLICY

EMAIL (NAURUGOV.NR) POLICY

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

Table of Content

Scope

This policy provides guidelines for the use of emails as a means for communication for all government purposes. All staff who use or access any form of email services for the purpose of their work 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 and visitors, must adhere to this policy. In addition, this policy makes reference to other specific policies that require further elaborations.

Purpose

The purpose of this ICT policy is:
• To ensure that the ICT systems are used for its intended purposes
• To define acceptable use of systems and use of government data
• To follow government guidelines and applicable laws
• To protect the government from any possible litigation
• To establish processes for addressing policy violations and sanctions for violators
This document sets forth the policy of the Department of ICT, nauru.gov.nr email exchange with respect to Government of Nauru - ICT email exchange. All public servants who use the government "nauru.gov.nr" email exchange is required to comply with this policy statement.

Government Email

Intended Use

All official email communications from the Government departments must use email address ending in domain.
The official email channel must not be used for personal purposes including signing up to social media accounts.

Ownership

The Government is the owner and custodian of all email communications within and outside the Government using its official email channel.
The Government is also liable for all communications through its official email channel and may require trails of emails in case of any breach or investigation.
The official email address ending with *.gov.nr* is reserved to be managed by the Department of ICT. Any unauthorized registration of .gov.nr domain is strictly prohibited unless an exemption is provided by Secretary of ICT. No other domain including naurugov.nr and naurugovernment.nr shall be permitted to be used for external communications.

Email Monitoring

The Department of ICT has the right to monitor email services ensuring compliance.
Monitoring of email does not explicitly imply reading of emails. Authorized ICT administrators only can see the senders, recipients and subject of the email while the body of the email remains confidential between the sender and receiver.

If the Department of ICT is required by law or is summoned by the court to provide email trails, the Department of ICT will then export the copies of the emails required and submit it to the authorities through the Secretary of ICT.
The Secretary for ICT will run audit on all administrator activities on a monthly basis to ensure compliance and integrity of the email services.

Prohibited Content
Official emails may not contain statements or content that are libelous, offensive, harassing, illegal, derogatory, or discriminatory. Foul, inappropriate or offensive messages such as racial, sexual, or religious slurs or jokes are prohibited. Sexually explicit messages or images, cartoons or jokes as well as chain messages either religious, financial or for luck are prohibited.

Access to email
All public servants who need to communicate electronically will need to apply for the email accounts. The ICT Form needs to be endorsed by their respective Secretary.

Security
The official email platform is only to be used by authorized persons. Users shall not disclose their passwords to others and may not use someone else's password without express written authorization from the Department of ICT.
Emails are not scanned for viruses at the server however they are scanned once email is opened on the User's devices. It is mandatory to have Sophos Anti-Virus installed on all windows devices where the files will be scanned as it is opened.
Use of email from devices which do not have the mandatory anti-virus installed is strictly prohibited.

Terminated/ Suspended Employees
For employees who have been terminated or suspended, the respective Department Secretary may ask for a copy of their emails by writing to the Secretary of ICT within 14 days of their termination/ suspension.
Allowing suspended or terminated staff to continue to access will also require a letter specifying the duration of access from the respective Secretary endorsed by HR to the Secretary of ICT.

Email forwarding
Authorized users are permitted to forward their emails to other colleagues' official email addresses while being away from work.
Forwarding all emails to personal emails like yahoo/ Gmail is strictly prohibited.

No Presumption of Privacy
While the Department of ICT will ensure appropriate patching and security controls are in place, there are new and emerging threats that still pose a risk to all ICT services throughout the world. For highly confidential emails that involve sensitive details such as credit card numbers, these

should never be sent through email. If there is dire need to send such an email, then only encrypted emails need to be sent. Refer to the Department of ICT Helpdesk for assistance on sending encrypted email messages.

Data Loss Prevention

It is forbidden to transmit highly confidential and proprietary data or information to anyone's personal email or with the intention to leak such data or information.

The Department of ICT may enforce settings such that the email server detects violations of Australian Financial Data, Australian Health Records Act, Australian Personally Identifiable Information Act and Australian Privacy Act and hence prevents such transmissions.

Spam Emails

Users are to ensure they inspect the email messages properly before opening. Spam emails crafted by hackers will look so legitimate that it can also bypass the email security solutions. Users who find suspicious emails in their mailbox needs to notify the Department of ICT Helpdesk immediately.

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 action. 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.