(DRAFT)
STATE OF HAWAII
Office of Enterprise Technology Services Policy No. 509
Secure Access Policy – Next Generation Network
Effective Date: xx
Revision No./Date: xx

INTRODUCTION

The purpose of the Secure Access Policy – Next Generation Network ("Policy") is to identify minimum requirements for authorizing any device, as appropriate, to connect to the State of Hawaii ("State") government network, the Next Generation Network ("NGN"). The intent of this Policy is to protect the integrity of State information technology infrastructure and private and confidential data.

SCOPE

This Policy applies to all users of the NGN.

This Policy applies to devices provided by the State that can connect to the NGN, including but not limited to smartphones, tablets, laptops and computers.

Each department, division and agency within the State may establish supplemental standards and procedures that enhance the Policy to meet other specific security requirements.

POLICY

NGN

Devices provided by the State may connect to the NGN, provided the devices meet applicable minimum requirements listed in Office of Enterprise Technology Services Policy No. 505.01, Secure Device Standards, as applicable. "Connect to the NGN" means connecting by direct cable or wirelessly to the NGN, or connecting to devices or local area networks that connect to the NGN.

Devices not owned or issued by the State (Non-State Devices), including personal devices, shall not connect to the NGN under any circumstances.

NGN Guest Network

To accommodate use of Non-State Devices, departments may install a guest network approved by the Office of Enterprise Technology Services and the department director or the director's designee, provided that the guest network requires network login credentials and has no connection to the NGN other than network transport to the Internet.

The State reserves the right to refuse or terminate, the connection of any device, without notice, if it appears the device is being used in a manner that puts the State's systems, data, employees, and/or customers at risk.

ADVISORY: CONNECTING DEVICES SUBJECT TO CONFISCATION, INSPECTION, AND/OR DISCOVERY

By choosing to connect a device to a State network or resource, the user acknowledges that the device may be subject to removal from the network, containment and/or confiscation and content inspection, if the device is found to be exhibiting questionable behavior, such as:

- imposing an exceptional load;
- exhibiting a pattern of network traffic that disrupts centrally provided services;
- exhibiting a pattern of malicious network traffic associated with scanning or attacking others;
- exhibiting behavior consistent with host compromise; and/or
- exhibiting behavior that is inconsistent and/or a violation of this Policy or other applicable State policies, such as Department of Human Resources Development Policy No. 103.001, Acceptable Usage of Information Technology Resources, as amended.

Emails may be subject to public records requests pursuant to Chapter 92F, Hawaii Revised Statutes, as well as litigation holds (requests by the Attorney General's Office to preserve records) and discovery for litigation purposes. Emails and other State of Hawaii data stored on devices such as smartphones, tablets, laptops, and computer workstations may also be subject these requests; and the devices, whether or not provided by the State of Hawaii, may be required to be turned over for review and production of data.