(DRAFT)
STATE OF HAWAII
Office of Enterprise Technology Services Policy No. 510
Secure Access Policy – Microsoft Office 365
Effective Date: xx
Revision No./Date: xx

INTRODUCTION

The purpose of the Secure Access Policy – Microsoft Office 365 ("Policy") is to identify minimum requirements for authorizing any device, as appropriate, to access Microsoft Office 365 cloud resources licensed to the State of Hawaii ("State"), while ensuring adequate security to safeguard State information technology infrastructure and protected information. The intent of this Policy is to protect the integrity of private and confidential data.

SCOPE

This Policy applies to all users of Microsoft Office 365 cloud resources licensed to the State.

This Policy applies to all devices, whether or not provided by the State, and related software applications and utilities that can connect to Microsoft Office 365 cloud resources, 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

Prior to connecting to Microsoft Office 365 cloud resources licensed to the State, all devices shall meet minimum requirements listed in Office of Enterprise Technology Services Policy No. 505.01, Secure Device Standards, as applicable. Devices failing to meet these requirements shall not be allowed to connect.

The State reserves the right to refuse 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.