	State of Connecticut **Office of Policy and Management**		
Policy Title:	**Personal Wireless Device Policy**		
Policy ID:	IT-SEC-12-01		
Version:	2.00		
Date Issued:	9/9/2020	**Date Effective:**	9/9/2020
Next Review:	9/9/2022	**Supersedes:**	Version 1.00 dated 2/15/2012
Scope:	Executive Branch Agencies	**Authority:**	C.G.S. § 4d-8a
Summary:	This policy defines the requirements to authorize a user to connect a personally owned wireless device to the State of Connecticut's enterprise electronic mail and calendaring system, other internet facing systems or for use when utilizing multi-factor authentication.		

Purpose

This policy defines the requirements to authorize a user to connect a personally owned wireless device to the State of Connecticut's Executive Branch electronic mail and calendaring systems, other internet facing applications (hereafter referred to as "the state systems") or to use a personally owned wireless device for use when authenticating with state systems that utilize multi-factor authentication (hereafter referred to as "multi-factor authentication".

For the purpose of this policy, a personally owned wireless device is defined as any cellular phone, smart phone, tablet or other similar portable device (hereafter referred to as "wireless device") that utilizes a cellular or wireless network to provide internet access and where such device has the capability to directly access the state systems.

Scope

This policy covers all State of Connecticut Executive Branch and Higher Education agencies including all employees and contractors whether permanent or non-permanent, full, or part-time (hereafter collectively referred to as "users") who access or use the state systems in the performance of their assigned duties.

This policy does not apply to the Judicial or Legislative Branches of government. However, these branches may consider adopting any or all parts of this policy for use within their own branches.

Authority

In accordance with C.G.S. § 4d-8a, the Office of Policy and Management (OPM) is

responsible for developing and implementing an integrated set of policies governing the use of information and telecommunications systems for state executive branch agencies.

Policy Statements

1. As necessary, agencies may establish or impose additional restrictions related to this policy that may be in the best interests of that agency. Any agency imposing additional restrictions must do so in written policy form, a copy of which is to be provided to the Office of Policy and Management and the affected employees, prior to the effective date of that agency policy. No agency policy may be less restrictive than this policy. The Director of Human Resources (or person serving in this capacity) within each State agency is responsible for addressing individual employee questions concerning this policy. The Office of Labor Relations will serve as consultant to agencies in this regard.

2. Users, at their request, may be granted the authority to configure their personally-owned wireless devices to access the email and calendar system, and other web based applications that do not locally process or store protected or confidential information under the following conditions:

    - The user understands and agrees that any such request is considered a personal convenience for the user and as such, the State will not reimburse or otherwise compensate the user for any costs associated with such access. Such costs may include, but are not limited to, monthly call and data plans, long distance calling charges, additional data or roaming fees, charges for excess minutes or usage, equipment, surcharges and any applicable fees or taxes
    - The user must complete a "Request to Use a Personal Wireless Device" form that designates requested applications to be accessed and receive the approval of their agency head or their designee prior to any such request being granted. The form will include the user's responsibilities described in this policy, the implementation procedures and any more restrictive agency policies. Approval is not required when using device for just multi-factor authentication.
    - The user understands that they may be held liable for any criminal and/or civil penalties that may result due to loss, theft or misuse of the confidential information accessed and/or stored on the personal device.
    - When accessing the state system, users recognize that the information being accessed by their wireless device is State property. Therefore, information created, sent, received, accessed or stored using a personal wireless device remains the property of the State.
    - Users agree to secure their wireless devices using a PIN, security pattern, password or other form of authentication as may be provided by the device manufacturer.
    - All activities involving the use of the state systems is considered state business. Therefore, users should be aware that they have no expectation of privacy in the use of these state resources. Users must also be aware that information stored, created, sent or received via State systems is subject to the Freedom of Information Act.
    - The user understands that they shall not be entitled to any additional compensation as a result of being granted their request to access the email

and calendar system on their personal device.

3. Users are expected to take the appropriate precautions to safeguard their personal wireless device against loss or theft. Users who experience the theft or loss of a device that has been authorized to access the state system must immediately report the incident to the Department of Administrative Services' Bureau of Enterprise Systems and Technology Help Desk by dialing (860) 622-2300.

4. No devices may connect to the state systems which have circumvented the security features from manufacturer specifications.

5. Users understand that utilizing their personal device for only multi-factor authentication does not make it subject to the Freedom of Information Act. No data or information is stored on the device in this use case. Other applications must be assessed on an individual basis to determine if any data is stored locally that may create a state record.

Compliance

Agency Heads are responsible for ensuring compliance with this policy and may appoint a responsible designee from within their agency for policy oversight and administration.

Services provided under this policy may be revoked when an employee has terminated his/her state service or due to a policy violation or if it is determined that access is no longer needed or beneficial to the agency.

Compliance with this policy is subject to audit by the Auditor of Public Accounts.

Implementation

The State's Chief Information Officer is responsible for developing and disseminating procedures and standards governing the implementation of this policy. Such procedures and standards are therefore considered an extension of this policy and compliance is required thereto.

Additional Resources

Acceptable Use of State Systems Policy

Policy on Security for Mobile Computing and Storage Devices