1.0 PURPOSE

State-provided wireless devices may be made available to any employee with management's approval. This policy establishes a framework for procurement, possession, and appropriate use of West Virginia state-owned and/or paid wireless communication equipment and/or service within the Executive Branch.

Wireless service includes, but may not be limited to the following: voice, data, text messaging, voicemail, caller ID, call waiting, call forwarding, and three-way calling.

2.0 SCOPE

This policy applies to all employees who use state-issued portable and/or mobile devices, unless classified as "exempt" in West Virginia Code Section 5A-6-8, "Exemptions." The State's users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

3.0 POLICY

3.1 Conditions of Use

3.1.1 The State has the right to monitor and review wireless devices for operational or management purposes.

3.1.2 Each agency is responsible for monitoring and controlling the wireless communication spending by its employees, and for keeping costs under control.

3.1.3 Wireless devices and service are intended to provide the means to enhance the staff's ability to conduct State business.

3.1.4 Personal use of wireless devices and service is prohibited except in certain limited and occasional circumstances that meet with the supervisor's approval. Personal use should only occur when it does not (1) interfere with the employee's work performance; (2) interfere with the work performance of others; (3) have undue impact on business operations; (4) incur incremental cost; or (5) violate any other provision of this policy or any other State policy, procedure, or standard. Use of wireless devices is a privilege that may be revoked at any time. (See Appendix A for more information.)

3.1.4.1 Employees must ensure that all non-business calls that would add incremental charges to the invoice are made at the employee's own expense, (e.g., charged to personal calling or credit cards, home telephones, or other non-State subsidized telephone numbers), and do not increase air time charges to the State.

3.1.4.2 The State reserves the right to address excessive personal usage and recover the cost of excessive personal usage from the user.

3.1.5 Employees will contact an immediate supervisor if there is doubt concerning authorization to access any State-provided IT resource, or if questions arise regarding an unacceptable use. If criminal activity is suspected or detected, reporting should occur up the supervisory or management chain without delay.

3.1.6 Employees should have no expectation of privacy regarding their use of wireless devices. The State reserves the right to review calls, voicemail messages, E-mails, text messages, etc., on all State-provided wireless devices.

3.1.7 The State will, consistent with applicable law and for any legitimate business reason, exercise its right to monitor, inspect, and/or review the contents of all State wireless devices at any time without the consent, presence, or knowledge of the affected employee.

3.1.8 Employees will not knowingly or inadvertently spread computer viruses. To reduce this threat, employees must not import files from unknown or questionable sources.

3.1.9 Reasonable precautions should be taken to prevent equipment theft and/or vandalism. **Employees must report lost or stolen devices as soon as the loss becomes apparent at WVOT's Incident Reporting Page -- https://apps.wv.gov/ot/ir/**

3.2 Procurement

3.2.1 The State will negotiate services with several cellular providers via statewide contract(s). All cellular services must be acquired through the statewide contract(s).

3.2.1.1 Individual agencies will not be authorized to create separate contract(s) with cellular suppliers.

3.2.1.2 The State reserves the right to change service or plans at any time, for any reason, when it is in the best interest of the State.

3.2.1.3 Wireless equipment and/or services obtained independently from the statewide contract(s) will not be eligible for State reimbursement.

3.2.1.4 Wireless integrated devices, “SmartPhones” (i.e. Blackberry, Treo, and personal digital assistants [PDA] with both voice and data capabilities), or air [edge] cards are available through the statewide contract(s), and are subject to the same qualifying criteria as standard wireless devices.

3.2.1.5 Agency leadership approval is required for all new orders and/or reassignments of service based on established and objective needs criteria.

3.3 Roles and Responsibilities

3.3.1 Supervisors will be responsible for the following:

3.3.1.1 Approving new service;

3.3.1.2 Terminating or reassigning service;

3.3.1.3 Recovering equipment or redistributing upon separation;

3.3.1.4 Tracking usage and spending; and

3.3.1.5 Adjusting service plans (as necessary) based on usage and spending;

3.4 Employees will be responsible for the following:

3.4.1 Responsible usage to minimize spending (i.e. use land line whenever possible);

3.4.2 Recommending service plan adjustments based on increasing or decreasing usage requirements; and

3.4.3 Protection of equipment to prevent loss, unauthorized use, or disclosure of sensitive information.

3.4.4 Employees must report the following instances to a supervisor or designated security contact:

- Receiving or obtaining confidential information to which the employee is not entitled (Note: the owner or sender of such information must also be notified);
- Becoming aware of breaches in security; or

- Becoming aware of any inappropriate use of State-provided IT resource.

3.5 The West Virginia Office of Technology (WVOT), working with the Department of Administration (DOA) Purchasing Division, will be responsible for the following:

3.5.1 Negotiating contracts with suppliers; and

3.5.2 Regularly monitoring industry pricing and plan changes; and updating contracts to utilize improved plans and pricing.

3.6 Establishing a Need for Standard Wireless Service

3.6.1 Several criteria exist for establishing an approved need for standard wireless equipment and/or service (the more criteria that apply, the higher the need and likelihood of approval). This criterion includes, but may not be limited to the following:

3.6.1.1 A requirement to travel frequently on State-related business with a need beyond a calling card;

3.6.1.2 Large amounts of time spent away from the office without access to a landline;

3.6.1.3 A need for other State employees to be in constant communication with the individual;

3.6.1.4 A need for the individual to communicate frequently to support state business objectives while traveling; and/or

3.6.1.5 A consistent need for business communication outside normal business hours

3.7 The WVOT, or a designated individual(s), will be responsible for loading portable devices with a standard configuration.

3.8 Each agency must maintain a list of the portable devices that it maintains in service, including:

3.8.1 Number of each device type,

3.8.2 Serial Number

3.8.3 Name of person to whom it was issued,

3.8.4 Date of purchase,

3.8.5 Date of the end of the warranty

3.8.6 Date issued

3.9 Working with the WVOT Cyber Security Office (CSO), agencies must develop procedures to keep accurate inventory of portable devices to maintain security patches and updates where applicable.

3.10 Each agency must verify this list by an annual physical audit of the following: device type, location, user, date issued, warranty expiration, and software installed.

3.11 Encryption

3.11.1 All portable devices must be encrypted if technically possible. Highly sensitive data must be safeguarded to a standard that reflects due care.

3.11.2 Encryption software will be installed and configured by the appropriate WVOT technician or a WVOT designated individual.

3.11.3 Due to the vulnerability of encryption keys remaining in computer memory, portable devices must be shut down completely when the device is in an unsecured location. Hibernation and stand-by modes should **not** be utilized. Examples of unsecured locations may include hotel rooms, vehicles, or unattended public locations.

3.12 Safeguarding Data from Unauthorized Viewing

3.12.1 Employees must take every precaution to ensure the privacy of information shown on the portable device's display or screen when in a public setting (e.g., hotels, airports, hospitals, dial-up modem access, Broadband access [wired or wireless Hotspots], or other private network access).

3.12.2 If the employee cannot restrict confidential and/or sensitive information on the screen from public view, the portable device **must not** be used.

3.13 All rules regarding the acceptable use of IT resources within State agencies apply to the utilization of portable devices. (See WVOT-PO1001 - "Information Security" policy and WVOT-PO1002 – "Acceptable Use of State-Provided Wireless Devices" policy for more information.)

3.14 Portable devices are not to be used as the primary storage location for any data. Data which is no longer in active use, or critical user data that is needed for an extended time, must be backed up to an alternate storage location or media and safeguarded.

3.15 Employees **must not** alter portable devices in any way. This includes, but may not be limited to, standard setup loads (e.g. productivity suite), as well as security and anti-virus software.

3.16 All portable devices will be configured with standard device firewall and encryption software, if available, and Virtual Private Network (VPN) software, if appropriate.

3.17 (Federal Tax Information) FTI, Protected Health Information (PHI), and Personally Identifiable Information (PII) should only be viewed or accessed on agency approved mobile devices:

3.17.1 Use of FTI, PHI, and PII may be viewed and accessed on laptops, if approved by agencies, if those laptops are encrypted and connected to the State network.

3.17.2 Virtual Private Networks (VPNs) must be used on any portable devices that will be used to access FTI, PHI, and/or PII.

3.18 The safety and security of the State network is the responsibility of each employee having access. Therefore, when using a portable device the following security rules apply:

3.18.1 Portable devices that can be connected to the network must be attached at least once every 14 days for a minimum of two hours and until all updates have been successfully loaded, to receive program updates, security patches, and anti-virus definition updates.

3.18.2 Portable devices connecting by dial-up must be connected directly to the network.

3.18.3 Portable devices that do not use dial-up must be connected via Broadband and VPN. Exceptions to this rule may include PDAs and SmartPhones.

3.18.4 The Configuration Management Group at WVOT is responsible for updating all laptops with necessary program updates, security patches, and anti-virus definitions.

3.18.5 Designated WVOT technicians will be responsible for updating portable devices used in WVOT-supported agencies with field offices.

3.19 Passwords

3.19.1 All portable devices must have password functionality enabled.

3.19.2 The auto lock feature must be set to a maximum one hour.

3.19.3 A default password will be assigned and installed by the appropriate WVOT technician or designated individual.

3.19.4 Employees will change the default password immediately after initial sign-on.

3.20 Physical Care

3.20.1 In all cases, employees must follow manufacturer's guidelines for portable device care and safe operation. In addition, the following safety precautions must be taken:

3.20.1.1 Employees must store the portable device within its case when not in use to protect it from dust and spills, for cushioning purposes, and to keep it with its cords and cables. (If a case is not available, effort must be made to afford the care a case would provide).

3.20.1.2 Employees must protect the portable device from harm due to environmental hazards. The portable device must be protected from temperature extremes at all times – never colder than 35 degrees or hotter than 95 degrees.

3.20.1.3 Employees must never leave the portable device unattended in a public place or exposed on public transportation. (This may include hotel lobbies, airports, taxis, trains, buses, subways, etc.)

3.20.1.4 When traveling by air, employees should always carry portable devices onto the plane. These devices must remain in the possession of the employee as hand luggage unless federal or state airline authorities require other arrangements.

3.20.1.5 If the portable device must be temporarily left in the employee's vehicle, it must be placed out of direct view.

3.20.1.6 Employees must not leave the portable device exposed to direct sunlight or near any heat source for extended periods of time.

3.20.1.7 Employees must keep liquids away from the portable device at all times to prevent spill damage.

3.20.1.8 Due to the potential damage from magnetic fields, employees must keep the portable device away from magnets, activated cell phones, electrical appliances, and powered audio speakers, as this exposure could compromise data.

3.20.1.9 Employees should consult the owner's manual for proper cleaning and maintenance of the portable device.

3.20.1.10 In order to prevent the loss of valuable information on the portable device, employees should anticipate the need for battery life by maintaining an appropriate charge and/or keeping a spare battery.

4.0 RELEVANT MATERIALS/DOCUMENTS

This policy is consistent with the following federal and state authorities:

- 45 Code of Federal Regulations (CFR) §§ 164.308-316
- Freedom of Information Act
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Privacy Rule
- NIST SP 800-14 and NIST SP 800-53
- State Health Privacy Laws
- WV Code § 5A-6-4a
- WV Executive Order No. 7-03
- WVOT Policies Issued by the Chief Technology Officer (CTO), www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx

5.0 ENFORCEMET

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action will be administered by the employing agency and may be based upon recommendations of the WVOT and the **West Virginia Division of Personnel**. Please review the **WVOT Policy and Procedure Policy #1000** to review additional provisions concerning enforcement and policy authority.

6.0 POLICY-SPECIFIC DEFINITIONS

6.1 Information Security Administrator (ISA) – The person designated by the agency head to assure the agency's compliance with State Information Security policies and procedures. The ISA is the agency's internal and external point of contact for all Information Security matters.

6.2 Information Security Liaison (ISL) - Employees assigned by the ISA to assist in the protection of information resources.

6.3 Personal Digital Assistants (PDA) – A handheld device that combines computing, telephone/fax, and networking features. A typical PDA can function as a cellular phone, fax sender, and personal organizer.

6.4 Security Contact – These individuals include the ISL or the ISA.

6.5 SmartPhone – A wireless handheld device that supports e-mail, mobile telephone, text messaging, web browsing and other wireless information services. (ex: iPhone, Android, Blackberry, Treo, etc.)

6.6 Wireless Device – Any device that can communicate with other devices without being physically attached to them. Most wireless devices communicate through radio frequency.

7.0 Change Log History

- July 1, 2015 –
  - Modified section 4.1.2, changed “department” to “agency”; Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions
- 9/1/2016 – Policy Reviewed. No edits made.

APPENDIX A: Acceptable/Unacceptable Use of State-provided Technology

Policy No: WVOT-PO1002

The information contained within this Appendix applies to the State of West Virginia Acceptable Use of State-Provided Wireless Devices policy.

Relevant technologies include, but may not be limited to the following:

(a) Personal computers;
(b) Personal Digital Assistants (PDA);
(c) Internet or Intranet;
(d) E-mail;
(e) Voice Mail;
(f) Cell phones (including camera phones and smart phones with data communications and databases);
(g) Pagers;
(h) Media including disk drives, diskette drives, optical disks (CD), tape drives, and USB drives (flash drives);
(i) Printers

Unacceptable uses include, but are not limited to the following:

(a) Any use which violates local, state, or federal laws;
(b) Any use for commercial purposes, product advertisements, or “for-profit” personal activity;
(c) Any use for viewing, transmitting, receiving, saving, or printing sexually explicit material;
(d) Any use for promotion of political or religious positions or causes;
(e) Any use in relation to copyright infringement;
(f) Any use in relation to participating in chain letters or unauthorized chat programs, or forwarding or responding to SPAM;
(g) Any attachment or use of devices on the State network that are not owned by the State or authorized by the WVOT;
(h) Redirecting State data to a non-State owned computing device or PDA on a routine basis, or without authorization from the CTO; or
(i) Any use in relation to downloading, attaching, changing, distributing, or installing any software or inappropriate files for non-business functions (ex: downloading MP3 files and/or broadcast audio or video files) including streaming content.
(j) Any use for promoting harassment or illegal discrimination on the basis of race, gender, national origin, age, marital status, religion, or disability;
(k) Any use for promoting the misuse of weapons or the use of devices associated with terrorist activities;
(l) Any use related to pyramid selling schemes, multi-marketing schemes, or fundraising for any purpose unless agency sanctioned;
(m) Any use for dispersing data to customers or clients without authorization;
(n) Any use in relation to placing wagers or bets;
(o) Any use that could be reasonably considered as disruptive to another’s work;
(p) Any sending or sharing of confidential information for unauthorized purposes;

APPENDIX A: Acceptable/Unacceptable Use of State-provided Technology

Policy No: WVOT-PO1002

(q) Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.

Employees will not knowingly or inadvertently commit security violations. This includes doing one or more of the following:

(a) Accessing or attempting to access records within or outside the State's computer and communications facilities for which the employee is not authorized; or bypassing State security and access control systems;
(b) Copying, disclosing, transferring, examining, re-naming, or changing information or programs belonging to another user unless given express permission to do so by the user responsible for the information or programs;
(c) Violating the privacy of individual users by reading e-mail or private communications without legal authority, or authorization based upon documented just cause;
(d) Misrepresenting oneself or the State of West Virginia;
(e) Making statements about warranty, express or implied, unless it is a part of normal job duties;
(f) Conducting any form of network monitoring, such as port scanning or packet filtering unless expressly authorized by the WVOT; or
(g) Transmitting through the Internet confidential data, to include without limitation, credit card numbers, telephone calling cards numbers, logon passwords, and
(h) other parameters that can be used to access data without the use of encryption technology approved by the WVOT.

Employees are prohibited from transmitting personal information about themselves or someone else without proper authorization while using State-provided IT resources.