STATE OF MARYLAND
DEPARTMENT OF HUMAN RESOURCES
OFFICE OF TECHNOLOGY FOR HUMAN SERVICES

ELECTRONIC COMMUNICATIONS POLICY

1.0 SCOPE:

This document sets forth policy of the Department of Human Resources, DHR, ("Agency") with respect to access, disclosure, recording, and general usage of electronic communications created, received, or stored through the use of the electronic communications systems owned, leased, or otherwise affiliated with the Agency and/or the State of Maryland ("State"). The purpose of this policy is to explain the ownership of the electronic communications created, received, or stored on the Agency's and/or State's electronic communications systems and to inform users of the systems about their rights and duties with respect to electronic communications.

This policy applies to users of Agency or State electronic communications systems and may be changed by the Agency, in its discretion, without prior notice. This policy is in addition to and not in replacement of any other policy or code of conduct of the Agency, State, or other State agencies.

2.0 DEFINITIONS:

Term	Definition
Electronic Communication	Including, but not limited to, messages, transmissions, records, files, data, and software, whether in electronic form or hardcopy.
Electronic Communication Systems	Including, but not limited to, hardware, software, equipment, storage media, electronic mail, telephones, voice mail, mobile messaging, Internet access, and facsimile machines.
Network	A computer network is a system for communication among two or more computers.
User(s)	Person(s) using Agency or State electronic communications systems including, but not limited to, employees, public officials, contractors, consultants, temporary employees and other individuals affiliated with Agency and/or State operations.

3.0 POLICY:

The Agency encourages the use of electronic communications and electronic communications systems to enhance efficiency. Electronic communications and electronic communications systems are to be used for business purposes in serving the interests of the Agency, the State, and the citizens, visitors, and commerce partners of the State of Maryland. All electronic communications created, received, or stored on the Agency's or State's electronic communications systems are the sole property of the Agency and/or State and not the author, recipient, or user. Furthermore:

1. Any non-government business use or intentional misuse of the Agency's electronic communications systems is a violation of this policy. Non-government business uses include, but are not limited to:

    - Sending and responding to lengthy private messages,
    - Sending political messages,
    - Operating a business for personal financial gain, and
    - Purchasing goods or services for private uses.

2. Intentional misuse includes, but is not limited to, receiving, displaying, storing, or transmitting threatening or sexually-explicit images, messages, or cartoons as well as epithets or slurs based upon race, ethnic or national origin, gender, religious affiliation, disability, or sexual orientation and harassing, offensive, discriminatory, or defamatory communications or images without a government business purpose. It also includes attempting to access a secure database, whether private or public, without permission.
3. The Agency's electronic communications systems may be used for minor, incidental personal uses, as determined by management that are not intentional misuses. Personal use shall not directly or indirectly interfere with the Agency's business uses, directly or indirectly interfere with another user's duties, or burden the Agency with more than a negligible cost.
4. Users shall have no expectation as to the privacy or confidentiality of any electronic communication, including minor incidental personal uses.
5. The Agency reserves and will exercise the right to access, intercept, inspect, record, and disclose any and all electronic communications on the Agency's and/or State's electronic communications systems, including minor incidental personal uses, at any time, with or without notice to anyone, unless prohibited by law or privilege.
6. The Agency reserves the right to monitor compliance with this policy by accessing, intercepting, recording, or disclosing any electronic communications , including minor incidental personal uses, unless prohibited by law or privilege.
7. The Agency reserves the right to access, intercept, inspect, record, and disclose any electronic communications during or after normal working hours and even if the electronic communications appear to have been deleted from the electronic communications systems. The use of an Agency or State password shall not restrict the Agency's right to access electronic communications.
8. Supervisors have the authority to determine when employee personal use exceeds minor, incidental, or inappropriate.
9. Authorized users are responsible for the security of their passwords and accounts. Users shall not disclose their passwords unless authorized by the Agency or disclosure is necessary to support the business of the government.
10. Users are not permitted to hinder or obstruct any security measures instituted on the Agency's electronic communication systems.

4.0 ACCEPTABLE USE:

The following activities are examples of acceptable use of agency electronic communications:

1. Send and receive electronic mail for job related messages, including reports, spreadsheets, maps etc.
2. Use electronic mailing lists and file transfers to expedite official communications within and among state agencies, as well as other job related entities.
3. Access on line information sources to gather information and knowledge on state and federal legislation, industry best practices, or to obtain specialized information useful to state agencies.
4. Connect with other computer systems to execute job related computer application, as well as exchange and access datasets.
5. Communicate with vendors to resolve technical problems.

5.0 UNACCEPTABLE USE:

The following activities are examples of unacceptable use of agency electronic communications:

1. Engaging in any activity that is illegal under Local, State, Federal or International law in conjunction with the usage of the Agency's electronic communications systems.

2. Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations.

3. Unauthorized reproduction of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Agency or the user does not have a specific and active license.
4. Exporting software, technical information, or technology in violation of International or regional export control laws.
5. Introduction of malicious programs into the Agency's or State's electronic communications systems infrastructure including, but not limited to, computer workstations, servers, and networks.

6. Circumventing user authentication or security of any account, host, or network, including disclosing a user's password to others or allowing a user's account to be used by others.

7. Interfering with or denying electronic communications system services to any user.

8. Inappropriate purposes, in violation of the intended use of the network, as defined by this policy and DHR.

9. Private, commercial purposes such as business transactions between individuals and/or commercial organizations

10. Interference or disruption of network users, services, or computers, including distribution of unsolicited advertising, and/or propagation of computer viruses

11. Effecting security breaches or disruptions of any electronic communications system. This includes, but is not limited to tampering with the security of State owned computers, network equipment, services or files.

6.0 STATE INFORMATION TECHNOLOGY POLICY AND STANDARDS:

Users of Agency or State electronic communications systems should also familiarize themselves with applicable State Information Technology Policy and Standards. The State Information Technology Security Policy and Standards are available at: http://doit.maryland.gov/support/Pages/SecurityPolicies.aspx

7.0 POLICY VIOLATIONS:

Violations of the policy governing electronic communications may result in restriction to access to Agency and/or State electronic communications systems without notice and without the consent of the user. Additional disciplinary action, up through termination, may be warranted.

8.0 END OF USE:

User's access to Agency electronic communications systems resources shall cease when one of the following occurs:

- Termination of employment.
- Termination of a contractor's or consultant's relationship with the Agency.
- Leave of absence of employee.
- End of public official's term.
- Lay-off of employee.

9.0 REPORTING LOST OR STOLEN EQUIPMENT:

OTHS has established an emergency contact number to use in the event your electronic equipment is lost or stolen. In such an event, it is imperative that you report the lost or stolen device as soon as you determine the device is missing to minimize the risk to DHR. The **EMERGENCY** contact number to call is **the OTHS Help Desk 410-767-7002 or 1-800-347-1350.** This is the 24/7 DHR Help Desk contact number to call any time of the day or night 365 days a year. To have a work order created, provide the information identified below:

Please provide the following information:

1. Your Name.
2. Equipment type (ex laptop, cell phone, blackberry, portable media device, etc.) , telephone number (if applicable), make, model, asset tag number, serial number or any other indentiying marking.
3. Time of the loss or theft.
4. Whether a police report has or will be filed. (Note a police report MUST be filed for all laptop thefts)
5. A contact number for you. (other than the BlackBerry or cell phone if it is lost or stolen).

Notification of the loss or theft of state issued equipment is mandatory. If your device is stolen, a police report should be filed and a copy of that report should be provided to the OTHS Security Director. Employees should be aware that they may be required to make restitution for loss or damage to state property due to their negligence per Maryland State Law. Employees may read more about this in the State Personnel and Pensions Article 11-107 (c).

10.0 NOTIFICATION AND RESPONSIBILITIES:

All users, including contractors and consultants, shall be notified of this policy and shall agree to comply with its terms as a condition for access to the Agency's systems by signing a copy of the Acknowledgment Form appended to this policy.

Supervisors shall be responsible for ensuring that the employees, contractors, consultants, temporary employees, and all other users are cognizant of this policy and sign a copy of the Acknowledgement Form appended to this policy. For State employees, a copy of the Acknowledgement Form shall be retained in the employee's personnel file. Supervisors shall retain copies of Acknowledgement Forms for all other users.