GEORGIA
DEPARTMENT OF NATURAL RESOURCES

Office of Human Resources
Standard Operating Procedure
HR SOP #404

Subject: Appropriate Use of Information Technology Resources

Effective Date: September 1, 2019

Policy Statement:

The agency's information technology resources are provided for official agency business use only. Inappropriate use of agency information technology resources by agency employees, interns, contractors, volunteers, etc. may result in disciplinary action up to and including dismissal from employment or termination of affiliation.

Definitions:

Information Technology Resources: Hardware, software, and communications equipment, including, but not limited to: personal computers, email, internet, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, and other relevant hardware and software items.

Information Security Officer (ISO): The ISO is designated as the Agency Computer Liaison. The ISO is delegated full authority to manage and control the uses and proscribe the procedures related to the agency's computer systems subject to the approval of the Chief Informational Officer (CIO).

Personally Owned Device: All devices and accompanying media (e.g. USB thumb and external hard drives) that are not DNR property. Examples are: smartphones, other mobile/cell phones, tablet computers, portable media devices, ~~PDAs~~, ultra-mobile PCs (UMPCs), laptop/notebook computers, home desktops, and/or any device capable of storing organizational data and connecting to a network.

Procedure:

All employees, interns, contractors, etc. must adhere to strict guidelines concerning the appropriate use of the internet and Information Technology resources.

Internet:

This policy applies to all users with access to the Internet and related services through the agency's network infrastructure. Internet related services include all services provided with the TCP/IP protocol, including but not limited to Electronic Mail (email), File Transfer Protocol (FTP), and World Wide Web (WWW) access.

Acceptable Use of the Internet:

Users are expected to use good judgment in the use of agency Internet resources; however, the final determination of appropriate use is determined by the Commissioner, or in EPD, the Director.

In addition to access in support of specific work related duties, the agency's Internet connection may be used for educational and research purposes.

Questions regarding what constitutes acceptable use should be directed to the user's supervisor. Management or supervisory personnel shall consult with the ISO for clarification of these guidelines.

Inappropriate Use of the Internet:

The agency's Internet access shall not be used:

- For any illegal or unlawful purposes. (i.e. the transmission of violent, threatening, fraudulent, pornographic, obscene or otherwise illegal or unlawful materials); or
- For commercial purposes; or
- For political purposes; or
- To perform work for profit with agency resources in a manner not authorized by the agency.

Users shall not:

- Attempt to circumvent or subvert security measures on agency network resources or any other system connected to or accessible through the Internet; or
- Use Internet access for interception of network traffic for any purpose unless engaged in authorized network administration; or
- Make or use illegal copies of copyrighted material, store such copies on agency equipment, or transmit these copies over the agency's network.

Email Usage:

Email is to be used for agency business and should not be misused. Users shall ensure all communication through agency email or messaging services is conducted in a professional manner.

DNR may access and monitor Department email at any time for any reason without notice. Users should not expect or treat email as confidential or private. Except for authorized DNR personnel, no one is permitted to access another person's email without consent. System users should exercise good judgment and common sense when distributing messages Client-related messages should be carefully guarded and protected, like any other written materials. Users must also abide by copyright laws, ethics rules and other applicable laws. Users should ensure that email messages are sent to only those users with a specific need to know.

Prohibited Use of Email:

Confidential information should never be disseminated to unauthorized sources. This includes the transmission of documents containing financial information or Social Security numbers. Users shall not reveal private or personal information without specific approval from

management. The transmission of email to large groups or messages with large file attachments should be avoided.

Sending harassing, abusive, intimidating, discriminatory, or other offensive e-mails is strictly prohibited. If users receive a message that contains defamatory, obscene, offensive or harassing information, or that discloses personal information without permission, they must report it immediately to the Human Resources Director. Do not forward the email. Use of the system to solicit for non-profit charitable organizations without the prior consent of the Commissioner is strictly prohibited. Chain-type messages and executable graphics files should be deleted and not forwarded because they cause overload on the agency's system.

Software:

Authorized Software:

Only software authorized and approved for office use will be installed on the agency's computer systems. No software or data files (whether proprietary, shareware, public domain, etc.) not generated within the agency system by agency personnel or their authorized agents, will be installed, downloaded or otherwise utilized on the agency's computer systems without the approval of the ISO. This policy applies to software installed on local drives as well as the network file server. See *Guidelines for the Acceptable Use of Microsoft Office 365* (Attachment 1).

Use of Personal Software:

DNR provides its users with the job required computing environment. To ensure the efficiency and supportability of agency computing resources, strict software configuration control procedures are required. The use of personally owned, unlicensed or unauthorized software on agency computing assets is prohibited.

Common Forms of Computer Abuse:

Privacy

- Attempting to access another user's files without permission;
- Furnishing false or misleading information or identification in order to access another user's account;
- Attempts to access DNR's computers, computer facilities, networks, systems, programs or data without authorization;
- Unauthorized manipulation of DNR's computer systems, programs or data.

Theft

- Removing computer equipment (hardware, software, data, etc.) without authorization;
- Copying or attempting to copy data or software without authorization;
- Abusing specific resources such as the Internet.

Vandalism

- Sending mail or a program which will replicate itself (such as a computer virus) or do damage to another user's account;
- Tampering with or obstructing the operation of DNR's computer systems;

- Inspecting, modifying or distributing data or software (or attempting to do so) without authorization;
- Damaging computer hardware or software.

Harassment

- Interfering with legitimate work of another user;
- Sending abusive or obscene messages via computers;
- Using computer resources to engage in abuse of computer service personnel or other users.

Neglect

- Spilling of liquid in or on computer systems causing damage;
- Mishandling of computer systems (dropping, etc.);
- Removal of outer casing or housing causing damage;
- Theft caused by user leaving laptop unattended.

Copyright Issues

- The copying, transmitting, or disclosing of proprietary data, software or documentation (or attempting to commit these acts) without proper authorization.

Miscellaneous

- Unauthorized and time-consuming recreational game playing;
- Using computer accounts for work not authorized by DNR;
- Sending chain letters or unauthorized mass mailings;
- Using the computer for personal profit or other illegal purposes;
- Personal and/or political advertisements.

Security:

Users who identify or perceive an actual or suspected security problem shall immediately contact the Agency's CIO, at Richie.Golden@dnr.ga.gov or (404) 218-4866.

Users shall not reveal account passwords or allow another person to use their account. Similarly, users shall not use the account of another user.

Access to agency network resources shall be revoked for any user identified as a security risk or a demonstrated history of security problems.

Users have responsibility for:

- Accessing information only in support of their authorized job responsibilities;
- Complying with Information Security procedures and with all established controls. See *Password Control Standards* (Attachment 2);
- Keeping personal authentication devices (passwords, PINs, etc.) confidential;
- Promptly reporting the loss or misuse of DNR information to the ISO;
- Initiating corrective actions when problems are identified;
- Ensuring that if data is accessed, it is not stored or accessed from any hardware that fails to meet the State of Georgia's established information technology security

standards in accordance with the Federal Information Security Management Act (FISMA).

Users must report a lost or stolen device that is connected to the DNR system to OIT immediately. See **http://dnrintranet.org/technology-services** for contact information. The device will be remotely wiped of all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning. Appropriate steps will be taken to ensure that agency data on or accessible from the device is secured - including remote wiping of the device where appropriate. The remote wipe will destroy all data on the device, whether it is related to agency business or personal.

Users agrees to immediately report any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of agency resources, databases, networks, etc. to his/her supervisor and OIT.

OIT may establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the organizational network, and the resulting reports may be used for investigation of possible breaches and/or misuse. User agrees to and accepts that his or her access and/or connection to DNR's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties.

Personally Owned Devices:

Any personally-owned computers used to connect in to the DNR network or DNR devices (such as your work computer) – either through DNR's SSL VPN or other methods (such as GoToMyPC) – must have up-to-date anti-virus and anti-malware software installed on it. This is a security requirement mandated by GTA. See **http://dnrintranet.org/it/antivirus**.

Personally-owned tablets, smartphones, and computers can freely access the individual user's Office 365 account – and any documents stored therein – by using smartphone apps and OneDrive. Personally-owned computers can also access the Department network and data through the Internet using a SSL VPN connection or other agency approved access software such as Touchdown and GoToMyPC. However, such personal computers must have sufficient anti-virus protection. (NOTE: Individuals desiring SSL VPN access must first have a SSL VPN account created for them, which incurs a monthly cost. The SSL VPN web address will then be provided to the user.)

All personally owned devices that are able to store data must be protected by a strong password. Users must agree to never disclose their passwords to anyone, including family members, or store passwords on personally-owned devices.

All users of personally-owned devices must also employ reasonable physical security measures. Users are expected to secure all such devices whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain department data.

Users must follow all approved data removal procedures to permanently erase department data from personally owned devices.

Users must understand that they may be required to surrender personally owned devices that contain Department data if such data is required to satisfy Open Records Act requests.

Cell Phones and Devices:

It is the responsibility of the employee to whom these devices are assigned to maintain and safeguard these assets as if they were their personal property. It is the policy of this agency to hold the individual responsible for devices that are lost, stolen or damaged through negligence. A periodic inventory and inspection of the devices will be conducted.

Cell phones assigned to agency employees are for official business use only. If a personal emergency arises that requires the use of the cell phone to make a personal call, the employee is responsible for any charges that are incurred.

Disposition of Computer Systems Equipment:

No part of the agency's computer systems will be moved, swapped, exchanged, dismantled, cannibalized, or removed from the office premises without the approval of the ISO. Portable computers, when used for official business purposes, may be transported outside the office premises with the approval of the direct supervisor.

Training:

New Employee Training:
All new employees are required to complete a security awareness training video as part of orientation. The training link will be emailed to the new employee's DNR email address 10 days after first day of employment.

Security Awareness Training:
All employees must complete mandatory security awareness training bi-annually as part of the Executive Order issued by the Governor. The training is intended to protect state information systems from cyber-attacks and is based on the recommendations of the State Government Systems Cybersecurity Review Board. All employees are mandated to take initial training focusing on Phishing & Ransomware and further security awareness training or role-based training as directed by GTA or IT Security Team.

Failure to Comply with Information Security Policies:

Failure to comply with this procedure to use information technology resources appropriately, by employees and other users, may result in suspension of access to agency network resources, disciplinary action up to and including dismissal in accordance with applicable DNR procedures, or, in the case of outside affiliates, termination of the affiliation. Penalties associated with state and federal laws may apply.

Attachments:

Attachment 1 – *Guidelines for the Acceptable Use of Microsoft Office 365*

Attachment 2 – *Password Control Standards*