

DEPARTMENT OF NATURAL RESOURCES

Human Resources Policy No.: 36

EFFECTIVE: JUNE 1, 2015

SUBJECT: COMPUTER USAGE POLICY

AUTHORIZATION: STEPHEN CHUSTZ, SECRETARY

I. POLICY

Computers, software, computer media such as diskettes, flash drives, CD-Roms, cartridges, tapes, optical disks, etc. are provided to the employees of the Department of Natural Resources (DNR) primarily for business use. Internet, e-mail and other online services likewise are provided primarily for business communications. Employees therefore are limited in their use of such equipment/services for personal reasons except to the extent permitted by the express terms of this policy.

Employees are required to use the computer equipment/services provided, including the Internet, in a professional, ethical and lawful manner. Business related e-mail communications must comply with the standards of decency and professionalism observed in other forms of written communication, including proper spelling and grammar. The creation of, access to and transmission of any materials or writings on or through the Internet or via use of the computer equipment/services provided by DNR in violation of this policy or any federal, state or local law or regulation are strictly prohibited.

II. PURPOSE

This policy establishes guidelines to ensure that computers, networks, software, services, systems and other information technology resources provided by DNR are used primarily for business purposes; to identify the limitations placed upon personal computer equipment/services use; to ensure that all communications are made in a professional manner; to describe the improper, inappropriate and prohibited use of the Internet and computer equipment/services; to inform employees of management's access to and intention of tracking, auditing, inspecting and/or monitoring, as deemed appropriate, any and all sites visited, information stored, downloaded, uploaded, transmitted and received through the computer systems/services provided; and to advise employees that they have a limited expectation of privacy/security regarding their computer usage. Compliance with this policy ensures that DNR's employees' business activities are conducted professionally and in accordance with law.

III. APPLICABILITY

This policy applies to all DNR employees, regardless of status, and all other individuals (collectively referred to herein as "employees") authorized to and using the computers, equipment and services provided by DNR for business use.

IV. CONSENT

By logging-on and using these computers and related equipment, systems and services, including the Internet, employees expressly consent to the department's information technology personnel inspecting, auditing, tracking and monitoring such usage. This consent authorizes DNR to undertake any inquiry and institute any process deemed necessary to further the intent of this policy. Such inquiries and processes include the right to directly or remotely access and review computer usage, without employee knowledge or participation, and the right to enter offices and work locations to inspect/secure/retrieve computers and related equipment, data and files therein.

V. EXPECTATION OF PRIVACY

DNR employees are hereby advised that information technology personnel perform special and routine support services and maintenance upon our computers and related equipment, which service/maintenance requires such personnel to view and review computer usage, Internet searches performed and sites visited. As such, DNR employees are hereby advised that their computer and Internet usage, e-mail and other on-line communications, and the materials stored on any computer, including computer hard drives and other media such as diskettes, flash drives, CD-ROMs, etc., are not privileged nor private. This lack of privacy extends to anything a DNR employee views, creates, sends, receives, uploads, downloads, stores, prints or transmits.

DNR employees are further advised that their computer and Internet usage, e-mail and other on-line communications, and the materials stored on any computer, including computer hard drives and other media such as diskettes, flash drives, CD-ROMs, etc., are subject to review and inspection, upon authorization of the appointing authority, based upon reasonable suspicion of computer usage that is unrelated to legitimate business purposes, in violation of this policy or any federal, state or local law or regulation.

DNR employees should also be aware that their communications and transmissions via the use of the computers and related equipment, systems and services provided by DNR are generally publicly accessible and subject to the provisions of Title 44 of the Louisiana Revised Statutes (Louisiana's Public Records Act).

VI. PERSONAL USE

Given the ever increasing reliance upon information technology systems as the customary, acceptable mode of communication, DNR recognizes that occasional,

personal use of its computer systems and the Internet will inevitably occur. In most circumstances, such usage will be of no concern and indeed, not detected. While not encouraged, such occasional, personal use will be tolerated provided such:

- 1) Is incidental, brief and intermittent;
- 2) Does not result in any additional cost to the department;
- 3) Does not interfere with the employee's job duties;
- 4) Does not impact system-wide usage;
- 5) Does not circumvent security systems or protocols;
- 6) Is not intended to produce personal monetary gain;
- 7) Is not offensive, profane, vulgar or otherwise inappropriate; and/or
- 8) Does not violate the prohibitions of this policy or any federal, state or local law or regulation.

Employees should understand that the occasional, limited personal use of the department's computers and related equipment, systems and services tolerated by this policy does not diminish DNR's ownership of the data, files and transmissions thereon, nor diminish the authority DNR has to access, review, track, audit and monitor employee usage of computers, equipment, systems and services.

Employees also should understand that the occasional, limited personal use of the computers, as authorized by this policy, does not convey ownership of the personal data received, transmitted or stored, and does not permit an employee to demand retrieval of such data upon separation.

Employees must be mindful that the privilege of occasional, limited use of the computers and related equipment, systems and services provided by DNR may be revoked and lead to disciplinary action, including termination, if such use interferes with DNR's operations or is in violation of this policy.

VII. REPORTING REQUIREMENT

Employees who receive improper computer communications are required to notify the sender of the inappropriateness of the transmittal and direct the sender to immediately cease sending such communications. After doing so, if the improper communications persist, the employee is to report such continuing receipt to the Human Resources Director. Improper communications are those which are abusive, intimidating, discriminatory, harassing, obscene, vulgar, defamatory, derogatory or otherwise violative of this policy or any federal, state or local law or regulation.

VIII. COPYRIGHTED/PATENTED MATERIALS

DNR employees should be aware that certain on-line information is copyrighted or patented, including text, pictures, video and sound. Employees are not to duplicate, upload or download any software or materials that are copyrighted, patented or otherwise identified as intellectual property without the written, authorized consent of

the owner, and then only with approval of the department's information technology personnel. Any such material currently stored, without authorization, is to be immediately deleted from department equipment.

Commercial software is copyrighted and may not be reproduced except as stipulated in the licensing agreement. It is the policy of DNR to comply with all patent/copyright laws and licensing agreements related to software installed on its computers. Reproduction, duplication, distribution or illegal installation of such licensed software without appropriate licensing agreements, are prohibited. Likewise, employees are prohibited from installing, storing or using software not specifically licensed through the department. This prohibition includes software purchased by employees for home use and then installed on a department computer or network.

IX. PROHIBITIONS

- 1) **E-mail Prohibitions:** Employees are expressly prohibited from using (sending and receiving) the DNR email messaging system for the following:
 - To engage in any unlawful or illegal activity as defined by federal, state or local law or regulation
 - To send threatening, harassing, malicious or intimidating communications to anyone
 - To send or receive sexually harassing, obscene, vulgar, pornographic, sexually suggestive or sexually explicit communications
 - To promote discrimination of any nature
 - To send or receive messages containing objectionable language, materials or content, including racial slurs and epithets
 - To conduct or participate in political activities or fundraisers
 - To conduct personal business or commercial activities, including fundraisers
 - To send or receive mass solicitations or chain letters
 - To send or receive messages that express personal views, beliefs or opinions on non-department issues
 - To send or receive messages or information that are critical of, disparage, defame or provide opinions concerning the operations, activities, decisions, policies or practices of the department, its supervisors and employees
 - To send messages under the name of another employee unless specifically authorized by supervisory personnel
 - To alter electronic messages, without authorization, including attachments
- 2) **Internet Prohibitions:** Employees are expressly prohibited from using the Internet system for the following:
 - To engage in any unlawful or illegal activity as defined by federal, state or local law or regulation

- To view, receive, transmit, print, download, store and/or distribute obscene, vulgar, pornographic, nude, profane, sexually explicit, racist, harassing, discriminatory, malicious, intimidating, violently graphic or threatening materials
- To post messages or information that are critical of, disparage, defame or provide opinions concerning the operations, activities, decisions, policies or practices of the department, its supervisors and employees
- To play video games
- To download/view/hear music, videos or movies
- To engage in non-business streaming, skyping and other such video/audio activities
- To engage in any non-business activity which significantly impacts bandwidth
- To knowingly create, introduce or propagate a virus, worm or other destructive program code
- To knowingly engage in any activity that disables, impairs or overloads the performance of any computer system or network, or circumvents any security system
- To view, receive, transmit, print, download, store or distribute materials or records that are copyrighted
- To download executable files (programs) on a department computer unless specifically authorized by information technology personnel
- To send or receive mass solicitations or chain letters
- To conduct personal business or commercial activities, including fundraising
- To conduct or participate in political activities or fundraisers

X. STORED DATA

Files should be stored on designated network drives such as the "F" drive, not on local PC hard drives. Only network drives are regularly backed up and secured and can be restored in the event of data loss. Any files stored on local PC hard drives should be considered to be "temporary" or "working" files, with the understanding that such files will not be recovered by IT personnel in the event of loss due to computer issues.

Although DNR permits occasional, personal use of its computer systems/services, only work-related data may be stored on network drives. Under no circumstance should personal data, including pictures, music, videos, movies, etc. be stored on any network drive. Such impermissible data limits critical bandwidth. Upon implementation of this policy, non-work related files are prohibited and must be deleted.

XI. WEBSITE ACCESS

DNR recognizes the wealth of information readily accessible via the Internet. Indeed, to perform customary job duties, many DNR employees regularly and routinely access a variety of websites. Although IT personnel have purposefully restricted access to sites

identified as having no business value, certain Internet sites must be accessible for business purposes. IT personnel can identify and track Internet usage. Employees are cautioned to limit their access via the department's computer system to sites needed for business purposes only.

Additionally, DNR requires that employees limit their access to social media and other non-business Internet sites via the use of personal electronic devices. During the workday, occasional, limited access to such sites and communications of a personal nature via the employee's own personal electronic device/service are permissible; however, such activities should be limited to break times and in no event inappropriate or impact an employee's performance of job duties.

XII. PASSWORD AND LOG-ON REQUIREMENTS

Employees are responsible for all computer activity under their User ID, whether generated from their work stations, remote locations or on a department laptop. Any and all computer activity occurring under an employee's User ID and password will be considered an act of the employee unless compelling evidence demonstrates otherwise.

Employees are responsible for maintaining the confidentiality of their computer passwords and properly signing-off whenever departing the work station and at the end of each work day. Password control and adherence to proper log-off protocols are required to protect against unauthorized access to department computers.

Network passwords shall not be shared nor disclosed except on a need-to-know basis. No employee may use another employee's password without express supervisory authorization. Furthermore, no employee is to log-on to or use another employee's computer without express supervisory authorization.

Employees are prohibited from encrypting files on their computers or taking any steps that block access to files or access to their computer, other than the use of passwords or approved encryption programs.


XIII. COMPLIANCE/VIOLATIONS


All employees are required to sign a formal Acknowledgment evidencing their receipt, understanding and intent to comply with the terms and provisions of this policy. Failure to follow this policy and violations of the prohibitions therein shall be cause for disciplinary action in accordance with the Civil Service Rules, including termination of employment.

Any violation of this policy which also is criminal in nature will be referred to the appropriate law enforcement authority for prosecution. Additionally, violations may result in restrictions or limitations upon the employee's access to the Department's computers and related equipment, systems and services.

XIV. QUESTIONS

Any questions regarding the interpretation or enforcement of this policy should be addressed to the Human Resources Division.



STEPHEN CHUSTZ, SECRETARY


DATE

INITIAL ISSUE DATE: 08/99

**REVISION DATES: 08/00; 01/06; 06/06;
03/07; 05/08; 05/15**

DEPARTMENT OF NATURAL RESOURCES

COMPUTER USAGE POLICY ACKNOWLEDGMENT

My signature hereon acknowledges:

- 1) My receipt and review of DNR's policy on computer usage;
- 2) My understanding of the content and prohibitions within this policy;
- 3) My intention of complying with this policy;
- 4) My understanding that the computers and related equipment, systems and services provided for my use are the property of the State;
- 5) My consent, by logging-on and using the State's computers and related equipment, systems and services, for the department to review, inspect, audit and monitor my computer usage; and
- 6) I have no expectation of privacy regarding my use of the State's computers and related equipment, systems and services.

Employee Signature

Printed Name

Date