DEPARTMENT OF FINANCE AND ADMINISTRATION

INFORMATION TECHNOLOGY RESOURCES POLICY

DFA Policy No. 19.0

19.1 PURPOSE

The purpose of this policy is to provide DFA with a policy and procedure for the use of technology resources.

19.2 SCOPE

This policy applies to all DFA employees, contractors, and vendors.

19.3 REFERENCES

New Mexico Administrative Code (NMAC) 1.12.1 through 1.12.20, General Services Electronic Communication Policy 350-2.E, Governor's Code of Conduct.

19.4 BACKGROUND

One of the main tools used in conducting agency administration and business is the use of Information Technology ("IT") systems, which include hardware, software, internet, intranet, email, and digital network usage. Therefore, this policy provides guidelines for agency employees on the proper use of information technology resources.

19.5 DEFINITIONS

19.5.1 **"Access"** means the ability to read, change, or enter data using a computer or an information system.

19.5.2 **"Agency"** means an organization which is required to be in compliance with New Mexico State Personnel Board Rules and Regulations.

19.5.3 **"Agency Head"** means the DFA cabinet secretary.

19.5.4 **"BYOD"** means Bring Your Own Device. Any device not owned by the Department of Finance and Administration. This includes, but is not limited to, laptops, tablets, and phones.

19.5.5 **"Contractor"** means any individual or entity that has entered into either a verbal or written agreement to provide a service to DFA and the State of New Mexico.

19.5.6 **"E-mail"** means all technologies used to transfer messages, including instant messaging and peer-to-peer file exchange.

19.5.7 **"Employee"** means a person working in a classified or exempt position for DFA.

19.5.8 **"Equipment"** means: computers, monitors, keyboards, mice, routers, switches, hubs, networks, or any other information technology assets.

19.5.9 **"Freeware and Shareware"** means software that is available free of charge and available for download from the internet. Freeware is protected by copyright and is subject to applicable copyright laws.

19.5.10 **"Information Technology Resources"** or **"Information Systems"** means computer, hardware, hard drives, floppy disks, CD's, portable storage devices (i.e., USB and external drives), software, databases, electronic message systems, communication equipment, computer networks, and telecommunication circuits within.

19.5.11 **"IT"** means the DFA Information Technology Bureau.

19.5.12 **"Malicious Code"** means any type of code intended to damage, destroy, or delete a computer system, network, file, or data.

19.5.13 **"Pirated Software"** means licensable software installed on a computer system, for which a license has not been purchased or legally obtained.

19.5.14 **"Security Mechanism"** means a firewall, proxy, internet address-screening or filtering program, or other system installed to prevent the disruption or denial of services or the unauthorized use, damage, destruction or modification of data and software.

19.5.15 **"Sexually Explicit or Extremist Materials"** means images, documents, or sounds that can reasonably be construed as discriminatory, harassing, defamatory, libelous, obscene, pornographic, threatening to an individual's physical or mental well-being, or read or heard for any purpose that is illegal.

19.5.16 **"User"** means any person authorized by DFA to access agency IT resources, including a state employee, officer, or contractor; a user, for purposes of this policy, does not include a person who accesses state telecommunications resources offered for use by the general public.

19.6 POLICY

This policy governs the usage of DFA IT resources. Employees are required to comply with this policy, as well as the General Services Electronic Communications Policy 350-21 and Governor's Code of Conduct (April 25, 2011), which concerns the internet and other IT resources such as iPhones, iPads, laptops, printers, removable drives, and other devices.

19.6.1 Information Technology Policy Acknowledgment:

DFA shall provide all users with a written copy of this policy. All users shall sign and date a statement acknowledging they have received, read, and been provided an opportunity to ask questions about, this policy.

Each user's signed acknowledgment shall be kept on file and renewed only when DFA IT Policy is updated. This will ensure employees understand, and are allowed an opportunity to ask questions about, IT policy.

19.6.2 Future Use:

For the purposes of this policy, IT resources usage includes, but is not limited to: all current and future Information Technology Resources or Information Systems, internet/intranet communications services, the World Wide Web (WWW), agency intranet, voice over internet protocol, file transfer protocol, network protocol, email, peer-to-peer exchanges, various proprietary data transfer protocols, and other services.

19.6.3 No Expectation of Privacy:

Electronic records sent or received in conjunction with agency business may be releasable to the public under the Inspection of Public Records Act. Employees are prohibited from disclosing, copying, distributing, or forwarding email messages exempted from public disclosure under state and federal laws.

Any and all passwords must not be shared with anyone; except, for password protected documents, Adobe templates and/or forms provided to the public, said passwords will be provided only to IT Staff. Personal passwords or encryptions will not be placed on any state owned USB drives, archived email folders, or state owned files by the users. Only designated IT staff are permitted to encrypt files. The use of passwords to gain access to the email system or to secure specific files does not provide the employees with an expectation of privacy in the respective system or document. Noncompliance may result in disciplinary action, up to and including dismissal.

DFA may conduct workplace monitoring to help ensure quality control, employee safety, security, and customer satisfaction. The computer equipment and systems, and internet/intranet access that employees may use, are always the property of the State of New Mexico. Therefore, DFA reserves the right to monitor computer activities. DFA also reserves the right to retrieve and read any computer files or data that are composed, sent, or received through internet connections and/or stored in the computer systems. DFA will make every effort to guarantee that workplace monitoring is always done in an ethical and respectful manner.

DFA will perform audits periodically for hardware, software, passwords written down or saved inappropriately, and any other information or conditions deemed important to IT, as long as said condition is substantially related to IT. Prior notification will be given to Division Directors, but not necessarily given to users.

19.6.4 Information Technology Resource Usage:

DFA IT resources shall be used solely for agency business purposes except as addressed in Section 19.6.8.9. All users shall conduct themselves in a professional manner consistent with appropriate behavior standards, as stated in the Code of Conduct. All agency policies relating to intellectual property protection, privacy, misuse of state equipment, sexual harassment, sexually hostile work environment, data security, and confidentiality shall apply to the use of IT resources.

Serious disciplinary action, up to and including dismissal, may result from evidence of prohibited activity. Illegal activity involving DFA IT resources usage may be referred to appropriate authorities for prosecution.

19.6.5 Software/Program Usage:

19.6.5.1 Employees shall not download executable software, including freeware and shareware, unless it is authorized by management in conjunction with IT.

19.6.5.2 Employees will not install any software unless permission has been granted by IT.

19.6.5.3 Employees shall not use Information Technology Resources to download or distribute pirated software or data, including music or video files.

19.6.5.4 Employees shall not use Information Technology Resources to deliberately propagate any malicious code.

19.6.5.5 Employees shall not use Information Technology Resources to intentionally disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of DFA's IT resources, unless such action is required by IT.

19.6.5.6 Software licensed by the state or the agency, and data owned or licensed by the state or agency, shall not be uploaded or otherwise transferred out of the state's or agency's control without explicit authorization by the Agency Head and IT.

19.6.6 **Virus Protection:**

19.6.6.1 Approved antivirus software will be installed on all Information Technology Resources under IT's direct control.

19.6.6.2 Employees are prohibited from removing, disabling, or circumventing antivirus software.

19.6.6.3 Other malwaredetecting software may be installed and controlled by IT.

19.6.7 **Email Usage:**

Email is a business communication tool, and users are obligated to use this tool in a responsible, effective, and lawful manner. Employees shall represent themselves, DFA, or any other state agency accurately and honestly through email. Although by its nature email appears less formal than other written communication, the same laws apply.

DFA considers email to be an important means of communication, and recognizes the importance of proper email content and expedient replies in conveying a professional image and delivering good customer service. Therefore, DFA employees should adhere to the following:

19.6.7.1 all users are responsible for ensuring that their email usage is within the policies and regulations, and is both ethical and lawful.

19.6.7.2 prohibited uses include, but are not limited to:

19.6.7.2.1 engaging in activities or using the internet or email for any illegal purposes, including initiating or receiving communications that violate any state, federal, or local laws and regulations.

19.6.7.2.2 using resources to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws. This includes statements, language, imagesb or other materials that are reasonably likely to be perceived as offensive or disparaging of others based on race, national origin, sex, sexual orientation, age, disability, religious, or political beliefs.

19.6.7.2.3 sending or forwarding chain letters or other pyramid schemes of any type.

19.6.7.2.4 sending or forwarding unsolicited commercial email (spam), including jokes.

19.6.7.2.5 soliciting money for religious or political causes, advocating religious or political opinions, and endorsing political candidates.

19.6.7.2.6 any other non-business related activities that will cause congestion, or disruption of networks or systems, including but not limited to, internet games, online gaming, unnecessary listserve subscriptions and email attachments. Chat rooms and messaging services such as Internet Relay Chat (IRC), AOL Instant Messenger, MSN Messenger, and similar internet-based collaborative services.

19.6.7.2.7 any sharing or exchanging of email account passwords, for any purpose, between users.

19.6.7.2.8 any unlawful exchange of proprietary information, or any other privileged, confidential, or sensitive information outside of the department.

19.6.7.2.9 any use of third party email for government or work related purposes, including the use of a mail relay feature, which forwards email originally sent to a third party address to the state email server.

19.6.7.2.10 email signature lines shall only consist of the DFA employee's name, department, job title, and contact information. The use of themes, graphical backgrounds, and characters such as emojis or quotations, is prohibited.

19.6.7.3 **DFA expects users to adhere to the following:**

19.6.7.3.1 use professional courtesy and discretion;

19.6.7.3.2 write well-structured emails and use short, descriptive subjects;

19.6.7.3.3 do not send unnecessary attachments;

19.6.7.3.4 do not write emails with excessive use of capital letters or other inappropriate characters;

19.6.7.3.5 set the out-of-office option when away, stating an estimated date and time of return;

19.6.8 **Internet Usage:**

19.6.8.1 DFA IT resources shall not be used for anything other than official DFA business unless otherwise specifically allowed by the Agency Head, or as permitted under Section 19.6.8.9. of this policy. Violation of this policy could lead to discipline, up to and including dismissal.

19.6.8.2 Employees with Internet access shall not upload any software licensed to the state nor data owned or licensed by the state without explicit authorization from the manager responsible for the software or data.

19.6.8.3 Employees may only use downloaded files or software in ways that are consistent with licenses or copyrights. Any software or files downloaded via the internet onto state computers becomes the property of the state.

19.6.8.4 Employees with Internet access shall not upload any software licensed to the state nor data owned or licensed by the state without explicit authorization from the IT Staff, management when necessary, and approval from the appropriate vendor.

19.6.8.5 Employees shall not reveal confidential or sensitive information, client data, or any other information covered by existing state confidentiality policies, procedures, or contract terms. Chat rooms and newsgroups are public forums. Staff who release confidential information via a newsgroup or chat room will be subject to sanctions in existing policies and procedures associated with unauthorized release of such information.

19.6.8.6 Employees shall not use DFA IT resources for illegal activity, gambling, personal businesses (such as sale of products, promotion of products, etc.), or to intentionally violate the laws or regulations of the United States, New Mexico or any other state or jurisdiction, or any other nation.

19.6.8.7 Use of peer-to-peer (referred to as P2P) networks are prohibited.

19.6.8.8 Employees who inadvertently connect to a site containing sexually explicit or extremist material shall disconnect from that material immediately. The employee's supervisor, Secretary and legal will be notified immediately.

19.6.8.9 If permission is acquired from an immediate state supervisor, employees may use the internet for non-business research or personal use if the employee is browsing during mealtime or other breaks, or outside of working hours, provided that all other requirements of this guideline are met. Personal use of the internet is prohibited if:

19.6.8.9.1 it materially interferes with the use of IT resources by the state or any political subdivision thereof;

19.6.8.9.2 such use burdens the agency, state, or any political subdivision thereof with additional costs;

19.6.8.9.3 such use interferes with the user's employment duties or other obligations to the agency, state, or any political subdivision thereof; or

19.6.8.9.4 such personal use includes any activity that is prohibited under this rule.

19.6.9 **Security:**

19.6.9.1 Employees shall keep passwords and user IDs for network, internet, email, and other state applications confidential.

19.6.9.2 Employees shall not share user IDs or passwords.

19.6.9.3 Employees shall not attempt to disable, defeat, or circumvent any agency, state, or other organizations/entities security mechanisms.

19.6.9.4 Employees are prohibited from accessing or attempting to access IT resources for which they do not have explicit authorization by way of user accounts, valid passwords, file permissions, or other legitimate access and authentication methods.

19.6.9.5 Passwords are not to be written down or stored electronically unless using IT authorized password management software.

19.6.9.6 Unauthorized virtual private network access to the internet is prohibited from any device that is attached to any part of DFA's or the state's network. Information Technology Resources shall not be used to establish connections to non-agency internet service providers without prior written authorization by the office of NM DoIT.

19.6.9.7 Contractors will not have access to DFA's Information Technology Resources unless permission has been requested by Division Head and approved and granted by IT.

19.6.9.8 Prior to an employee being placed on administrative leave due to pending disciplinary action or investigation, Human Resources and or Legal will work with IT to secure employee access and the employee

will be required to turn in all computer IT resources. This will also include retirement or resignation of an employee.

19.6.10 **File/Data/Information Sharing:**

Employees shall not reveal confidential or sensitive information, client data, or any other information covered by existing state confidentiality policies, procedures, or contract terms. Chat rooms and newsgroups are public forums. Staff who release confidential information via a newsgroup or chat room will be subject to sanctions in existing policies and procedures associated with unauthorized release of such information.

19.6.11 **Hardware:**

19.6.11.1 Acquisition/Disposal of Equipment will be controlled by IT. Standards and requirements have to be maintained and are set forth by statute, IT, and DoIT. IT will ensure standards and requirements set forth by statute, IT, and DoIT are met for all equipment. IT will be responsible for the registration of all equipment with the appropriate vendor. IT with ASD Asset Management will dispose of equipment (following State statutes for disposal of equipment) deemed to be no longer useful to the Department.

19.6.11.2 Installation of all hardware will be performed by IT. Manuals, tutorials, and other materials will be provided to the user when available and deemed necessary. Support materials will be kept safely stored and maintained by IT in a defined designated area. DFA's equipment is not allowed to be taken home for use without the approval of IT and DFA management.

19.6.11.3 Employees shall not access, edit, record, or display sexually explicit or extremist materials or reproduction of sexually explicit or extremist sounds on any Information Technology Resources.

19.6.11.4 Computer Equipment:

19.6.11.4.1 state purchased equipment will be utilized for state business only. Personal business will not be conducted using state equipment.

19.6.12 **External Storage:**

19.6.12.1 DFA-purchased external storage is not to be taken home or connected to non-DFA equipment unless prior permission has been granted by IT.

19.6.12.2 Non-issued external storage devices should not be connected to any computer or laptop unless permission has been granted by IT.

19.6.13 **State-Issued Phone:**

State-issued phones will not be used for personal usage unless another policy specifically allows for such use and reimbursement to the State for such use.

19.6.14 **BYOD:**

19.6.14.1 BYOD devices should not be used to conduct State business.

19.6.14.2 BYOD devices will not be connected to the DFA Information Technology Resources unless permission has been granted by IT.

19.6.14.3 BYOD devices will need to have updated antivirus programs and critical patches installed, as determined by IT.

19.7 REVIEW AND APPROVAL

This DEPARTMENT OF FINANCE AND ADMINISTRATION INFORMATION TECHNOLOGY RESOURCES POLICY is effective upon the signature of the cabinet secretary.

Approved by:

Duffy Rodriguez
Cabinet Secretary

11/1/18
Date

APPENDIX A
ACKNOWLEDGMENT FORM

I, _____, acknowledge that I have received a copy of the DEPARTMENT OF FINANCE AND ADMINISTRATION INFORMATION TECHNOLOGY RESOURCES POLICY, effective upon the signature of the cabinet secretary.

Further, I acknowledge that I have read this Policy and understand its contents, including all of my associated duties and responsibilities. Moreover, I understand potential disciplinary procedure connected to those duties and responsibilities.

By signing this Acknowledgment Form, I affirm that I will abide by my incumbent duties and responsibilities located in the Policy, and I understand that disciplinary action may in fact be taken in the absence of my compliance with this Policy.

_____ _____

Signature Date