ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
March 3, 2021 – PT 2021.03

Section

20.1 Purpose
20.2 Definitions
20.3 Permissible uses of Electronic Mail, Internet, and Data Distribution Function
20.4 Transmission of Confidential Information
20.5 Prohibited Uses of Electronic Mail
20.6 State Computer Equipment Usage
20.7 Use of Unauthorized Equipment
20.8 Prohibited Uses of the SACWIS and Any Other Search Function
20.9 Statewide Business-Related Announcements
20.10 Department Monitoring, Access and Disclosure
20.11 Security and Confidentiality
20.12 Maintenance of Electronic Mail
20.13 Policy Enforcement
20.14 Policy Acknowledgement
Appendix A Electronic Mail/Internet Usage/SACWIS Search Function and Distribution Certificate of Understanding
Appendix B State of Illinois Department of Innovation and Technology Mobile Device Security Policy

20.1 Purpose

The purpose of this Administrative Procedure is to establish the Department's policy regarding the access, use, maintenance and disclosure of electronic communication, data distribution, and the minimum security policy for remote access to State information and systems both from State-owned and User-owned Authorized Mobile Devices which includes, but is not limited to, electronic mail, Internet usage and BYOD (Bring Your Own Device). The Department adheres to the best practices outlined in the State of Illinois Mobile Device Security Policy. Every participant with a User-owned Authorized Mobile Device must electronically receive, read, and formally accept the terms of service agreement prior to participation in the DCFS BYOD Program. The benefit of using a User-owned Authorized Mobile Device is inextricably linked to the risk the device will need to be temporarily turned over and its contents copied for legal purposes, including but not limited to, FOIA requests for State information, legal hold or litigation hold notices, law enforcement requests, subpoenas, OIG investigations etc. The State of Illinois Mobile Device Security Policy is included in Appendix B of this procedure.

Basic Principles that Govern the Use of Electronic Communication

- The Department's electronic mail and Internet systems should be used only for business-related communications and research.
- Department employees and other authorized users should have no expectation of privacy in anything they access, create, store, send or receive when using the Department's electronic mail and Internet systems.
- All users of the Department's electronic mail and Internet systems are required to use these resources in a responsible, professional, ethical and lawful manner.

- E-mail or Internet, used inappropriately, could result in lawsuits, costly litigation and/or employee discipline.
- The sending of E-mail does not absolve the sender from communicating orally with the recipient on critical job-related matters or tasks.

Electronic Data Distribution

- Data distribution standards and methodologies shall be implemented or approved by the Illinois Department of Innovation and Technology (DoIT@DCFS).
- Data distribution standards and methodologies will be observed at all times to ensure the quality and security during delivery.
- Data movement via physical devices such as flash, removable hard drives, tape, etc. shall meet with DoIT@DCFS approval.

Virtual Private Network (VPN)/Remote Access

- Secured internet access into the DCFS network must be requested from and approved by DoIT@DCFS and the user's business manager/supervisor. Upon approval, DoIT@DCFS will provide client (local computer) software and permission. Approval may be requested by contacting the DoIT@DCFS Help Desk by calling 1-800-610-2089.
- Usage is restricted to DCFS employees or contracted business partners, to utilize for access to DCFS applications and services only.
- All VPN/remote connectivity constitutes an acceptance of the "acceptable use policies" of DCFS and its information and computing systems. All VPN connections are subject to investigation, monitoring.

20.2 Definitions

"Authorized Mobile Device" means any Mobile Device authorized by State management to be used to connect to State network resources or contain State data. A Mobile Device that is owned by the User can become an Authorized Mobile Device pursuant to this Policy and may be referred to as a "Bring Your Own Device" or "BYOD" option. Mobile Devices, regardless of ownership, which are not Authorized are prohibited from connecting to the State network, IT infrastructure, or resources and must not store, contain, or transmit State data.

"Child and Youth Centered Information System (CYCIS)" means the database where confidential information of persons served by the Department of Children and Family Services is stored.

"DoIT" means the Department of Innovation and Technology of the State of Illinois. For purposes of this procedure "DoIT@DCFS" shall be referenced throughout.

"Electronic Mail System" means the State's messaging system that depends on computing equipment to create, send, forward, receive, reply to, transmit, store, hold, copy, view, print, and read electronic mail.

"Electronic Mail (E-mail)" means any electronic computer document or message created, sent, forwarded, received, replied to, transmitted, stored, copied, downloaded, displayed, viewed, read, or printed via the Internet or Intranet.

Encryption means the process of transforming information or messages in such a way that only authorized recipients can read it.

"File Transfer Protocol (FTP)" means a communications protocol governing the transfer of files from one computer to another over a network.

"Internet" means a group of independent, self-defined, and self-contained computer communication areas. Internet connections enable access to the Internet (a.k.a. the World Wide Web) when appropriate software has been installed on a workstation.

"Intranet" means a self-contained computer communication network that is strictly internal to the Department and authorized users.

"Management and Accounting Report System (MARS)" means a database where confidential information of persons served the Department of Children and Family Services is stored.

"State Automated Child Welfare Information System (SACWIS)" means the main database where the confidential information of persons served by the Illinois Department of Children and Family Services is recorded and stored.

"SACWIS Search Function" means the mechanism by which authorized SACWIS users may retrieve information maintained in the Department's database regarding child abuse and neglect investigations, child welfare service cases, and related information involving mandated reporters and Department personnel.

"Social Media" means current and future interactive technologies including, but not limited to, text, audio, video, images, podcasts, and other multimedia communications, in virtual communities and online networks.

"Virtual Private Network (VPN)" means a technology that allows for the creation of a secure connection to access the DCFS network from other less secure networks outside of DCFS.

20.3 Permissible Uses of Electronic Mail, Internet, Department Social Media Accounts, and Data Distribution

a) Authorized Users

Only Department staff, authorized contractual staff, and private agencies (POS) with active DCFS contracts using the DCFS network are considered authorized users of the Department's electronic mail, Internet systems, and other data distribution methods. Department social media accounts may only be used by authorized staff. Each Department social media account will be monitored by an individual site contact person, who will be designated as such by DoIT@DCFS. Each site contact person for a Department Facebook account must sign as **CFS 123-1, Facebook Site Contact Agreement**.

b) Purpose of Use

1) Electronic Mail and Internet

Internet usage, electronic mail, or the use of any Department resources for electronic mail should be related to Department business. This includes union-related business as stipulated in the agreements between the Department of Central Management Services and the applicable collective bargaining entities.

2) SACWIS, CYCIS, MARS, and Other Search Function

The SACWIS, CYCIS, MARS, and other search function shall be limited to use by authorized persons that have need of specific database information for the accomplishment of assigned case management functions.

3) Department and Personal Social Media Accounts

Acceptable uses of the Department's Facebook account include, but are not limited to:

- Locating parents and missing children;
- Sending messages to missing children in care in an effort to locate them;
- Sending messages to family members of children in care, provided confidentiality is maintained;
- Monitoring the Facebook page of any youth in care;
- Monitoring the Facebook page of the caregiver or parent of any child in care for anything that may impact the child's safety;
- Determining if parents are violating safety plans or orders of protection;
- Determining if parents are using drugs or alcohol;
- Determining if parents are making online threats toward DCFS or others;
- Determining if parents or children are posting inappropriate messages;
- Determining if alleged perpetrators of sexual abuse or child pornography are having contact with minors; or
- Determining if inappropriate pictures are being posted.

Prohibited uses of Department social media accounts, include, but are not limited to:

- Using the Department's Facebook account for personal purposes;
- "Friending" or otherwise inviting clients to be part of the Department's social media account;
- Posting any information, or contacting anyone through social media, in a way that may be construed as a violation of confidentiality per **Rule and Procedure 431, Confidentiality of Persons Served by the Department**; or
- Posting anything related to the client.

Prohibited uses of employees' personal social media accounts, include, but are not limited to:

- Using a personal account to correspond with clients via messaging or posting to clients' accounts;
- "Friending" or otherwise inviting clients to be part of the employee's personal social media account;
- Posting any information, or contacting anyone through social media, in a way that may be construed as a violation of confidentiality per **Rule and Procedure 431, Confidentiality of Persons Served by the Department**; or
- Posting anything related to the client.

20.4 Transmission of Confidential Information

Confidential information may be transmitted only as authorized under Rule and Procedure 431, Confidentiality of Personal Information of Persons Served by the Department of Children and Family Services. It may only be sent using the approved DoIT standard encryption methodology and only if a business need exists. Information related to the Health Insurance Portability and Accountability Act (HIPPA), the Comprehensive Medicaid Billing System and Medicaid Community Mental Health Services shall remain confidential and may only be transmitted by authorized persons in accordance with Rule and Procedure 431, Appendix H of Procedure 359, and Medicaid Community Mental Health Services Program.

Note: Section 20.5 lists specific information the Department prohibits sending via the Internet.

20.5 Prohibited Uses of Electronic Mail or Internet

Displaying or disseminating materials that can be considered by some people to be obscene, racist, sexist, or otherwise offensive may constitute harassment by creating a hostile work environment. Accessing non-business-related Internet sites may subject the user to discipline, up to and including discharge. Furthermore, unintended usage or unauthorized access or interference may subject the employee and/or the Department to legal action. Consequently, the Department requires appropriate standards of conduct to be employed when using electronic mail or Internet.

Specific prohibited uses of electronic mail include, but are not limited to:

- Using electronic mail systems for any purpose restricted or prohibited by State and Federal laws or regulations;
- Sending electronic mail that is considered offensive to any individual or group or accessing Internet websites for non-business purposes;
- Including inspirational quotations, religious verses, or other non-business-related information in the body, signature block, or beneath the signature block of the E-mail is prohibited. Staff may only use their name, contact information, and appropriate confidentiality notice in their signature block if they choose;

- Transmitting, via the Internet, case-related information such as, but not limited to, case notes, correspondence or documents in violation of Rules and Procedures 431. Personal information of persons served by the Department shall not be transmitted using the Internet, except through a secure connection approved by the Director or Chief Legal Counsel for purposes of automated E-mail reminders of juvenile court hearings and case reviews. Personal information, including SACWIS investigation and case photos of persons served by the Department may be transmitted via Outlook E-mail to external authorized recipients and other Illinois state agencies when the disclosure is in accordance with Rule and Procedure 431, and the information is sent through the DCFS Outlook E-mail system using the approved DoIT standard encryption methodology. Examples of external authorized external recipients include, but is not limited to, doctors, judges, State's Attorneys, local law enforcement;
- Transferring or downloading any confidential information onto user-owned personal computers, flash drives or other removable media or email is prohibited;
- Transmitting confidential personnel, employee discipline, or employee evaluation-related information unless necessary as part of the employee's job duties within the Department;
- Sending copies of documents in violation of copyright laws;
- Unauthorized intercepting and opening of electronic mail except as required for authorized employees to diagnose and correct delivery problems or to monitor usage in accordance with this Administrative Procedure, or for authorized investigations pursuant to Rule 430 or other appropriate Department purposes;
- Using electronic mail to harass or intimidate others or to interfere with the ability of others to conduct Department business;
- Accessing or attempting to access websites for non-business purposes that are sexually explicit, demeaning or exploitive of minors, women or minorities or otherwise counter to the purposes of the Department;
- Unauthorized use of an individual's E-mail account other than for monitoring or investigative purposes consistent with this Administrative Procedure or Rules 430;
- Constructing an electronic mail communication so it appears to be from someone else;
- Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization;
- Downloading and installing of unauthorized software;
- Using the E-mail or Internet system to conduct statewide mailings for notifications of births, deaths, illness, parties and social events;
- Using E-mail or Internet for other such non-business-related matters;
- Including non-business-related graphics within an E-mail message;
- There is a presumption that the use of chat rooms is non-business related; or
- Unauthorized use of Internet access is not limited to business hours. DCFS equipment cannot be used for non-business purposes.

20.6 State Computer Equipment Usage

Desktop computers, laptop computers, printers, and other equipment that is issued to employees should only be used for State business. Misuse of DCFS/State equipment may result in disciplinary action up to and including dismissal.

Unauthorized use of State property is prohibited. Staff should not lend any computer equipment that was issued to them.

Proper care should be taken in the use of State-owned equipment. It is prohibited to damage or expose State owned computer equipment to any condition that might cause damage.

Files/data of a personal nature such as music, photos/pictures, and movies should not be loaded, run, printed or viewed on State property. DoIT@DCFS has the right and will remove these files on discovery.

Unauthorized programs/applications that were not authorized and issued by DoIT@DCFSshould not be loaded or run on State equipment. This includes screen savers, add-on graphics/fonts, slideshow applications, or any other application that was not authorized/issued and installed by DoIT@DCFS. DoIT@DCFShas the right and will remove these files on discovery.

20.7 Use of Unauthorized Equipment

It is prohibited to connect non-State-owned computer equipment to the DCFS Network without written authorization from DoIT@DCFS. This includes personal computers, hubs, switches, printers, scanners, storage devices, and other peripherals.

Add-on equipment such as storage devices, cameras, printers, or other peripherals should not be installed/connected to State property unless authorized and installed by DoIT@DCFStechnicians.

20.8 Prohibited Uses of the SACWIS and Any Other Search Function

Purposes for which the SACWIS search function and any other electronic means may not be used include, but are not limited to the following:

- The SACWIS search function may not be used by persons other than those authorized by the Department.
- The SACWIS search function may not be used to retrieve database information for purposes other than the accomplishment of assigned duties.
- Information obtained via a SACWIS search shall not be transmitted using the Internet or contained in an Internet E-mail message, listed in conversation in a “chat room,” or otherwise referenced in any Internet communication.

20.9 Statewide Business-Related Announcements

Business-related announcements to all Department users must be directed to the following E-mail address: ANNOUNCEMENTS. Include in the first line of the message the date that you wish the announcement to be sent.

E-mail sent to this address will be reviewed for appropriateness prior to distribution. The submitter will be contacted, if necessary, to discuss any issues with the announcement. Allow a minimum of one business day for distribution. Emergency announcements should be marked URGENT and include in the first line an explanation of the situation creating the emergency. (Note: This will be removed prior to distribution.)

20.10 Department Monitoring, Access and Disclosure

Electronic mail created or stored on Department equipment or Internet usage constitutes a Department record and is subject to the disclosure laws of the State of Illinois. The Department reserves the right to monitor, access and disclose contents of electronic mail or Internet usage without the consent of the originator or the recipient of the correspondence.

The SACWIS search and the information developed from the search that is stored on Department equipment constitutes a Department record and is subject to the disclosure laws of the State of Illinois. The Department reserves the right to monitor, access and disclose contents of searches without the consent of the originator of the search.

20.11 Security

Users are advised that electronic mail messages that are transmitted, received, or stored on the Department's electronic mail systems are the property of the Department, and as such, may be considered public records. All Internet sites accessed and attempts to access are subject to monitoring by the Department. The SACWIS search and the information developed from the search that is stored on the Department's electronic systems are the property of the Department, and as such, may also be considered public records.

All Department electronic mail and Internet usage that connects to the Internet, or Outlook, uses the DoIT@DCFS computer network. DoIT@DCFS conducts regular back-ups of the electronic mail files. Even though the sender and recipient have discarded or deleted their copies of an electronic mail record, there are back-up copies that can be retrieved as the result of discovery requests in the course of litigation or other official inquiry.

20.12 Maintenance of Electronic Mail

All electronic records will be maintained according to the rules and timeframes set forth by the State Records Commission and the Department. Staff should preserve essential electronic business records through archiving documents on their workstation or through conventional filing and maintenance.

DoIT@DCFS will maintain a back-up copy of all E-mail transactions and they will be retained for seven years.

20.13 Policy Enforcement

Violations of Department E-mail or data distribution polices will subject employees to disciplinary action up to and including discharge.

20.14 Policy Acknowledgement

Users of the Department's electronic mail system and/or SACWIS search function *must* sign a **CFS 123** (**Electronic Communication and Distribution Certificate of Understanding**) acknowledging that they have read and understand the conditions and terms of this agreement (See Appendix A). The signed copy is to be maintained in the employee's on-site personnel file for all DCFS and POS users and a copy sent to the Office of Employee Services for inclusion in the employee's personnel file for all DCFS users. Failure to sign a CFS 123 will result in loss of network privileges.

This page intentionally left blank.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
March 3, 2021 – PT 2021.03

APPENDIX A

CFS 123
Rev 3/2021

State of Illinois
Department of Children and Family Services

ELECTRONIC MAIL COMMUNICATION AND DISTRIBUTION CERTIFICATE OF UNDERSTANDING

1) I acknowledge that I have read Administrative Procedure #20, Electronic Communication and Distribution, and that I am responsible for abiding by the policies contained, therein.

2) I understand that the use of computer equipment, software and the electronic mail system is for State of Illinois business only.

3) I understand that unencrypted transmittal of confidential information to unauthorized recipients via the DCFS Outlook email system is prohibited.

4) I understand that encrypted transmittal of confidential information (including SACWIS investigation and case photos) to internal and external authorized recipients via the DCFS Outlook E-mail system is permissible when there is a business need

5) I understand that only non-confidential information may be transmitted across the Internet (outside the Department's Outlook E-mail system) and that I may never use specific names of youth in care (except as approved in writing by the Director or Chief Legal Counsel for purposes of automated E-mail reminders of juvenile court hearings and case reviews), perpetrators, witnesses, or any other persons served by the Department in an Internet E-mail message, listed in conversation in a "chat room," or otherwise referenced in any Internet communication.

6) I understand that, to maintain confidentiality, the Department prohibits transferring or downloading any confidential information onto personal computers or email.

7) I understand that information obtained via a SACWIS search shall not be transmitted using the Internet or contained in an Internet E-mail message, listed in conversation in a "chat room," or otherwise referenced in any Internet communication.

8) I understand that electronic mail records are considered Department business records subject to Federal and State freedom of information laws and official State of Illinois record retention rules.

9) I understand there is no expectation of privacy in any E-mail, Internet or SACWIS search document I create, store, send, or receive when using the Department's electronic mail and Internet systems.

10) I understand that Internet access is limited to only those areas directly related to State business and that I must refrain from accessing, displaying or creating any offensive, malicious or illegal material.

11) I understand that downloading from or uploading to the Internet copyrighted material that will then be distributed to other individuals is prohibited.

12) I understand that a violation of this policy may result in disciplinary action, up to and including possible discharge, as well as civil and criminal liability that my action may create.

Signature: _____ Date: _____

Printed Name: _____

Work Location: _____

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
March 3, 2021 – PT 2021.03

APPENDIX B

State of Illinois
Department of Innovation and Technology
Mobile Device Security Policy

Contents

OVERVIEW
PURPOSE
GOAL
SCOPE
DEFINITIONS
ENFORCEMENT
POLICY
RESPONSIBILITY
POLICY COMPLIANCE
AUTHORITIES, GUIDELINES OR SOURCES
REVISION HISTORY

OVERVIEW

The Department of Innovation & Technology (DOIT) seeks to protect State of Illinois (State) information, systems and records from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and/or removal.

PURPOSE

The purpose of the Mobile Device Security Policy is to describe the minimum-security policy for remote access to State information and systems both from State-owned and user-owned Authorized Mobile Devices. All Authorized Devices used to access State information and systems must be appropriately secured to prevent unauthorized access and to prevent confidential data (as defined in the Data Classification Policy) from being lost or compromised, to reduce the risk of spreading viruses, and to mitigate other forms of abuse of the State of Illinois' computing and information infrastructure.

GOAL

The goal of Mobile Device Security Policy is to create a consistent, secure, and operationally effective set of parameters within which users of State-owned or user owned (and used for State purposes) mobile devices can utilize those available communication devices while simultaneously adhering to a best practice based approach to preventing unintended consequences, security risks and other negative outcomes that interfere with successful achievements of the mission of the State of Illinois.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
March 3, 2021 – PT 2021.03

SCOPE

This Policy applies to any Authorized Mobile Device, owned either by the State or by a User, which is used to remotely access State information and systems. The procedures underlying this policy will be reviewed and updated every 365 days, and the policy will be reviewed and updated every three years. This policy applies to all personnel in State of Illinois agencies under the Executive Branch.

DEFINITIONS

Definitions for terms used in this policy can be found in the DOIT Terminology Glossary located on the DOIT web page under Support/Policies. The terms and definitions listed below are meaningful for this policy. In the event of conflict between the definition in the DOIT Terminology Glossary and the definition contained in this policy, the definition below shall control for this Policy.

1. User: Anyone with authorized access to State business information systems, including, but not limited to, permanent and temporary employees or third-party personnel such as contractors, and consultants.

2. Mobile Devices: These include, but are not limited to, any portable cartridge/disk- based, removable storage media (e.g., compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain non-volatile memory), or any mobile computing and communications device with information storage capabilities (e.g., notebook/laptop computers, tablets, public internet access devices, personal digital assistants, smart phones, cellular telephones, etc.).

3. Authorized Mobile Device: Any Mobile Device authorized by State management to be used to connect to State network resources or contain State data. A Mobile Device that is owned by the User can become an Authorized Mobile Device pursuant to this Policy and may be referred to as a "Bring Your Own Device" or "BYOD" option. Mobile Devices, regardless of ownership, which are not Authorized are prohibited from connecting to the State network, IT infrastructure or resources, and must not store, contain or transmit State data.

4. Screen Lock: A software mechanism used to hide data on a visual display while the computer or device continues to operate. A screen lock requires authentication before a User can access organization resources.

5. Screen Timeout: A mechanism that will automatically lock idle Devices or end a session when the Device has not been used for a specified time period (e.g.,5 minutes).

6. Encryption: The process of transforming information or messages in such a way that only authorized parties can read it.

ENFORCEMENT

Participation in the BYOD option is voluntary. Users who select BYOD option voluntarily agree to comply with all provisions of this policy as applied to User-owned Mobile Devices.

Both State-owned and User-owned Mobile Device Users understand that noncompliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including discharge, and may subject the User to civil or criminal penalties, litigation, restitution, fines, and/or other consequences or penalties.

POLICY

1. All Authorized Mobile Devices must be approved by an authorized Agency representative and approved by DOIT to transmit, receive, store, or process State information.

2. As a prerequisite to using an Authorized Mobile Device, Users must receive, read, and formally agree to comply with this Policy before authorization is granted to ensure the User is aware of the risks and procedures associated with this privilege.

3. The State retains the right to refuse Authorization of a User's Device, and/or to discontinue the support of a previously Authorized Mobile Device. If a User is provided a State-owned Authorized Mobile Device similar to an existing BYOD device, then the similar BYOD device will be removed from having access to State data and will no longer be eligible as an Authorized Mobile Device.

4. Communications on all Authorized Mobile Devices, regardless of ownership, are not presumptively private. DOIT may monitor any Authorized Mobile Device for the security and administration of State data. While DOIT will generally attempt to only monitor communications strictly related to State business on a User-owned Authorized Mobile Device, and to limit any such monitoring to the minimum required to achieve its legitimate security and administrative needs, technological and practical constraints may result in the capture or monitoring of personal information on a User-owned Authorized Mobile Device. As a result, every User of an Authorized Mobile Device acknowledges and agrees that the User has no reasonable expectation of privacy for any Authorized Mobile Device, whether State-owned or User-owned.

5. Participation in the BYOD option is voluntary, and no User will be required to use their own device for the purpose of conducting State business unless they voluntarily agree to participate in the BYOD option. However, all Users must agree to immediately upon request temporarily turn over to the State any Authorized Mobile Device, including a User owned Device, when security incidents occur and/or for the installation of required software to protect State systems. The benefit of using a User-owned Authorized Mobile Device for State business is inextricably linked to the risk the Device will need to be temporarily turned over and its contents copied for legal purposes, including, but not limited to, FOIA requests for state information, legal hold or litigation hold notices, law enforcement requests, subpoenas, etc. The risk of participating in the BYOD option also includes the possibility the telephone number for a User-owned Authorized Mobile Device may become publicized.

6. The State is not responsible for any software, data, or hardware problems with, or the loss, damage, or theft of, any User-owned Authorized Mobile Device. The State will not provide any reimbursement for State business-related data/voice plan usage on any User-owned Authorized Mobile Device, or for hardware or device upgrades.

7. Certain State approved and installed software and/or applications are a prerequisite to use of an Authorized Mobile Device, whether User-owned or a State-owned. Users must accept and not delete, remove, modify, disable, or otherwise alter any third-party software that is provided by or installed by the State on any Authorized Mobile Device.

8. The State retains the right to quarantine an Authorized Mobile Device, and to prevent the download of, delete, or require the deletion of any unauthorized third-party software or applications on any Authorized Mobile Device to achieve the State's legitimate security and administrative needs, regardless of whether it is a State-owned or a User-owned device.

9. The User understands and accepts the risk of having data, files, and/or applications, including personal files or applications, on the Authorized Mobile Device deleted by the State to effectuate the State's legitimate security and administrative needs if malware or viruses are detected. Accordingly, the State recommends that a User-owned Authorized Mobile Device should be backed up on the User's own hardware or system with sufficient regularity to protect the User's personal data from this risk.

10. Users must comply with all applicable State password policies on Authorized Mobile Devices, including on User-owned Authorized Mobile Devices. This includes the use of strong passwords, password expiration, and password history limitations.

11. Authorized Mobile Devices must, when applicable, enable screen locking and screen timeout functions in combination with a password or passcode for protection.

12. The physical security of every Authorized Mobile Device is the responsibility of the User. Authorized Mobile Devices shall be kept in the employee's physical presence whenever possible. Whenever an Authorized Mobile Device is being stored, it shall be stored in a secure place, preferably out-of-sight.

13. If an Authorized Mobile Device is lost or stolen, User shall immediately, but no later than 24 hours, report the incident to the DOlT Help Desk, law enforcement and his or her supervisor.

14. If an Authorized Mobile Device is lost or stolen, DOlT reserves the right to remotely wipe the Device of any State data stored on the Authorized Mobile Device. While the State will use reasonable efforts to delete only State data, the User acknowledges the possibility and accepts the risk that all data, including personal data, could be wiped in some circumstances.

15. State-owned Authorized Mobile Devices should be kept in provided protective cases whenever possible. If a State-owned Authorized Mobile Device is damaged because it was not kept in the provided protective case, the User's Department Director or a delegate may require User to reimburse the State for the cost of repair or replacement.

16. State data, software, and applications must be removed from a User-owned Authorized Mobile Device utilizing DOIT-approved procedures before the Authorized Mobile Device is returned, exchanged, sold, disabled, or otherwise disposed of, and before a User leaves State employment.

17. Authorized Mobile Devices shall have connectivity limited to State resources on an as needed basis, and in accordance with the IT Resource Access Policy. Individual Agencies reserve the right to implement a more restrictive connectivity policy.

18. Every State-owned Authorized Mobile Device used to gather, process or store personal information (as defined by the Personal Information Protection Act - 815 ILCS 530) shall be equipped with full-disk encryption. Users of these Devices are the data owners and must ensure the confidential data is encrypted while stored on the Device.

19. It is a violation of this Policy for any User to attempt to bypass, penetrate, alter the configuration of, or to otherwise affect the operation of any encrypted storage media.

20. The State retains the right to filter and track web access on any State-owned Mobile Device.

21. Any User conducting State business on User-owned Authorized Mobile Devices must do so only via the User's State email account.

22. State email accounts must not be used to engage in prohibited political activity (as that term is defined in the State Officials and Employees Ethics Act (5 ILCS 430/1-1*et seq.))* at any time, and this prohibition continues to apply to the use of State email accounts, regardless of the means of access, including State-owned and User-owned Mobile Devices.

23. The use of State email on a User-owned Authorized Mobile Device is subject to the same restrictions, limitations, and monitoring as covered by other applicable policies and laws.

24. The use of text messaging, instant messaging, or any other related communication method/application to conduct any State business on an Authorized Mobile Device is strictly forbidden.

25. The use of State-owned telephones is the primary and preferred method for conducting telephone communication for State business. State business should only be conducted by telephone on a User-owned Mobile Device when a State-owned telephone is not reasonably available.

26. The State can employ or enable geolocation services on State-owned Authorized Mobile Devices to effectuate the State's legitimate security and administrative needs, and these functions and settings must not be disabled or modified in any way by the User.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
March 3, 2021 – PT 2021.03

RESPONSIBILITY

1. Each User of an Authorized Mobile Device used to remotely access State information and systems is responsible for following this Policy and any related policy or procedure promulgated by the head of his or her Agency.

2. Each Agency may establish policies and procedures and assign responsibility to specific Agency personnel to achieve compliance with this Policy.

3. Anyone observing what appears to be a breach of security, a violation of this policy, a violation of state or federal law, theft, damage, or any action placing State information and systems at risk must immediately report the incident to an appropriate level supervisor, manager, or security office within their organization.

4. Managers and supervisors are responsible for ensuring that Users are aware of and understand this policy and all related policies and procedures.

POLICY COMPLIANCE

In order to implement this Policy, the Department of Innovation & Technology establishes procedures and designates responsibility to specific personnel. To the extent necessary, each Agency must establish procedures in order to achieve policy compliance. It is the responsibility of all authorized users of IT Resources to understand and adhere to this Policy. Failure to comply with this policy could result in discipline, up to and including discharge.

AUTHORITIES, GUIDELINES OR SOURCES: None

Revised Date: November 2, 2016