| GEORGIA DEPARTMENT OF COMMUNITY HEALTH | | Enterprise Policy | |
|---|---|---|---|
| **Policy No.:** | **419** | **Division:** | **Office of Information Technology** |
| **Policy Title:** | **Appropriate Use of Information Technology Resources** | **Effective Date:** | **February 21, 2024** |
| **Version:** | **2** | **Category:** | **Cybersecurity Governance, Risk, and Compliance** |

## I. Purpose

The purpose of this policy is to establish guidelines for the use of all Georgia Department of Community Health (DCH) Information Technology (IT) Resources, including those IT Resources managed by the Georgia Technology Authority and delivered by the State's IT Enterprise Service Providers. These guidelines define appropriate business use of DCH IT Resources and establish requirements for protecting the privacy and security of electronic DCH information.

IT Resources are provided to authorized individuals to facilitate the efficient and effective performance of their duties for DCH. The IT Resources provided to individuals by DCH or at the request or direction of DCH, in order for those individuals to provide services for DCH, are referred to in this policy and procedure as "DCH IT Resources."

To ensure that the Agency's internal employees, subcontractors and vendors, and anyone with access to sensitive agency information are in compliance with the HIPAA Security Rule and FISMA federal laws through the implementation of the NIST Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53;

To establish Appropriate Use requirements for DCH contractors, business owners, vendors, sponsors, and business partners regarding their roles and responsibilities when access to DCH data and use of applications associated with DCH operations is authorized; and

To reinforce the role of the business owner in providing adequate oversight of contractor responsibilities specific to Appropriate Use obligations outlined in DCH contracts.

## II. Scope

**A.** This document applies to all DCH personnel accessing or utilizing sensitive information in computer resources, data communication networks, or other information technology infrastructure resources owned or leased by DCH, including any other corporation or Agency with connectivity to the network, which are subject to these Information Security Policies.

**B.** This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

**C.** Any personnel found to have violated any agency policy or process shall be subject to sanctions or disciplinary action, up to and including termination of employment.

## III. Policy

**A.** DCH IT Users must protect DCH IT Resources from unauthorized access, misuse, and loss. DCH IT Users must protect the privacy and security of DCH IT Resources over which they have control or to which they have access. The User is responsible for manually locking their computer screen before leaving it unattended for any period. The DCH Division of Information Technology, Office of Information Security shall ensure that all DCH IT Users receive the training necessary for them to protect the confidentiality, integrity, availability, privacy, and security of the information over which they have control or to which they have access, because of their use of DCH IT Resources. This training must be provided upon receipt of access to DCH IT Resources and on an as-needed basis. In addition, this training must be provided on a regularly scheduled basis (at least annually).

**B.** DCH shall implement and disseminate this Appropriate Use policy and procedures to all personnel and contractors.

**C.** The Chief Information Security Officer is designated to manage the development, documentation, implementation, and dissemination of the Appropriate Use policy and procedures in addition to managing the program.

**D.** DCH Users that become aware of any incident that threatens the privacy or security of DCH IT Resources should immediately report the existence of such incident to their immediate Supervisor, the Agency Information Security Officer (see Section IV for contact information), or in the case of security incidents involving PHI, the HIPAA Privacy and Security Officer (see Section IV for contact information). Such incidents include, but are not limited to:

**1.** Loss, theft, or destruction of a DCH-issued desktop or laptop, regardless of whether the information is believed to be encrypted or otherwise safeguarded;
**2.** Loss, theft, or unintended destruction of any Media (including thumb drives, flash drives, CD's, DVD's, external hard drives, etc.) that contains DCH information, regardless of whether the information stored in the Media is believed to be encrypted or otherwise safeguarded;
**3.** Loss, theft, or destruction of a DCH issued wireless or mobile device; including, but not limited to, an iPhone, iPad, or other PDA, regardless of whether the information contained in the device is believed to be encrypted or otherwise safeguarded.
**4.** Fraudulent or unauthorized access to DCH information systems, including, but not limited to, those managed by GTA/GETS.
**5.** Sharing of passwords.
**6.** Improper use of GTA/GETS Managed email services or Internet access.
**7.** Threats or damage to DCH employees, facilities, or systems.

**E.** DCH IT Resources are to be used only in a manner consistent with the goals and objectives of DCH, and are to be used to accomplish work-related assignments. DCH Users who divert DCH IT Resources for personal gain will be required to reimburse DCH

and will be subject to other appropriate disciplinary action, including but not limited to termination.

**F.** DCH IT Users may not connect a personal flash drive, CD, DVD, or external hard drive to a DCH computer without written approval by a supervisor and the IT Department.

**G.** The State's GETS Service Provider-managed networks, department software applications, and software are to be used responsibly by all DCH IT Users. DCH IT Users must comply with local, State, and federal laws related to copyrights, software licensing, and restrictions regarding transmitting threatening or obscene materials. All computer software installed on DCH computers and systems must be licensed as the software manufacturer requires. All DCH IT Users must follow and abide by commercial licensing laws and requirements.

**H.** Passwords protect State networks, systems, and sensitive agency data. Each DCH User establishes and maintains individual passwords to access sensitive information, business systems, and software. Network, system, and application user accounts must be assigned to specific individuals and not assigned to anonymous user accounts, groups, departments, job functions, etc. DCH Users are responsible for ensuring that passwords remain private and confidential. Sharing LAN network, system, application, and/or screen saver passwords with anyone else is prohibited. Passwords prevent unauthorized access to various common directories on the network and the email system and possibly access to external computer systems. DCH IT Users may give specific individuals access to their files and email by requesting such access through the Division of Information Technology. As defined by State Enterprise Information Security Policies and Standards, Strong Password Standards must be followed for access to any State LAN network, system, or business software application.

**I.** Personal information technology resources may never be connected to DCH IT Resources. DCH Management reserves the right to examine and review content on personal information technology resources reasonably believed to have been connected to DCH IT Resources or to contain DCH information. Examples include but are not limited to personal USB drives, external hard drives, individual CDs, DVDs, personal laptops, or any other personal computing device that can connect with DCH Information Technology Resources.

**J.** Internet and Email Use Personal The State's Infrastructure Service Providers provide Internet access and email addresses as required by DCH to DCH Users to perform their duties for DCH efficiently and effectively. Internet access is provided to allow business-related research and access to information needed to facilitate business communication with customers, vendors, colleagues, and others receiving services from, doing business with, or seeking information from DCH. Computer equipment and other IT Resources required for Internet access and email accounts are provided at significant cost to the State. As with other State property, DCH IT Users must ensure that such resources are not misused. Although valuable business tools, Internet and email access are considered privileges, and as such DCH reserves the right to revoke access to either or both for inappropriate usage or take any other appropriate disciplinary action, including termination. Examples of inappropriate Internet use include, but are not limited to, the following:

1. Private or personal for-profit business activities. This includes Internet use for private purposes such as private advertising of products or services, or any activity meant to foster personal gain.
2. For profit business transactions or unauthorized not-for-profit business activities.
3. Conducting any illegal activities as defined by federal, State, and local laws or regulations.
4. Political or religious causes.
5. Accessing or downloading sexually explicit or pornographic material.
6. Accessing or downloading material that could be considered discriminatory, offensive, threatening, harassing, or intimidating, including ethnic or racial slurs or jokes.
7. Deploy alternative security mechanisms when the primary security mechanisms are unavailable or compromised (e.g., different methods of authentication when one mode of authentication is unavailable.)
8. Uploading or downloading commercial or Agency software in violation of copyright or trademark.
9. Downloading any software or electronic files without approval from the IT Division or ensuring that DCH provided virus protection is active.
10. Online shopping and auctioning.
11. Accessing personal chat, social media, and dating sites.

**K.** Information, data, and files composed, transmitted, or received on DCH IT Resources, including Internet data and email messages, are subject to disclosure under the Georgia Public Records Act. DCH IT Users should ensure that all data accessed with or stored on DCH IT Resources is appropriate, ethical, and lawful. Email users should be mindful of how they represent themselves since any message or data sent through the email system clearly identifies the message as coming from DCH and could be interpreted as a Statement of DCH opinion, position, or policy. Additionally, data that is composed, transmitted, accessed, or received via State Internet resources must not contain content that may be considered discriminatory, offensive, threatening, harassing, intimidating, or disruptive.

**L.** Email is NOT the same as a letter sent through the normal mail. Your messages are "written" on the electronic equivalent of postcards. What does this mean? Anyone can look at your message. Do not email ePHI to a non-DCH email account unless the email has been encrypted. If you need to email ePHI to perform your job, please use encryption or contact your local support team for instructions. Do not use non-DCH email such as Web Mail (like gmail, hotmail, yahoo, etc.) to conduct business or send ePHI. Secure FTP (SFTP) may be used to send ePHI outside of DCH. Contact the IT Help Desk for instructions.

**M.** DCH respects the privacy of DCH IT Users, and ensuring compliance with this policy and procedure is of utmost importance. Therefore, DCH reserves the right to retrieve and read content or data, including but not limited to any data composed on DCH IT Resources, transmitted using DCH IT Resources, received through DCH online connections, or stored on DCH IT Resources, to monitor Internet sites visited and access attempts, and provide information relevant to an investigation of suspected violations of DCH policies and procedures or laws. Inappropriate Internet or email usage can expose DCH to significant legal liability and reflect negatively on DCH. The State's Infrastructure Service Provider has installed software to prevent access to many objectionable Internet Web content and to monitor State Internet access. The Division of Information Technology may review and

document Internet activity, email usage or usage of other DCH IT Resources. DCH IT Users should be aware that any information accessed, downloaded, or transmitted may be reviewed by information security staff, the Office of Inspector General, and the HIPAA Privacy and Security Officer, as needed, and DCH management will be notified if a DCH IT User's use of DCH IT Resources violates DCH policies or procedures or laws, such as by repeatedly attempting to reach blocked Internet sites, frequently visiting non-work related sites, or emailing DCH information to personal email accounts. When using DCH IT Resources, including, but not limited to, email and the Internet, DCH IT Users consent to monitor their use and have no reasonable expectation of privacy in the use of the DCH IT Resources. Failure to comply with this policy and procedure may result in disciplinary action, including termination from employment.

## IV. Information Security and HIPAA Privacy and Security Contacts

Agency Chief Information Security Officer:
William Monahan
Phone: 770-310-1662
Email: William.Monahan@dch.ga.gov

Agency HIPAA Privacy & Security Officer:
Suzannah Lipscomb, Esq.
Phone: 404-909-2155
Email: slipscomb1@dch.ga.gov
Email: hipaa@dch.ga.gov

Division of Information Technology Help Desk
Phone: 404-657-7171
Email: helpdesk@dch.ga.gov

## V. Definitions

- DCH – Georgia Department of Community Health
- ePHI - Electronic protected health information or ePHI is defined in HIPAA regulation as any protected health information (PHI) that is created, stored, transmitted, or received in any electronic format or media. HIPAA regulation states that ePHI includes any of 18 distinct demographics that can be used to identify a patient. See 45 C.F.R. §§ 160.103 and 164.514(b)(2).
- FISMA – Federal Information Security Modernization Act.
- HIPAA - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law requiring national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
- NIST - The National Institute of Standards and Technology as part of the U.S. Department of Commerce. See https://www.nist.gov/.

- PII – Personally Identifiable Information - PII is defined by Office of Management and Budget (OMB) Memorandum M-17-12 (January 3, 2017). PII means information that can be used to distinguish or trace an individual's identity either alone, or when combined with other information that is linked or linkable to a specific individual.
- PHI – Protected Health Information – Individually identifiable health information that is:
    - Transmitted by electronic media
    - Maintained in electronic media; or
    - Transmitted or maintained in any other form or medium.
    - Excluding individually identifiable health information in:
        - Education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g;
        - Records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
        - Employment records held by DCH (a covered entity) in its role as employer; and
        - Regarding a person who has been deceased for more than fifty (50) years.
- Sensitive Information - PII, PHI, ePHI, SSA PII, and similar data that require special handling.

**N. References:** Please refer to NIST 800-53 and Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Contingency Planning.

**20240221**

***Signature*** ***Date***

## Appendix A
## Information Technology User Agreement

By accessing DCH IT Resources, DCH IT Users agree to maintain the privacy, security, confidentiality, and integrity of State and DCH data and computing resources over which they have control or to which they may have access. DCH IT Users must review this policy and procedure and the current Information Security Training materials and agree to comply with them by signing the DCH Policies and Procedures Acknowledgement Form upon starting work and annually after that.

Use of Information Technology Resources:

(1) DCH IT Users shall not attempt to circumvent IT privacy or security safeguards, and any such attempts may lead to revocation of a DCH IT User's access and may result in disciplinary action, as appropriate.
(2) DCH IT Resources, including email accounts and Internet access, may be monitored at any time without additional prior notice, and if such monitoring reveals violations of State or DCH policies, the Chief Information Officer (CIO) or his designee and the Office of Human Resources will be notified, and appropriate sanctions will be applied. If such monitoring reveals misconduct or illegal behavior, the activity will be referred to the DCH Office of Inspector General for internal investigation and further action, as needed.
(3) DCH IT Users shall not add any network equipment or infrastructure to the State network except as authorized by the Division of Information Technology or GTAlGETS Service Provider management as part of a DCH IT User's job responsibilities. The DCH IT User's supervisor or contracted business program sponsor must inform the Division of Information Technology when he or she no longer requires access to DCH IT Resources in accordance with DCH Policies.
(4) DCH IT Users shall not relocate computing equipment, workstations, printers, scanners, etc., without proper authorization or assistance from the appropriate Division of Information Technology support staff.
(5) DCH IT Users shall only physically connect to the State's Infrastructure network using DCH IT Resources.
(6) DCH IT Users shall not disclose ePHI in email unless the email is encrypted as described in current training guidelines.
(7) DCH IT Users shall use their best efforts to send only email content that is appropriate for transmission in that media, ensuring messages are professional, current, accurate, and factual.
(8) DCH IT Users will be mindful of any person's right to inspect and copy emails upon request under the State of Georgia public records law.
(9) DCH IT Users shall take reasonable and appropriate steps to protect DCH IT Resources from loss, damage, or theft and understand that failure to do so may result in disciplinary action.

(10) DCH IT Users shall not attempt to introduce a computer virus or other malicious program code into State networks, systems, or software.
(11) DCH IT Users shall not attempt to bypass, strain, or test security safeguards or mechanisms unless authorized as required by specific job responsibilities.
(12) DCH IT Users shall comply with guidelines set forth in current Information Privacy and Security training materials.

Software Licensing and Intellectual Property:

DCH IT Users requiring additional computer software, equipment, or media that was not issued initially shall contact the Division of Information Technology Help Desk to request the necessary resources. The Division of Information Technology will ensure that the appropriate software licensing and agreements are obtained. DCH IT Users shall not download, use, or connect any unauthorized software, freeware, adware, shareware, or hardware onto any State network, system, workstation, or wireless/mobile device, nor violate software copyright, trademark, or licensing restrictions.

***Signature*** ***Date***