DEPARTMENT OF ADMINISTRATION
Enterprise Policy

DOIT-00-02-2018

DIVISION OF INFORMATION TECHNOLOGY

Technology Acceptable Use Policy

Date of Last Revision 11/07/2018

Brian Tardiff
(401) 462-1783
doa.entsec@doit.ri.gov

1. Purpose

a. Establish policy for the acceptable use of State network resources. Protect employees and the workplace environment through reducing the risk of compromising State data, disruption of network resources, and legal-related issues. The intent of this policy is to maintain the confidentiality and integrity of State data, ensure the availability of network resources, and assist in the reduction of financial and legal penalties associated with non-compliance of federal and State programs.

2. Applicability

a. This policy is applicable to all State of Rhode Island Executive Branch Departments[1] (including agencies, boards and commissions), and their employees (permanent, non-permanent, full-time, and part-time), interns, consultants, contractors, vendors, contracted individuals, and any entity with authorized access to State information systems and data, whether operated or maintained by the State or on behalf of the State. For this policy, the term "Agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

a. **Classified Data** - Any data that is not public (private, sensitive, confidential). Classified data requires additional security controls, such as access restrictions and encryption. Examples of classified data include Personally Identifiable Information (PIT), Personally Identifiable Health Information (PHI) or Federal Tax Information (FTI). If you are unsure if the data you are processing is classified or not, consult your supervisor.

b. **Network Resources -** Information systems, system components, devices, and data that are accessible by computer via the local area network or State intranet. Network resources include:

(i.) Data, information, and files (in storage and in transmission).

(ii.) Desktop computers

(iii.) State issued mobile devices (e.g. laptops, tablets, notebooks, smartphones).

(iv.) Peripheral devices (e.g. printers, scanners, fax machines, monitors).

[1] State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State colleges, the General Treasurer, the Attorney General, or the Secretary of State.

(v.) Licensed software, hardware, and network equipment (e.g. applications, phone systems, servers, routers, switches).

4. Procedures for Compliance

a. General. All users within the scope of this policy must have a signed "Network Access Rights and Obligations User Agreement Acknowledgement" form on file prior to being granted access to State network resources. Users have no right to or expectation of privacy when using State network resources. The use of State network resources is monitored. State employees will perform State business using only State issued or State-approved network resources. All correspondence and transactions performed using State network resources are the property of the State and subject to RJGL Chapter 38-2 Public Records law.

(i.) Prohibited Actions

1. Using State network resources to support any unlawful activity that violates Federal, State, or local laws or that violates code of conduct policies and procedures established by DOA Division of Human Resources or the Agency.
2. Using copyrighted material (e.g. photographs, books, music, software) in any manner without permission from the author or publisher or that is not within its fair use guidelines.
3. Sharing user account or physical access credentials with others. Using someone else's user account or physical access credentials to access network resources or unauthorized areas.
4. Disclosing, sending, emailing, or sharing classified data with unauthorized individuals.
5. Using unmanaged devices to process or transmit classified State data.
6. Accessing or transmitting classified data without appropriate security controls in place.
7. Leaving workstation unattended without enabling the password protected screen lock feature.
8. Intentionally accessing, altering, damaging, or destroying data or software without prior authorization, in accordance with Rhode Island General Laws (RJGL) Section 11-52-3.

b. Network. DoIT reserves the right to implement management, operational, or technical controls to establish restrictions on an "as needed" basis to maintain the network and access to network resources for all users. Network resources should be locked when not in use.

(i.) Prohibited Actions

1. Knowingly installing software not authorized by DoIT.
2. Attaching peripheral, storage, or processing devices not authorized by DoIT (e.g. USB devices, flash drives, external drives, RAM chips) .

3. Knowingly introducing malware or malicious software (e.g. virus, worm, Trojan, bot) into the State network.
4. Using network resources to play games, music, videos, or other similar activities without authorization or for non-business purposes.

c. Email. State records are open to public review unless protected by federal or State laws, rules, or regulations. Pursuant to RIGL 38-2-2(4) Public Records law email is considered a public record open for public inspection, unless exempted from being deemed a public record. Third-party (e.g. Yahoo, Gmail, Cox, AOL) email services should not be used to conduct official State business. Users should be aware that anything emailed could be made available to the public. When accessing State email via web mail on unmanaged devices (e.g. personally owned or public accessible computers) users will read and send email only. Downloading or creating local copies of classified (not public) data or uploading of any attachments on unmanaged devices via State web mail is not authorized.

(i.) Prohibited Actions

1. Knowingly emailing spam (e.g. unsolicited junk email, advertising, chain letters).
2. Knowingly forwarding, auto-forwarding, or relaying State email to unauthorized third-parties or webmail services (e.g. Yahoo, Gmail, Cox, AOL).
3. Sending an employee, person, or any other entity an email that may be reasonably judged as being offensive, discriminatory, defamatory, disparaging, harassing, or threatening.
4. Downloading or uploading attachments or "clicking links" embedded in third-party (e.g. Yahoo, Gmail, Cox, AOL) email services from unknown or un-verified senders.
5. Using third-party (e.g. Yahoo, Gmail, Cox, AOL) email services to send or receive classified State data.
6. Using unmanaged devices to upload or download classified State data (attachments).

d. Internet. Internet access is provided to assist employees and other network users in performing duties and responsibilities associated with their job functions. Internet access should be used for business purposes. Internet use for personal interests is at the discretion of the supervisor. All internet use is monitored.

(i.) Prohibited Action – Knowingly:

1. Using proxies, software, hardware, or any other means to access websites prohibited by policy or blocked by DoIT.
2. Accessing prohibited websites without authorization, such as pornographic, discriminatory, explicitly violent, extremist, hacking, dating, gambling, gaming, political, religious or other non-business-related websites.

3. Using unauthorized peer-to-peer networking or peer-to-peer file sharing application software (e.g. BitTorrent, Spotify, Kazaa).
4. Using third party cloud-based online storage or file sharing services (e.g. Dropbox, Hightail, Google Docs, Google Drive) for storage or transfer of classified State data or as a part of a formalized business process.
5. Using unauthorized instant messaging or online texting services (e.g. Pidgin, Slack, Miranda).
6. Using audio, video, TV, radio, or other online streaming or bandwidth consuming services without authorization or for non-business purposes.

e. Social Media. Access to social media websites is subject to provisions of DoIT Policy 10-09 (Social Networking).

5. Repercussions for Noncompliance

a. Any user who willfully violates this policy will be subject to disciplinary action up to and including termination of employment and may face civil or criminal penalties.

b. Users that repeatedly and/ or negligently violate provisions of this policy are subject to re-training, counseling and / or termination of access to network resources.

6. Roles and Responsibilities

a. *Division of Information Technology*

(i.) Annually review and update this policy, as required.

(ii.) Maintain the network, network security and access to network resources. Implement controls or establish restrictions, as required, to ensure the correct level of access for all users.

(iii.) Monitor and report (as requested) use of State network resources.

b. *Agency*

(i.) Comply with provisions documented in this policy.

(ii.) Disseminate this policy to users to ensure they are aware of prohibited actions.

(iii.) Maintain a signed "Network Access Rights and Obligations User Agreement Acknowledgement" form on file for each user prior to granting access to State network resources.

(iv.) Monitor and manage employee personal internet usage

(v.) Act as good stewards of RI network resources.

c. *User*

(i.) Comply with provisions documented in this policy.

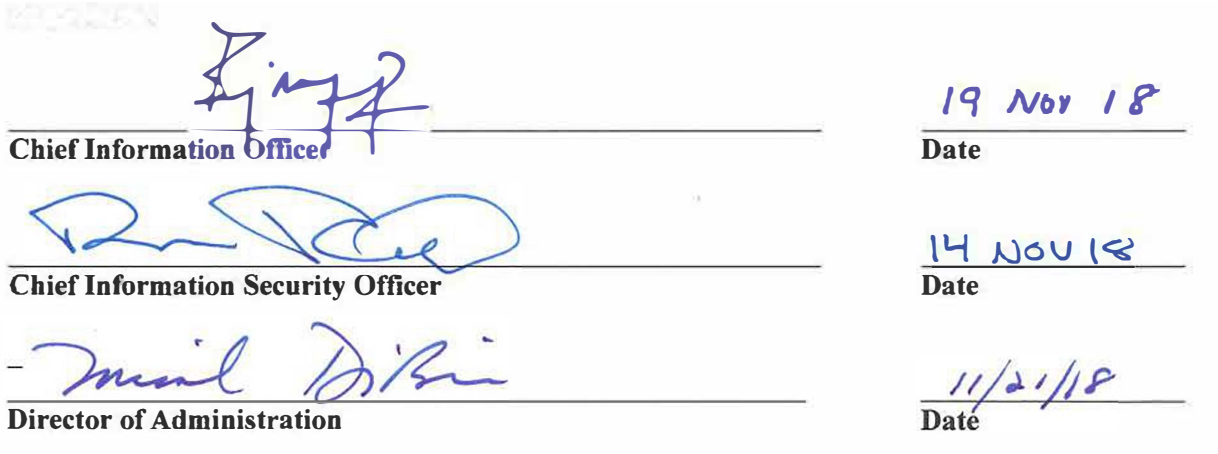
(ii.) Conduct State business using only State or State-approved network resources.

(iii.) Log off and lock computer network resources when not in use .

(iv.) Report known or potential malware or data breaches to the Helpdesk immediately.

(v.) Act as good stewards of RI network resources.

7. Signatures



Chief Information Officer	19 Nov 18 **Date**
Chief Information Security Officer	14 NOV 18 **Date**
Director of Administration	11/21/18 **Date**

Network Access Rights and Obligations
User Agreement Acknowledgement

As a user of State of Rhode Island data and network resources, I agree to abide by the Acceptable Use Policy and the following promises and guidelines as they relate to established policy:

1. I will protect State classified data, facilities, systems, and network resources against unauthorized use or disclosure.
2. I will maintain all computer access codes in the strictest of confidence, immediately change them if I suspect their secrecy has been compromised, and report activity that is contrary to provisions of this agreement to my supervisor or a State-authorized security administrator.
3. I will be accow,table for all transactions performed using my computer access codes.
4. I will not disclose any classified information other than to persons authorized to access such information as identified by my section supervisor.
5. I agree to report any suspicious network activity or security breach to the Division of Information Technology (DoIT).

The State of Rhode Island actively monitors network services and resources, including, but not limited to, real time monitoring. Users have no expectation of privacy. These commw,ications are considered State property and may be examined by management for any reason, including, but not limited to, security or employee conduct.

I acknowledge that I must adhere to this policy as a condition for receiving access to State of Rhode Island data and resources.

I understand that the willful violation or disregard of this policy, these guidelines, or statutes may result in my loss of access and disciplinary action, up to and including termination of my employment, termination of my business relationship with the State of Rhode Island, or any other appropriate legal action, including possible prosecution.

I have read and agree to comply with the policy set forth herein.

_____	_____
Print Name	Agency/Business Unit
_____	_____
Signature	Date