Department of Administration

Division of Enterprise Technology Strategy and Services

ETSS Policy 950.1

Network Resource Acceptable Use Policy

Publish Date: 1 August 2026
Effective Date: 1 August 2026
Last Revision: 17 July 2026

doa.entsec@doit.ri.gov

1. Purpose

Establish policy for the acceptable use of 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 incurred due to non-compliance with federal and State program requirements, while maintaining user productivity.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments (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. Non-Public Classified Data
Any data that is not public (including private, sensitive, or confidential data as defined by associated federal regulations and denoted by ETSS data classification labels). Non-Public Classified Data requires additional security controls, such as access restrictions and encryption.

b. Managed Device
A device that is managed and monitored by ETSS using endpoint management tools. It typically has security policies, software updates, and access controls enforced to ensure compliance and protection.

c. Unmanaged Device
A device that is not under ETSS management or monitoring. It lacks enforced security policies, making it more vulnerable to threats and potentially posing risks when accessing mechanisms and State resources.

d. Network Resources
Information processing systems, system components, devices, and data that are accessible via the local area network or State intranet. Network Resources include:
   a. Data, information, and files (in storage and in transmission).
   b. Desktop computers.
   c. State issued mobile devices (e.g., laptops, tablets, notebooks, smartphones).
   d. Peripheral devices (e.g., printers, scanners, fax machines, monitors).
   e. Software, hardware, and network equipment (e.g., applications, phone systems, servers, routers, switches).

e. Information Technology (IT) Governance
A defined, integrated, and sequenced set of processes and workflows that establishes authority, management, and decision-making parameters to ensure Network Resources and related services are well architected, procured, deployed, managed, monitored, and secured throughout the enterprise in a standardized manner

4. Procedures for Compliance

4.1. General. All users must have a signed "Network Access Rights and Obligations User Agreement Acknowledgement" form (attached hereto) on file with ETSS prior to being granted access to Network Resources. Users have no right to or expectation of privacy when using Network Resources. The use of Network Resources is continuously monitored. Users must use only State issued or State-approved Network Resources to perform State business. All correspondence and transactions executed using Network Resources are subject to Rhode Island General Laws (R.I. Gen. Laws) Chapter 38-2 Access to Public Records (everything on Network Resources is public and subject to disclosure to the public upon request).

Prohibited Actions Users shall not:

a) Use Network Resources for 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 and/or the Agency.
b) Knowingly use copyrighted material (e.g., photographs, books, music, software) in any manner without permission from the author, source, or publisher, unless specifically allowed by the copyrighted material's fair use guidelines.
c) Installation of software not authorized by ETSS.
d) Use Non-Public Classified Data as an input without ETSS authorization.
e) Share user's account or physical access credentials with others or use someone else's user account or physical access credentials to access Network Resources.
f) Knowingly, bypass security controls or introduce malware or malicious

software (e.g., virus, worm, Trojan, bot) into Network Resources.

g) Use Network Resources to play games, music, videos, or other similar activities for non-State business purposes or without express written authorization from ETSS.
h) Disclose, send, email, or share Non-Public Classified Data using non-secure or unauthorized methods.
i) Disclose, send, email, or share Non-Public Classified Data with unauthorized individuals.
j) Use Unmanaged Devices and/or State approved applications to process or transmit Non-Public Classified Data in performance of their roles.
k) Leave workstation unattended without enabling the password protected screen lock feature.
l) Intentionally access, alter, damage, or destroy data or software, without prior authorization from ETSS, that would violate retention policies or availability for audits or investigations.

4.2. Network and Internet. ETSS reserves the right to implement management, operational, or technical controls that establish restrictions on an "as needed" basis to maintain the network and access to Network Resources for all users. Network Resources must be locked when not in use. Internet access is provided to assist employees and other network users in performing duties and responsibilities solely associated with their job functions. Internet access on Managed Devices must be used only for State business purposes, except that limited internet use for personal interests is allowed at the discretion of the user's immediate supervisor. All network and internet uses are monitored and logged. State network and internet resources shall not be used for personal benefit, including but not limited to, gambling, political activity, unsolicited advertising, unauthorized fundraising, personal business ventures, or for the solicitation of performance of any activity that is prohibited by any federal, State, or local law.

Prohibited Actions Users shall not:

a) Use proxies, software, hardware, or any other means to access websites prohibited by policy or blocked by ETSS.
b) Access prohibited websites without ETSS authorization, such as pornographic, discriminatory, explicitly violent, extremist, hacking, dating, gambling, gaming, political, religious, or other non-State business-related websites that are outside the scope of their employment.
c) Use unauthorized peer-to-peer networking or peer-to-peer file sharing application software (e.g., BitTorrent).
d) Attach peripheral, storage, or processing devices not authorized by ETSS (e.g., USB devices, flash drives, external drives, RAM chips).
e) Use unauthorized third-party cloud-based online storage or file sharing services (e.g., Dropbox, Hightail, Google Drive) for storage or transfer of Non-Public Classified Data (unless the data is exclusively the personal data of the State employee in question) or as a part of a formalized State business process.
f) Use unauthorized instant messaging or online texting services .
g) Use audio, video, TV, radio, or other online streaming or bandwidth consuming services without authorization or for non-State business purposes.

4.3. Email. State records are open to public review unless protected by federal or State laws, rules, or regulations. Pursuant to R.I. Gen. Laws Section 38-2-2(4) Public Records, email is considered a public record open for public inspection, unless exempted from being deemed a public record. Third-party or web-based email services (e.g., Yahoo, Gmail, Cox, AOL) shall not be used to conduct official State business. Users should be aware that anything sent via email could be made available to the public. When accessing State email via a browser on Unmanaged Devices (e.g., personally owned or publicly accessible computers), users shall not download/upload attachments, create local copies of Non-Public Classified Data, and must immediately report any potentially malicious messages for review using mechanisms like 'report phish'.

Prohibited Actions Users shall not:

a) Email spam (e.g., unsolicited junk email, advertising, chain letters).
b) Forward, auto forwarding, or relaying State email to unauthorized third parties or webmail services.
c) Send an employee, person, or any other entity an email that may be reasonably judged as being offensive, discriminatory, defamatory, disparaging, harassing, or threatening, in accordance with DOA Division of Human Resources Violence Prevention in the Workplace Policy.
d) Download or upload attachments or click links embedded non-ri.gov email services from unknown or un-verified senders.
e) Use any non-ri.gov email services to send or receive Non-Public Classified Data unless the data is exclusively the personal data of the employee in question.
f) Use Unmanaged Devices to upload or download Non-Public Classified Data unless the data is exclusively the personal data of the employee in question.
g) Share Non-Public Classified Data using non-secure or unencrypted methods.

4.4. Social Media. Provisioning, access to, and management of social media websites is subject to ETSS Social Networking Policy 10-09.

4.5. Use of Removable Media. Non-Public Classified Data may not be stored on any non-State-owned removable storage device (e.g., USB, DVD, external storage). All Non-Public Classified Data on State-owned removeable storage devices must be encrypted. Non-Public Classified Data may not be electronically transferred unless there is written approval from ETSS with a justified State business need to do so. If there is a State business need, Non-Public Classified Data must be appropriately secured from unauthorized access prior to sending or during the transmission process (e.g., password-protecting files, using secure email to force email encryption, using workspaces.ri.gov to send large files securely). Note: contact Agency IT technical support or the ETSS Service Desk for assistance.

4.6. Telework. Employees and other network users approved for telework must comply with provisions documented within DOA Division of Human Resources Teleworking Policy.

Prohibited Actions Users shall not:

a) Print or retain hard copies of Non-Public Classified Data unless written authorization is provided by Agency management.
b) Leave mobile devices that have access to Network Resources or that are displaying Non-Public Classified Data unattended at any time.
c) Leave the screen un-locked when stepping away from the device for any reason.
d) Stay logged into interactive sessions when the session is over or no longer required.
e) Leave unsecured automated information processing equipment, including laptops when not in use or during temporary absences.
f) Bypass conditional access policies or use of multi-factor authentication (MFA).

5. Repercussions for Noncompliance

5.1. Users that repeatedly and/or negligently violate provisions of this policy are subject to retraining, termination of access to Network Resources, and disciplinary action up to suspension, with repeated violations leading to termination or civil or criminal penalties.

6. Roles and Responsibilities

Division of Enterprise Technology Strategy and Services

a) Annually review and update this policy, as required.
b) 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.
c) Monitor and report on the use of Network Resources when requested by users' supervision team members.
d) Execute an annual process for users to review and agree to the "Network Access Rights and Obligations User Agreement" within the Enterprise Resource Planning (ERP) platform.

Agency

a) Comply with provisions documented in this policy.
b) Disseminate this policy to users to ensure that users are aware of prohibited actions.
c) Enforce and track completion of the "Network Access Rights and Obligations User Agreement Acknowledgement" form for each new Agency user prior to granting access and then again annually for all Agency users.
d) Monitor and manage employee personal internet usage.
e) Understand and participate in ETSS defined IT Governance processes for assessment and authorization of any Network Resources.
f) Act as good stewards of Network Resources.

User

a) Complete all assigned training.
b) Do not share Non-Public Classified Data (digital or printed) with unauthorized individuals.
c) Comply with all documented agency or division requirements regarding the handling

of Non-Public Classified Data.

d) Review, acknowledge, and comply with the Network Access Rights and Obligations User Agreement Acknowledgement annually within the ERP platform.
e) Comply with provisions documented in this policy.
f) Report known or potential malware or data breaches to the ETSS Service Desk immediately.
g) Act as good stewards of Network Resources.

7. Approval / Review Signatures:

Digitally signed by Nathan Loura
Date: 2026.07.30 15:41:51 -04'00'

Chief Information Security Officer (CISO)
Division of Enterprise Technology Strategy and Services

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2026.07.30 15:47:01 -04'00'

Chief Digital Officer (CDO)
Division of Enterprise Technology Strategy and Services

Thomas Verdi
Digitally signed by Thomas Verdi
Date: 2026.07.31 11:34:42 -04'00'

Director
Department of Administration

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 Technology Acceptable Use Policy and the following promises and guidelines as they relate to established policy:

1. I will protect State Non-Public 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 accountable for all transactions performed using my computer access codes.
4. I will not disclose any Non-Public Classified Data other than to people authorized to access such information as identified by my section supervisor.
5. I agree to immediately report any suspicious network activity or security breach to the Division of Enterprise Technology Strategy and Services (ETSS).

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 communications 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 Network 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**

(1) Submit signed copy to ETSS Service Desk