Division of Enterprise Technology Strategy and Services

ETSS Policy 400.2

FTI Access and Data Handling Policy

Publish Date: 15 July 2026
Effective Date: 15 July 2026
Last Revision Date: 14 July 2026

doa.entsec@doit.ri.gov

1. Purpose

This policy establishes the requirements for the access, handling, processing, storage, retention, and disposal of Federal Tax Information (FTI), Personally Identifiable Information (PII), and other classified data throughout its lifecycle. It consolidates requirements for FTI access and safeguarding, PII processing and transparency, and data handling procedures into a single governance document. This policy ensures that the confidentiality, integrity, and availability of classified data is maintained and that agencies comply with IRS Publication 1075, the Privacy Act of 1974, the RI Identity Theft Protection Act (RIGL Chapter 11-49.3), HIPAA, FERPA, FISMA, PCI DSS, and other applicable federal and state laws and regulations.
Technical security controls that apply to systems processing FTI and classified data (access control, identification and authentication, system communications protection, etc.) are implemented through the individual ETSS control family policies referenced in the ETSS SSP. Appendix A of this policy maps FTI-unique requirements to the applicable ETSS policies and identifies any additional IRS Publication 1075-specific obligations beyond the standard NIST 800-53 Moderate baseline.

2. Applicability

This policy applies to all State of Rhode Island Executive Branch departments, including agencies, boards, and commissions, as well as their employees (permanent, non-permanent, full-time, and part-time), interns, consultants, contractors, vendors, and any entity that has access to State information systems and data, whether operated or maintained by the State or on behalf of the State. This policy applies to all data under agency control, with heightened requirements for FTI, PII, and other classified data types.

3. Definitions

The following terms are defined for the purposes of this policy. All other terms should be referenced in the ETSS Glossary and the ETSS Data Classification Policy.

Federal Tax Information (FTI)
Federal tax returns and return information (and information derived from it) covered by the confidentiality protections of Internal Revenue Code (IRC) Section 6103 and subject to IRC

6103(p)(4) safeguarding requirements. FTI includes information received directly from IRS or through authorized secondary sources (SSA, OCSE, BFS, CMS). FTI includes any information created by the recipient that is derived from federal return or return information. FTI may not be masked to circumvent IRC 6103 confidentiality requirements.

Personally Identifiable Information (PII)
Data that can be used, either alone or in combination with other data, to identify an individual. Data is considered PII when an individual's first name (or first initial and last name) is combined with SSN, driver's license number, financial account numbers with access codes, medical or health insurance information, or email address with required access credentials.

Classified Data
Any data that is not public, including confidential, sensitive, and private data as defined in the ETSS Data Classification Policy (400.1). Classified data requires additional security controls such as encryption and access restrictions.

Data Owner
A senior-level official at the agency who is ultimately responsible and accountable for agency data. Data owners approve access, designate data classification managers, and accept risks associated with data under their control.

Data Classification Manager
An individual designated by the data owner to have oversight of day-to-day administrative, operational, and technical requirements over agency data or data sets.

Access (FTI-specific)
When an individual enters a restricted area containing FTI or obtains, acquires, receives, examines, uses, or gains knowledge of FTI by physical, electronic, or any other method. Users with the ability to modify or bypass security controls protecting FTI (including decryption keys) are considered to have access.

4. Procedures for Compliance

4.1 Data Classification and Handling
All data under agency control shall be classified in accordance with the ETSS Data Classification Policy as one of the following types: Confidential, Sensitive, Private, or Public. Confidential and sensitive data shall only be processed, stored, transferred, or communicated via IAL2 moderate-risk information systems.
Each data type shall be handled according to the following requirements:

a. Confidential Data (IAL2): Access restricted to individuals with formal data owner approval and signed non-disclosure agreements. MFA is required for remote access. Digital files encrypted using FIPS-validated mechanisms during transmission and at rest. Hardcopies stored in secure locations, labeled "confidential," and cross-cut shredded upon disposal. Full-disk encryption required on mobile devices.
b. Sensitive Data (IAL2): Same access controls as confidential. Digital files encrypted during transmission; application-level password protection permitted for sensitive (not confidential) data. Same physical and disposal requirements as confidential data.
c. Private Data: Access restricted to authorized and authenticated individuals. Digital files encrypted during external transmission. Stored on State-owned systems or authorized cloud providers. Hardcopies cross-cut shredded upon disposal.

d. Public Data: No access, distribution, or storage restrictions. Recycling of paper is recommended. Because public and non-public data may be co-mingled, media wiping is recommended upon disposal.

4.2 FTI Access Requirements

Agencies authorized to access, store, process, or transmit FTI shall comply with all requirements of IRS Publication 1075 in addition to the requirements of this policy and all applicable ETSS control family policies. FTI-specific requirements include:

a. FTI shall be accessed only by personnel with a documented need-to-know and who have completed FTI-specific disclosure awareness training and signed applicable access agreements.
b. FTI shall not be accessed, stored, processed, or transmitted on information systems that are not authorized for FTI and documented within the applicable System Security Plan.
c. Systems processing FTI shall implement all NIST SP 800-53 Rev. 5 Moderate baseline controls plus IRS-defined enhancements as documented in Appendix A of this policy and the ETSS SSP.
d. FTI shall not be used for testing, training, or research purposes without prior submission and approval of a Data Testing Request (DTR) from the IRS Office of Safeguards.
e. Agencies shall submit an annual Safeguard Security Report (SSR) to the IRS Office of Safeguards after initial receipt of FTI and maintain compliance with ongoing safeguard review requirements.
f. Outsourced information system services that process, store, or transmit FTI outside the continental United States are prohibited unless explicitly authorized by the ETSS CDO and CISO with IRS notification.

4.3 PII Security and Handling

PII shall be classified as confidential or sensitive data in accordance with the ETSS Data Classification Policy (400.1). Each agency shall:

a. Encrypt PII at rest and during transmission in accordance with the ETSS System and Communications Protection Policy and the ETSS Data Encryption Standard.
b. Sanitize media containing PII using an approved sanitization method prior to disposal, reuse, or release in accordance with the ETSS Media Protection Policy.
c. Retain PII in accordance with all applicable federal and State laws and regulations. In the absence of documented retention requirements, retain PII for a minimum of six (6) months.
d. Report any real or suspected compromise of PII to the immediate supervisor and the ETSS CISO in accordance with the ETSS Incident Handling and Response Policy. FTI and SSA data breaches shall follow the specific reporting procedures defined in the IR Policy.

4.4 PII Processing and Transparency

The following requirements implement the NIST SP 800-53 Rev. 5 PII Processing and Transparency (PT) control family:

4.4.1 PII Processing and Transparency Policy and Procedures (PT-1)

Each agency shall develop, document, and disseminate PII processing and transparency procedures. The ETSS CISO, in coordination with the DOA Chief Privacy Officer, is responsible for the enterprise policy. The policy shall be reviewed at least every three (3) years.

4.4.2 Authority to Process PII (PT-2)

Each agency shall determine and document the legal authority that permits processing of

PII and restrict processing to only that which is authorized. Where required, agencies shall attach data tags to PII to identify relevant elements and authorized processing types and manage enforcement of authorized processing through automated tools where applicable.

4.4.3 PII Processing Purposes (PT-3)

Each agency shall identify and document the purpose(s) for processing PII throughout its lifecycle (creation, collection, use, processing, storage, maintenance, disclosure, dissemination, and disposal), describe the purpose(s) in privacy notices and agency policies, restrict processing to documented purposes, and monitor changes to ensure continued alignment.

4.4.4 Consent (PT-4)

Each agency shall implement mechanisms to obtain individual consent prior to PII collection when required by law, including determining whether individuals can reasonably understand privacy risks, identifying consent mechanisms (opt-in, opt-out), providing mechanisms for individuals to revoke consent, and using plain language in consent communications.

4.4.5 Privacy Notice (PT-5)

Each agency shall provide a privacy notice to individuals regarding the processing of PII that is clear, accessible, and compliant with applicable privacy requirements. Privacy notices shall be updated when processing purposes change or when new PII collection activities are initiated.

4.4.6 System of Records Notice (PT-6)

Each agency shall publish system of records notices in accordance with applicable federal and State requirements for systems that maintain records retrievable by individual identifiers.

4.4.7 Specific Categories of PII (PT-7)

Each agency shall apply additional protections to specific categories of PII that carry heightened sensitivity, including Social Security Numbers, financial account information, medical information, and FTI, in accordance with the applicable regulatory framework governing each data type.

4.4.8 Computer Matching Requirements (PT-8)

Each agency shall comply with applicable computer matching program requirements when conducting computerized comparisons of records from two or more automated systems, including compliance with the Computer Matching and Privacy Protection Act where applicable.

4.5 Data Marking and Labeling

All communications, emails, and physical documents containing classified data shall be marked with appropriate access restriction designations in accordance with the data classification of the most restrictive data element contained within the document. Markings shall be placed in a conspicuous location. Digital media marking shall be implemented through enterprise data classification and labeling tools (Microsoft Purview) in accordance with the ETSS Media Protection Policy. If classified data is received in error, the recipient shall notify the sender and promptly delete or destroy the data.

4.6 General Data Security Practices

All personnel with access to classified data shall:

a. Comply with the ETSS Technology Acceptable Use Policy (AUP) and all applicable ETSS security policies.
b. Complete annual cybersecurity awareness training in accordance with the ETSS Awareness and Training Policy. Personnel with access to FTI shall also complete FTI-specific disclosure awareness training.
c. Report any suspicious activity or suspected compromise to the ETSS Enterprise Service Desk immediately in accordance with the ETSS Incident Handling and Response Policy.
d. When unsure of the sensitivity of data, treat it as IAL2 data (confidential or sensitive) and contact the supervisor for clarification.
e. Not email classified data using non-secure methods. Encrypt classified data in transit using approved mechanisms.

5. Repercussions for Non-Compliance

Failure to comply with this policy may result in corrective action proportional to the severity of the violation. Consequences may include, but are not limited to:

a. Immediate revocation of access to FTI, PII, or other classified data.
b. Mandatory retraining on data handling and FTI safeguarding requirements.
c. Formal counseling or written reprimand.
d. Referral to agency management for disciplinary proceedings, up to and including termination.
e. Referral to law enforcement and the IRS Office of Safeguards for willful unauthorized disclosure of FTI.
f. Regulatory penalties, loss of FTI data sharing agreements, and federal audit findings for failure to comply with IRS Publication 1075 requirements.

Non-compliance findings shall be documented and tracked through ETSS governance processes and recorded in the agency Plan of Action and Milestones (POAM).

6. Roles and Responsibilities

The following roles are accountable for the implementation, monitoring, and enforcement of this policy:

Chief Information Security Officer (CISO)
Responsible for enterprise-level data handling and FTI access policy oversight, coordination of IRS Safeguard Security Reports, federal breach notification for FTI/SSA/NDNH incidents, and oversight of PII processing and transparency requirements in coordination with the DOA Chief Privacy Officer.

DOA Chief Privacy Officer
Coordinates with the CISO on PII processing and transparency requirements (PT controls), reviews privacy notices and consent mechanisms, and provides guidance on privacy impact assessments and computer matching program compliance.

Data Owners
Senior-level agency officials that are responsible for agency data. Approve access to classified data, designate data classification managers, define data retention requirements, and accept risk associated with data under their control.

Data Classification Managers
Individuals designated by data owners for day-to-day oversight of data classification,

handling, and access requirements for specific data sets.

System Owners

Responsible for ensuring information systems processing FTI and PII implement all required security controls, are documented in the SSP, and maintain compliance with IRS Publication 1075 and applicable privacy requirements.

Agency Information Managers (AIMs) / Technical Support Managers (TSMs)

Coordinate data handling activities at the agency level, ensure agency personnel complete required FTI disclosure awareness training, and support IRS Safeguard review requirements.

All Personnel

Responsible for handling data in accordance with its classification, completing required data handling and FTI-specific training, reporting suspected data compromises immediately, and complying with all provisions of this policy and the ETSS AUP.

7. Approval / Review Signatures

Scott Gausland

Digitally signed by Scott Gausland
Date: 2026.07.16 09:32:13 -04'00'

Chief Data and Analytics Officer (CDAO)
Division of Enterprise Technology Strategy and Services

Digitally signed by Nathan Loura
Date: 2026.07.15 10:49:46 -04'00'

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

Brian Tardiff

Digitally signed by Brian Tardiff
Date: 2026.07.16 09:53:07 -04'00'

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

Appendix A: FTI Control Overlay Mapping

The following table maps FTI-unique requirements from IRS Publication 1075 to the applicable ETSS control family policies and the ETSS System Security Plan (SSP). All systems processing FTI must implement the full NIST SP 800-53 Rev. 5 Moderate baseline as documented in ETSS PM-1, plus the IRS-defined enhancements listed below. For complete control implementation details, refer to the ETSS SSP.

AC (Access Control)
ETSS Policy Reference: Policy 300 Series
FTI-Unique Requirements: FTI access restricted to personnel with documented need-to-know. Access agreements and disclosure awareness training required prior to FTI access. Annual access recertification required.

AT (Awareness and Training)
ETSS Policy Reference: Policy 950 Series
FTI-Unique Requirements: FTI-specific disclosure awareness training required annually for all personnel with FTI access. Breach-specific training required per IRS Pub 1075 IR-2 CE-3.

AU (Audit and Accountability)
ETSS Policy Reference: Policy 300 Series
FTI-Unique Requirements: All FTI access events logged and retained per IRS Pub 1075 retention requirements. Audit reduction and reporting tools required.

CM (Configuration Management)
ETSS Policy Reference: Policy 500 Series
FTI-Unique Requirements: IRS Office of Safeguards SCSEM baselines required for FTI systems. Configuration deviations require documented POAM.

CP (Contingency Planning)
ETSS Policy Reference: Policy 100 Series
FTI-Unique Requirements: FTI systems included in contingency plan testing. FTI-specific recovery requirements per IRS Pub 1075.

IA (Identification and Authentication)
ETSS Policy Reference: Policy 300 Series
FTI-Unique Requirements: MFA required for all FTI access (local and remote). 14-character minimum passwords with all four complexity categories per IRS Pub 1075 IA-5.

IR (Incident Response)
ETSS Policy Reference: Policy 400 Series
FTI-Unique Requirements: FTI breach notification to IRS Office of Safeguards within 24 hours. Specific reporting procedures for FTI, SSA, and NDNH data per Policy 10-12 Section 4.6.

MA (Maintenance)
ETSS Policy Reference: Policy 100 Series
FTI-Unique Requirements: Maintenance personnel accessing FTI systems require documented authorization and monitoring.

MP (Media Protection)

ETSS Policy Reference: Policy 300 Series
FTI-Unique Requirements: FTI media sanitized per NIST SP 800-88. FTI media marking required.

PE (Physical and Environmental)
ETSS Policy Reference: Policy 100 Series
FTI-Unique Requirements: Physical access to FTI areas restricted to authorized personnel on the Authorized Access List (AAL). Visitor escorts are required.

PL (Security Planning)
ETSS Policy Reference: Policy 300 Series
FTI-Unique Requirements: SSP required for all FTI systems with annual review. SSP must document FTI-specific controls and authorization boundaries.

PS (Personnel Security)
ETSS Policy Reference: Policy 300 Series
FTI-Unique Requirements: Background checks required for all personnel with FTI access. Termination procedures must disable FTI access within 4 hours.

PT (PII Processing)
ETSS Policy Reference: This Policy Sec. 4.4
FTI-Unique Requirements: PII processing authority, purpose limitation, consent, privacy notices, and computer matching requirements as defined in Section 4.4.

RA (Risk Assessment)
ETSS Policy Reference: Policy 300 Series
FTI-Unique Requirements: Annual risk assessments for FTI systems. Supply chain risk assessments for FTI service providers.

SA (System and Services Acquisition)
ETSS Policy Reference: Policy 800 Series
FTI-Unique Requirements: SOC 2 Type II or FedRAMP Moderate required for FTI cloud services. IRS 45-day notification for FTI contractor access.

SC (System and Communications)
ETSS Policy Reference: Policy 300 Series
FTI-Unique Requirements: FIPS 140-2/3 encryption required for FTI at rest and in transit. TLS 1.2+ mandatory. VPN with MFA for remote FTI access.

SI (System and Information Integrity)
ETSS Policy Reference: Policy 300 Series
FTI-Unique Requirements: Critical FTI vulnerability remediation within 15 days. CrowdStrike EDR on all FTI endpoints. SI-12(2) DTR required for FTI in testing.

SR (Supply Chain Risk Management)
ETSS Policy Reference: Policy 800 Series
FTI-Unique Requirements: SCRM plan required for FTI supply chain. Anti-counterfeit controls for FTI system components. NAID certification for FTI media disposal vendors.