	PREPARED BY: TS SECURITY SOLUTIONS
ON THE BEHALF OF:	TStephens Information Security Committee
EFFECTIVE DATE:	July 2025
NEXT REVIEW DATE:	July 2026
REVIEW CYCLE:	Annually in July
STATUS:	☒ Working Draft ☐ Approved ☐ Adopted
CONTACT:	teriousstephens@gmail.com

TStephens LLC

Information Classification and Management Policy

TS Security Solutions
7-17-2025

Information Classification and Management Policy

Purpose

The purpose of the Information Classification and Management Policy for TStephens LLC, is to provide a system for classifying and managing Information Resources according to the risks associated with its storage, processing, transmission, and destruction procedures.

Audience

The Information Classification and Management Policy for TStephens LLC applies to any individual, entity, or process that interacts with any Information Resource belonging and pertaining to TStephens LLC.

Contents

- Information Classification
- Information Handling
- Information Retention and Destruction

Responsibilities

Information User

- The person(s), organization, or entity that interacts with information for the purpose of performing an authorized task.
- Have a responsibility to use information in a manner that is consistent with the purpose intended and in compliance with policy.

Information Owner

- The person responsible for, or dependent upon, the business process associated with an Information Resource.
- Knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.
- Determines the appropriate value and classification when the information generated is released outside of the department and/or TStephens LLC and its entirety.
- Must communicate the information classification when the information is released outside of the department and/or TStephens LLC and its entirety.
- Controls access to their information and must be consulted when access is extended or modified.
- Must communicate the information classification to the Information Custodian so that the Information Custodian may provide the appropriate levels of protection.
- Must periodically review their information to ensure that the proper classification is applied.

Information Custodian

- The person or system that is responsible for the implementation of controls and handling of data on behalf of the Information Owner. They are to enforce the security requirements as defined by the information owner and ensure that data is protected in daily operations.
- Information owned, used, created, or maintained by TStephens LLC should be classified into one of the following three categories:
    - **<u>Public</u>**
        - Information that may or must be open to the general public.
        - There are no existing local, national, or international legal restrictions on access or usage.
        - While subject to TStephens' disclosures rules, it is available to all TStephens employees and all individuals or entities external to the corporation.
        - Examples of Public Information include:
            - Publicly posted press releases
            - Publicly available marketing materials
            - Publicly posted job announcements
    - **<u>Internal</u>**
        - Information that must be guarded due to proprietary, ethical, or privacy considerations.
        - Must be protected from unauthorized access, modification, transmission, storage, or other use and applies even though there may not be a civil statute requiring this protection.
        - Restricted to personnel designated by TStephens LLC, who have a legitimate business purpose for accessing such information.
        - Examples of Internal Information include:
            - Employment information
            - Business partner information where no more restrictive confidentiality agreement exists
            - Internal directories or organization charts
            - Planning documents
            - Contracts
    - **<u>Confidential</u>**
        - Information protected by statutes, regulations, TStephens policies or contractual language. Information owners may also designate information as Confidential.
        - Sensitive in nature, and access is restricted. Disclosure is limited to individuals on a "need-to-know" basis.
        - Disclosure to parties outside of TStephens LLC must be authorized by executive management, approved by the Director of Information Technology and/or General Counsel, or covered by a binding confidentiality agreement.

- Examples of Confidential Information include:
  - Customer data shared and/or collected during consulting engagements
  - Financial information, including credit card and account numbers
  - Social Security Numbers (SSNs)
  - Personnel and/or payroll records
  - Any information identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction
  - Any information belonging to a TStephens customer that may contain personally identifiable information (PII)
  - Patent information

Information Handling

- All information should be labelled according to the TStephens Labelling Standard.
- **Public**:
  - Disclosure of Public information must not violate any pre-existing, signed non-disclosure agreements (NDAs).
- **Internal**:
  - Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
  - Must be protected by a confidentiality agreement before access is allowed.
  - Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
  - The “default” classification level if one has not been explicitly defined.
- **Confidential**
  - When stored in an electronic format, it must be protected with a minimum level of authentication to include strong passwords as defined in the Authentication Standard.
  - When stored on mobile devices and media, it must be encrypted.
  - Must be encrypted at rest.
  - Must be stored in a locked drawer, room, or area where access is controlled by a cipher lock and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other people without a need-to-know.
  - Must not be transferred via unsecure communication channels, including but not limited to:
    - Unencrypted email
    - Text messaging
    - instant messaging
    - unencrypted FTP
    - Mobile devices without encryption

  - When sent via fax, it must be sent only to a previously established and used address or one that has been verified as using a secure location.
  - When transmitted via USPS or other mail services, it must be enclosed in a sealed security envelope.
  - Must not be posted on any public website.
  - TStephens Management must be notified in a timely manner if information classified as Confidential has been or is suspected of being lost or disclosed to unauthorized parties.

Information Retention and Destruction

- All information stored by TStephens must be stored in accordance with the Data Retention Schedule governed by TStephens LLC.
- All information maintained by TStephens LLC must include a documented timestamp or include a timestamp as part of metadata.
- Information that is no longer required to be maintained by TStephens LLC is classified as *Expired* and must be destroyed in accordance with the Media Reuse and Destruction Standard governed by TStephens LLC.
- Information owners should be consulted prior to information destruction and may have the opportunity to extend information expiration, given business needs and/or requirements for extended retention.
- Customers of TStephens LLC may have their own information retention requirements that supersede the requirements set forth by TStephens LLC. Such customer requirements should be documented in contractual language.

References

- ISO 27002: 8, 14, 18
- NIST CSF: ID.AM, PR.DS, PR.IP
- Authentication Standard
- Data Retention Schedule
- Labelling Standard
- Media Reuse and Destruction Standard

Waivers

Waivers from certain policy provisions may be sought following the Waiver Process governed by TStephens LLC.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), or related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	July 2025		TS Security Solutions	Document Origination

Reach out to TS Security Solutions if you are interested in our services or in need of assistance.

TS Security Solutions specializes in providing consulting services related to information security.

404-555-1212 | 123 Main St NW, Suite 123

Atlanta, GA 30303