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

Acceptable Use Policy (AUP)

TS Security Solutions
7-16-2025

Acceptable Use Policy

Purpose

The purpose of creating an acceptable use policy for TStephens LLC is to create and establish acceptable practices regarding the use of TStephens LLC's resources used to protect confidentiality, integrity, and availability of information that is created, collected and maintained.

Audience

The intended audience that this acceptable use policy is any individual, entity, or process that interacts or communicates within any resources of TStephens LLC.

Contents

Policy

Acceptable Use

- Employees of TStephens LLC and partnering personnel are responsible for complying with TStephens LLC's policies and procedures when using TStephens LLC's information resources and/or while being on TStephens LLC's time. If any of the listed requirements or responsibilities are unclear, please reach out to the Human Resources department or to our Information Security team for further information or assistance.
- Employees and partnering personnel must promptly report harmful events or policy violations that involve the use, disclosure, altering or removal of TStephens LLC's assets or information, to their manager or a member of the Incident Handling team. These events include, but are not limited to, the following:
    - Technology Incident: Any potentially harmful event that can cause a failure, interruption, or loss to availability to TStephens LLC's Information resources.
    - Data Incident: Any potential loss, theft, or compromise of information or resources belonging to TStephens LLC.
    - Unauthorized Access Incident: Any potential unauthorized access to any resource belonging to TStephens LLC.
    - Facility Security Incident: Any damage or potentially unauthorized access to a facility owned, leased, or managed by TStephens LLC.

    - Policy Violation: Any potential violation of this or other policies, standards, or procedures related to or belonging to TStephens LLC.
- Personnel should avoid engaging in activities that involve:
    - Harassing, threatening, impersonating, or abusing others.
    - Degrading the performance of resources belonging to TStephens LLC.
    - Depriving TStephens' personnel of access to an information resource belonging to TStephens LLC.
    - Obtaining additional resources beyond those that had been previously allocated; or
    - Circumventing any TStephens' computer security measures.
- Personnel should avoid downloading, installing, or running security programs or utilities that reveal or exploit any weaknesses in the security of a system. Company personnel **should not** run password cracking programs, packet sniffers, port scanners, or any other programs that have not been approved for use on any information resource belonging to TStephens LLC.
- All inventions, intellectual property (IP) and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information developed on TStephens' time and/or information resources, are properties belonging to TStephens LLC.
- The use of encryption should be managed in a manner that allows personnel designated by TStephens LLC to promptly access all data.
- TStephens' information resources are to be used to conduct and facilitate company business and **should not** be used for any personal financial gain.
- All personnel are expected to cooperate with incident investigations, including any federal or state investigations.
- Personnel are expected to fully respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property (IP) rights for any software and/or materials viewed, used, or obtained using information resources provided by and belonging to TStephens, LLC.
- Personnel should avoid accessing, creating, storing or transmitting materials which TStephens LLC may consider to be either offensive, indecent, or obscene.

Access Management

- Access to information is based on the least privilege principle or "need-to-know"; personnel of TStephens, LLC will only have access to the specified information and resources needed to complete their job duties, regardless of their position and/or security clearance.
- Personnel of TStephens LLC are permitted to only use network and host address issued to them by TStephens' IT and should not attempt to access any data or programs contained on systems provided by and belonging to TStephens LLC, for which they **DO NOT** have access, authorization or explicit consent.

- All remote access connections made to TStephens' internal networks and/or environments, must be made through approved, company-provided equipment and virtual private networks (VPNs).
- Personnel **should not** disclose or reveal any access information to anyone that is not authorized to receive such information including IT support/service desk personnel.
- Personnel **must not** share their personal authentication information, including the following:
    - Account passwords
    - Personal identification numbers (PINs)
    - Security tokens (i.e. Smartcard)
    - Two-factor (2FA) or multi-factor authentication (MFA) information
    - Access cards and/or keys
    - Digital certificates
    - Similar information or devices that are to be used for identification and authentication purposes
- Access cards and/or keys that are no longer required **must** be reported to physical security personnel as soon as possible.
- A service charge may be assessed for access cards, security tokens, and/or keys that are lost, stolen, or not returned.

Passwords/Authentication

- All personnel are required to maintain the confidentiality of personal authentication information.
- Any group or shared authentication information must be maintained solely amongst the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be created and implemented according to the following rules:
    - Must meet all requirements including minimum length, complexity, and reuse history.
    - Must not be easily tied back to the account owner by using things like username, social security number (SSN), nickname, relative's names, birth date, etc.
    - Must not be the same passwords used for non-business purposes.
- Unique passwords should be used for each system, whenever possible.
- User account passwords must not be disclosed or revealed to anyone. TStephens' support personnel and/or contractors should never ask for user account passwords.
- If the security of a password is in doubt, the password should be changed immediately.
- Personnel SHOULD NOT circumvent password entry without application remembering, embedded scripts or hard-coded passwords in client software.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination/separation of the relationship with TStephens LLC, if issued.

Clear Desk/Clear Screen

- Personnel should log off from applications or network services when they are no longer needed.
- Personnel should log off or lock their workstations and laptops when their workspace is unattended.
- **Internal or confidential information** should be removed or placed inside of a locked drawer or file cabinet whenever the workstation is unattended.
- File cabinets containing **confidential information of any kind** should be locked when not in use or when unattended.
- Physical and/or electronic keys used to access **confidential information of any kind** should not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.
- Laptops should be either locked to personnel's individual desks with locking cables or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday if the laptop is not encrypted.
- Passwords must not be posted on or under a computer or in any other physically accessible location.
- Copies of documents containing **confidential information** should be immediately removed from printers and fax machines.

Data Security

- Personnel should use approved encrypted communication methods whenever sending **confidential information** over public computers.
- **Confidential information** that is transmitted via USPS or other mail and shipping service must be secured in compliance with the *Information Classification and Management Policy*.
- Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential and/or internal information.
- Information must be appropriately shared, handled, transferred, saved, and destroyed based on the sensitivity of the information.
- Personnel should not have any confidential conversations in public places or over insecure communication channels, open offices and meeting places.
- **Confidential information** must be transported by either a TStephens employee or a courier service approved by TStephens' IT Management.
- All electronic media containing **confidential information** belonging and pertaining to TStephens LLC must be securely disposed of. Please contact IT for references, assistance or guidance.

Email and Electronic Communication

- Auto-forwarding electronic communication to resources outside of TStephens LLC is strictly prohibited.

- All electronic communications should not mispresent TStephens LLC in any manner.
- All personnel are responsible for the individual accounts assigned to them and all actions taken with them as well.
- With the exception being with calendars, invites and other calendar-related functions, accounts must not be shared without receiving prior authorization from TStephens IT.
- All TStephens personnel are restricted from using personal email accounts for sending and/or receiving any **confidential information** belonging and pertaining to TStephens LLC.
- Any personal use of TStephens-provided email should not:
    - Involve solicitation.
    - Have an association with any political entity, excluding those of the TStephens sponsored PAC.
    - Have the potential to harm or slander the reputation of TStephens LLC
    - Forward chain email.
    - Contain any practices pertaining to any anti-social or unethical behavior.
    - Violate local, state, federal, or international laws, codes, or regulations.
    - Results in any unauthorized disclosure or reveal of **confidential information** belonging and pertaining to TStephens LLC.
    - Or otherwise violate any other policies governed at TStephens LLC.
- Personnel should only send **confidential information** using approved secure electronic solutions.
- Personnel should use caution when responding to or opening links or attachments included in electronic communications, especially messages that look suspicious.
- Personnel should use discretion in disclosing any confidential or internal information in Out of Office (OOO) or other automated responses, such as employment data, internal telephone numbers, location information or other data deemed sensitive.

Hardware and Software

- All hardware must be formally approved by IT Management before being connected to TStephens' networks.
- Software installed on TStephens' equipment requires prior approval from IT Management and will require the assistance of IT personnel to install.
- All assets belonging to TStephens LLC that are taken off-site should be physically secured at all times.
- All personnel traveling to a high-risk location or facility, as defined by the FBI or the Office of Foreign Asset Control, will be required to contact IT for approval to travel with corporate assets.
- Employees should not allow family members or others that are not employed by TStephens LLC to access any information resources owned by TStephens LLC.

Internet

- The Internet must not be used to communicate confidential or internal information belonging or pertaining to TStephens LLC, unless the confidentiality and integrity of the information is ensured and the identity of the recipient(s) is established.
- Use of the Internet with TStephens' networking or computing resources must only be used for business purposes and business-related activities. Unapproved activities include, but are not limited to:
    - Recreational games
    - Streaming media
    - Personal social media
    - Accessing or distributing any pornographic, sexually oriented, or other explicit materials
    - Attempting or making unauthorized entries to any network or computer accessible from the Internet, or
    - Otherwise, any other TStephens-governed policies.
- Access to the Internet from outside of the TStephens network using a TStephens-owned computer must adhere to all the same policies that apply to use within TStephens-owned facilities.

Mobile Devices and Bring Your Own Device (BYOD)

- The use of a personally owned mobile device to connect to the TStephens network is a privilege granted to employees only upon formal approval of IT Management.
- All personally owned laptops and/or workstations must have approved virus and spyware detection/protection software along with personal firewall protection active.
- Mobile devices that access TStephens' email domain must have a PIN or other authentication mechanism enabled.
- **Confidential Information** should be stored on devices that are encrypted in compliance with the encryption standard used at TStephens LLC.
- **Confidential Information** belonging or pertaining to TStephens LLC, should not be stored on any personally owned mobile device.
- Theft or loss of any mobile device that has been used to create, store, or access **confidential or internal information** must be reported to the TStephens Security Team immediately.
- All mobile devices are required to maintain up-to-date versions of all software and applications installed.
- All personnel are expected to use mobile devices in an ethical manner.
- Jailbroken (iOS/iPadOS) or rooted (Android) devices should not be used to connect to any information resources belonging to TStephens LLC.
- TStephens IT Management may elect to execute "remote wipe" capabilities for mobile devices without warning (please reference Mobile Device Email Acknowledgement).

- If there is a suspected incident or breach associated with a mobile device, it may be a necessity to remove the device from the personnel's possession as part of a formal investigation.
- All mobile device usage in relation to information resources belonging or pertaining to TStephens LLC, are at the discretion of TStephens IT Management.
- TStephens IT support for personally owned mobile devices is limited to assistance in complying with this policy. TStephens IT support may not assist in troubleshooting device usability issues.
- The use of personally owned mobile devices must follow and comply with all other policies governed by TStephens LLC.
- TStephens LLC reserves the right to revoke personally owned mobile device use privileges if personnel refuse to abide by the requirements put in place within this policy.
- Texting or emailing while driving is restricted while on company time or using company resources. Only hands-free talking while driving is permitted while on company time or when using company resources.

Physical Security

- All photographic, video, audio or other recording equipment, such as cameras, camcorders, and cameras in mobile devices, are strictly prohibited in secure areas.
- Personnel must always display photo ID access cards, while in the building.
- Personnel must badge in and out of access-controlled areas. Piggybacking, tailgating, door propping and any other activity to circumvent door access controls are strictly prohibited.
- Visitors accessing card-controlled areas of facilities must be always accompanied by authorized personnel.
- Food and drinks are not allowed in data centers. Caution must be used when eating or drinking near workstations or information processing facilities.

Privacy

- Information created, sent, received, or stored on information resources belonging or pertaining to TStephens LLC, are not private and may be accessed by TStephens IT employees at any time, under the direction of TStephens executive management and/or Human Resources, without the knowledge of the user or resource owner.
- TStephens LLC may log, review, and otherwise utilize any information stored on or passing through its information resource systems.
- Systems Administrators, TStephens IT, or other authorized TStephens personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges should not access files and/or other information that is not specifically required to carry out an employment-related task.

Removable Media

- The use of removable media for storage of information belonging and pertaining to TStephens LLC must be supported by a reasonable business case.
- All removable media use must be approved by TStephens IT prior to use.
- Personally owned removable media use is not permitted for storage of information belonging and pertaining to TStephens LLC.
- Personnel are not permitted to connect removable media from an unknown origin without prior approval from TStephens IT.
- All confidential and internal information belonging and pertaining to TStephens LLC should not be stored in any form of removable media without the use of encryption.
- All removable media must be stored in a safe and secure manner, in a safe and secure environment.
- The loss or theft of a removable media device that may have contained any information belonging and pertaining to TStephens LLC, must be reported to TStephens IT.

Security Training and Awareness

- All new personnel must complete an approved security awareness training course prior to, or at least within 30 days of, being granted access to any information resources belonging and pertaining to TStephens LLC.
- All personnel must be provided with and acknowledge that they have received and agree to adhere to the Information Security Policies governed by TStephens LLC, before they are granted access to information resources belonging and pertaining to TStephens LLC.
- All personnel are required to complete the annual security awareness training.

Social Media

- Communications made with respect to social media should be made in compliance with all applicable policies and procedures governed by TStephens LLC.
- Personnel are personally responsible for the content that they publish online.
- Creating any public social media account intended to represent TStephens LLC, including accounts that could reasonably be assumed to be an official TStephens account requires the permissions of the TStephens Communications Departments.
- When discussing TStephens LLC or any TStephens-related matters, you should:
    - Identify yourself by name
    - Identify yourself as a TStephens representative, and
    - Make it clear that you are speaking for yourself and not on behalf of TStephens LLC, unless you have been explicitly approved to do so.
- Personnel should not misrepresent their role at TStephens LLC.
- When publishing TStephens-relevant content online in a personal capacity, a disclaimer should accompany the content. One example of a disclaimer could be: *"The opinions and content are of my own and do not necessarily represent TStephens' position or opinion."*

- Content posted online should not violate any applicable laws (i.e., copyright, fair use, financial disclosure, or privacy laws).
- The use of discrimination in published content that is affiliated with TStephens LLC, will not be tolerated. This would include discrimination against age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status or any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances.
- Confidential information, internal communications and non-public financial or operational information may not be published online in any form.
- Personal information belonging to customers may not be published online.
- Personnel that are approved to post, review, or approve content on TStephens' social media sites must follow the Social Media Management Procedures as governed by TStephens LLC.

Voicemail

- Personnel should use discretion in disclosing confidential or internal information in voicemail greetings, such as employment data, internal telephone numbers, location information or other sensitive information.
- Personnel should not access another user's voicemail account unless it has been explicitly authorized.
- Personnel must not disclose or reveal confidential information in voicemail messages.

Incidental Use

- As a convenience to TStephens personnel, incidental use of Information Resources is permitted. The following restrictions apply:
    - incidental personal use of electronic communications, Internet access, fax machines, printers, copiers, etc., are restricted to TStephens-approved personnel; it does not extend to family members or other acquaintances.
    - Incidental use should not result in direct costs to TStephens LLC.
    - Incidental use should not interfere with the normal performance of an employee's work duties.
    - No files or documents may be sent or received that may cause legal action against or embarrassment to TStephens LLC or the company's customers.
- Storage of personal email messages, voice messages, file and documents within information Resources belonging to and pertaining to TStephens LLC, must be nominal.
- All information located on Information Resources belonging and pertaining to TStephens LLC, may be subject to open records requests and may be accessed in accordance with this policy.

References

- ISO 27002: 6, 7, 8, 9, 11, 12, 13, 16, 18
- NIST CSF: PR.AC, PR.AT, PR.DS, DE.CM, DE.DP, RS.CO
- Asset Management Policy
- Encryption Management Policy
- Encryption Standard
- Identity and Access Management Policy
- Incident Management Policy
- Information Classification and Management Policy
- Mobile Device Acknowledgement
- Personnel Security and Awareness Policy
- Physical Security Policy
- Social Media Management Procedure

Waivers

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

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.

Version History

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

Acknowledgment of Receipt and Understanding

I acknowledge that I have received, read, and understood the Acceptable Use Policy for TStephens LLC. I understand that violating this policy may result in disciplinary action and/or legal consequences.

_____

Name

_____

Signature

_____

Date

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