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

Risk Assessment Report

TS Security Solutions
7-19-2025

Risk Assessment Report

Purpose

This report is intended for authorized stakeholders of TStephens LLC and its clients who are responsible for reviewing, managing, or acting on identified security risks.

Audience

This report is intended for internal stakeholders of TStephens LLC, including executive leadership, system owners, IT security personnel, and compliance staff responsible for the oversight, risk management, and operation of identified security risks.

Policy

TStephens LLC performs structured risk assessments to help identify, evaluate, and manage security risks to systems and services. These assessments support informed decision-making, guide control implementation, and align with recognized frameworks such as NIST and ISO to meet organizational and regulatory requirements.

Methodology

This assessment used a qualitative risk analysis approach, guided by:

- NIST SP 800-30 Rev. 1 (Risk Assessment Guidelines)
- NIST CSF – ID.RA and ID.RM
- ISO 27005

The following criteria were used:

- Likelihood: Rated as High / Medium / Low
- Impact: Assessed across confidentiality, integrity, and availability
- Risk Score: Mapped to qualitative levels (High, Medium, Low)

Risk Identification & Analysis – SecureMail Gateway System (Example)

Risk ID	Threat/ Vulnerability	Asset	Likelihood	Impact	Risk Rating	Mitigation Strategy	Owner
R-01	Phishing Bypass via Zero-Day Exploit	Email Filtering System	Medium	High	High	Enable sandbox analysis; enforce attachment stripping for high-risk file types	Security Team
R-02	Misconfigured API to 365	Microsoft 365 Integration	Low	High	Medium	Conduct quarterly API reviews and access control validation	Cloud Admin
R-03	Lack of admin MFA	SecureMail Admin Portal	Medium	High	High	Enforce MFA + IP allowlisting for admin access	IT SecOps
R-04	Data leakage via outbound emails	End User Data	High	Medium	High	Implement content filtering + outbound encryption	DLP Team

Risk Treatment

Each identified risk will be assigned to the appropriate team and tracked through the organization's Risk Register. Risk treatment options include mitigation, transference, acceptance, or avoidance, depending on criticality and business tolerance.

Monitoring & Review

The platform in question (in this sample policy, SecureMail Gateway System) will be included in the organization's annual risk review cycle. Additional reviews may be initiated following significant system changes, vendor updates, or observed incidents.

References

- NIST SP 800-30 Rev. 1
- NIST CSF: ID.RA, ID.RM, PR.IP
- ISO 27005:2018
- Risk Management Policy v1.0.0
- Information Classification & Handling Policy v1.0.0

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