InfoSec at Posh

We help keep data safe, every step of the way

Given the critical work performed on our platforms, information security is our lifeblood.
Our industry-leading InfoSec team works tirelessly to stay ahead of adversaries by hunting for sophisticated threats, and mitigating risk.
Our information security program is designed to meet or exceed industry standards, and we use many different controls to keep your personal information safe.

Posh is certified in internationally-recognized standards like CSA STAR Level-2 and is SOC-2 Type 2 accredited.

The InfoSec program at Posh has following core objectives:

- Security based on well-architected design principles based on NIST standards
- Risk management supported by frameworks, best practices, controls and technologies
- Detect, investigate and respond to threats faster
- Provide secure access to systems, data and resources
- Protect our key business apps from fraud and web attacks
- Digital risk protection and attack surface management

Compliance Overview

Posh's SaaS AI infrastructure, applications, and operations have been developed to comply and align with some of the most rigorous legal and regulatory requirements in industries today, including:

- SOC 2, Type 2 (Security, Confidentiality,, Privacy and Availability)
    - Report provided upon request
- SOC 3 Type 2
    - Report is available here
- CSA STAR Level 2
    - Reports available here

And others, including:

- GDPR
- GLBA (Gramm Leach Bliley Act)

Data Security

Your financial information is both personal and powerful – that's why security is a top priority when we're designing our products, policies, and practices. Our information security program is designed to meet or exceed industry standards, and we use many different controls to keep your personal information safe.

Data encryption

Posh leverages TLS1.2+ for the encryption of traffic in transit and DEKs with AES-256 encryption for the encryption of data at rest.

Strong authentication

Posh requires multi-factor authentication along with complex passwords and regular rotation of passwords for added security to help protect your data in our systems.

Cloud infrastructure

Posh uses highly available, secure cloud infrastructure technologies to enable you to connect quickly and securely.

Robust monitoring

Posh's SaaS AI platform and all related components are continuously monitored by our information security team.

Penetration testing

We perform regular penetration tests to ensure our backing infrastructure and operations meets the highest security standards.
Current or prospective customers can reach out to Posh to learn more about our security assessments.

Application Security

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

Posh leverages OWASP Top 10 framework as its bedrock and as core foundation of its Web Application security.
Posh also addresses the following elements to establish effective application security policies:

- **Vulnerability prioritization** - Posh's application security policies apply a standard on what constitutes high, medium, and low risks. This helps us determine which vulnerabilities must be addressed and which to flag for consideration.
- **Remediation and mitigation** - This is closely tied to vulnerability prioritization, but gets more specific. Who determines what must be remediated? When should a vulnerability be fixed in the development process? Are there acceptable risks?
- **Processes** - Application security policies define the process by which security is applied to application code, for example use of SAST & DAST.
- **Roles and responsibilities**- The policy defines who is responsible for ensuring application security and at which stages in the SDLC.
- **Tool-specific** - Posh employs multiple security automation tools; the policy defines which tools will be used at which point in the SDLC.
- **Monitoring** - Application vulnerabilities can be discovered after the code has been pushed into production. Posh's policies define how deployed applications are monitored and use the priorities defined above to determine corrective actions.

Availability & Resilience

Business Continuity Planning / Disaster Recovery

Posh partners with Google Cloud for geographical-specific deployment options. This flexibility allows us to enable a robust failover system. We perform database and content backups at least daily and retain backups for no less than 14 days. All backup data is encrypted and held securely within Google's geographic redundant cloud platform.

Business Continuity Testing & Documentation

Posh tests business continuity and failover plans at scheduled intervals to ensure their continuing effectiveness. Posh's plan, process and the successful execution of this effort is independently audited via our SOC-2 auditors.

Environmental Risks

Posh's hosting partners deploy certified datacenters with countermeasures implemented against natural disasters, attacks, and other environmental and security risks, as well as equipment power failures, network disruptions, and outages.

Questions

If you have any questions, please do not hesitate to contact security@posh.tech