posh

Security Overview

March 2022

Contents

Introduction

Posh Tech Mission Statement

Our mission is to make AI accessible and bring better digital banking experiences to every financial institution. Banks and credit unions thrive when their customers thrive. Our top priority is a flawless end-user experience that's accessible to all. A close second, though, is making things easy—more self-service, simpler interfaces, and total personalization for all AI banking assistants.

Our Security Culture

Posh Tech promotes a robust, resilient and proactive approach to our security culture. By partnering with Google Cloud, we align our services by adopting a number of Google enhanced security services which manifests itself throughout our processes, culture, controls, policies and during the employee hiring process. One example is that all employees or contractors are required to successfully complete their assigned security awareness training and all users are required to use multi-factor authentication to access even basic services like email. The cornerstone of our security philosophy is deeply grounded in the Confidentiality, Integrity and Availability (CIA) principles.

Employee background checks

Before they join our staff, Posh Tech will verify an individual's education and previous employment and perform internal and external reference checks. Where local labor law or statutory regulations permit, Posh Tech may also conduct criminal, credit, immigration, and security checks. The extent of these background checks is dependent on the desired role.

Employee security training

All Posh Tech employees undergo security training as part of the orientation process and receive ongoing security training. During onboarding, new employees agree to our code of conduct highlighted in our employee handbook which highlights our commitment to keep customer information safe and secure.

Depending on their job role, additional training on specific aspects of security may be required. For instance, the Posh engineering team instructs new engineers on secure software development lifecycle training. The VP of Security and Compliance provides

technical presentations on security-related topics and publishes a security newsletter that covers new threats, attack patterns, mitigation techniques and more.

Change Management

Posh Tech uses internal tools to track all production incidents, problem and change requests. Separation of duties are adopted between the requester and implementer for production system changes. Specific processes in our change management process include rollback plans, test plans, back-up plans, and post-change reviews are incorporated to ensure we fully test changes prior to release and have an efficient plan to rollback changes in the event they cause unexpected results for our customers.

Product Level Security

To secure our SaaS based services, Posh adopts several security controls to protect their customers' content and information. For example, we adopt TLS 1.2 today but are in the process of incorporating TLS 1.3 for all data in transit communication along with strong ciphers. Our customers' information is encrypted at rest using Data Encryption Keys which are hosted, managed and controlled by Google and use an AES-256 key strength. Our roadmap will ensure our Top-Level Domain (TLD) is registered on the HSTS preload list across all main web browsers. This change will enforce HTTP Strict Transport Security protocol across all main web browsers thus further securing our connection between Posh and our clients.

A dedicated security team

Posh Tech’s dedicated security team actively scans for security threats using commercial and custom tools, penetration tests, quality assurance (QA) measures, and software security reviews. Within Posh Tech, members of the information security team review security plans for all networks, systems, and services. They monitor suspicious activities on Posh Tech's hosted networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments.

Privacy as a part of the development process

The security team operates separately from product development but participates in every Posh Tech product launch by reviewing design documentation and performing code reviews to ensure compliance with privacy standards. Posh’ Privacy by Design process incorporates conducting a Data Privacy Impact Assessment for all major new product releases.

Partnerships: Internal audit and compliance specialists

Posh Tech partners with Google Cloud. Google has a dedicated internal audit team that reviews compliance with security laws and regulations around the world. As new auditing standards are created, the internal audit team determines what controls, processes, and systems are needed to meet them. This team facilitates and supports independent audits and assessments by third parties. Posh Tech engages with Google teams as part of validating that our customer's compliance needs are met. Learn more about Google's compliance standards and security controls here.

Vulnerability management

Posh's engineering teams engage in a vulnerability management process which actively scans for security threats using a combination of commercially available and purpose-built in-house tools. Intensive automated and manual penetration efforts, quality assurance processes, software security reviews, and external audits are performed to ensure we adhere to our defense in-depth controls.

Endpoint Security

Posh adopts enhanced security controls across all company issued endpoints by enforcing a remote monitoring and management tool which allows our security team to manage, monitor and enforce policy restrictions related to our endpoints. The enforcement of these controls and measures reduces our attack surface considerably.

Application Security

Application Security

Posh AI and ML platform adopts several security controls from a secure software development perspective. Our development teams are required to follow OWASP Top 10 and SANS CWE 25 best practices when it comes to developing our chatbots, webhooks, web bots and IVR solutions

Our security practices are based on the core foundational components of OWASP here and governed through tools which perform SAST and DAST scans prior to the APIs being pushed to production.

Data Integrity

We implement data input and output integrity routines across our platform to ensure application interfaces and databases are protected from manual or systematic processing errors or data corruption. Posh Tech has also established policies and procedures in support of data security to avoid improper disclosure, alteration or destruction of data. These processes and internal tools address change detection and FIM alerts on critical production systems.

Audit Assurance & Compliance

Audit Planning

We have an extensive security process that includes ongoing testing of our hosted systems. We also undertake independent third-party assessments of our platform.

We have recently achieved our SOC-2 Type II compliance standard. We are currently working on a Cloud Security Alliance STAR Level 1 accreditation and have more compliance standards targeted for 2022.

Independent Audits

Posh's security team firmly believes in independent, unbiased opinions as it relates to their security program, defense in-depth controls and championing security across all stakeholders. Using this theme, Posh undertakes independent third-party assessments of our platform, third-party penetration tests of our application and infrastructure in order to provide our clientele with a high degree of confidence that our internal controls meet industry best practices.

Our hosting partners hold certification reports, such as SOC1, SOC2, SOC3 & PCI DSS, thus requests for copies of those reports would need to be directed at them. You can do so here: https://cloud.google.com/security/compliance/

Business Continuity Management & Operational Resilience

Business Continuity Planning / Disaster Recovery

Posh Tech 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

We test our business continuity and failover plans at scheduled intervals to ensure their continuing effectiveness. Our plan, process and the successful execution of this effort has been independently audited via our SOC-2 auditors.

Environmental Risks

Our 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. To learn more please go here.

Data Security

Data Classification

Through our Data Loss Prevention tools, we govern our data classification standards through tightly managing access to information, services and systems which may contain Restricted, Confidential and Private data. Posh does not limit access to “Public” data. In addition to our technical controls, our acceptable use policy, legal notice and privacy policy provides additional governance controls.

Data In Transit

Data flows between customer systems and the Posh cloud platform communicates over TLS 1.2 encrypted communications. We are in the process of moving to TLS 1.3. We additional recommend our partners review our ranking on Security Scorecard

Data Encryption

Posh leverages Data Encryption Keys through their cloud provider to encrypt all data at rest. The key management lifecycle for the Data Encryption Keys is managed by our cloud provider, so we do not need to be concerned with the secure rotation and destruction of the keys. The current key strength being adopted is AES256.

Entitlements & Key Generation

Posh uses security tokens generated upon session start to grant access within the platform. The lifecycle of these security tokens is valid for each active session. Upon session expiry after a set period of time, a new security token will be generated. At no time are these security tokens surfaced within the platform interface. In the event of a security incident, security tokens can be revoked as a means of containment.

Non-production Data

All non-production nodes in our cloud providers zones are both logically and physically segmented with several role-based access controls in place regarding who has access to the environment. Customer production data is not copied nor used in non-production.

Secure Disposal

Posh leverages Google's method of secure sanitization of customer data once the relationship between the customer and Posh ends. Google’s Data Deletion standards follow NIST SP 800-88 guidelines.

We adhere to NIST's special publication on "Guidelines for Media Sanitization" for secure disposal of data. To learn more, visit https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

Identity and Access Management

Auditing & Logging

All access is through our SAML 2.0 IdP is logged, and user’s authentication is validated by a strong password/passphrase policy.

User and Privileged Access

All Posh users are required to authenticate using a company-owned device which has a remote monitoring and management and mobile device management tool implemented which is wrapped around several technical controls. User authentication requires multi-factor authentication. Privileged Access users require to authenticate through controls defined by our remote monitoring and management tool. Privileged Access users are additionally presented with VPN-enforced controls to complete their MFA process prior to being able to perform administrative functions on the platform. Developers do not have access to production or production data.

Access reviews for privileged accounts are reviewed on a quarterly basis. All standard user access is reviewed on an annual basis.

User Access Revocation

In the event Posh requires revoking user access enforced Remote Monitoring and Management tools along with Single Sign-On controls, a user's access can be efficiently and effectively disabled. In the rare event of a security event, a device can be remotely wiped or removed from our network as part of our containment strategies.

User ID Credentials & Passwords

Posh adopts strong password/passphrase policies for user access. This is a sample of the complexity of our policy:

- A minimum of 12 characters.
- Must be a combination of:
    - uppercase letters (A-Z)
    - lowercase letters (a-z)
    - numbers (0-9) or special characters (!@?#$%&*)
- Does not contain the current username.
- Does not contain more than 3 consecutive repeating characters.
- Does not repeat the last three passwords/passphrases.

Password Expiry, Session Logout & Account Lockout

Posh passwords do not have expiry configurations in line with the latest NIST standards. Alternatively, a combination of AI-driven technologies powered by Google Cloud Platform enforces several controls when a user attempts to authenticate to our internal systems.

Data Usage

Data Privacy Regulations

Our part of our Data Protection Agreement, our contractual agreement, stipulates the customer as the controller, Posh is the processor and our sub-processor is Google. We adopt a number of hashing, cryptography, encryption and pseudonymization controls to ensure our customer data is confidentiality stored and processed.

In the event we receive law enforcement requests for data disclosure, we will notify our customers as part of the due diligence disclosure process.

Posh constantly updates their privacy policy as regulatory standards are updated and adheres the right to erasure requests and data deletion requests for example. In the event you may have questions, please contact us at privacy@posh.tech

Governance & Risk Management

Documented Procedures and Training

Posh Tech takes care that internal teams are aware of security guidelines and procedures, through detailed documentation and recurring training, we can maintain awareness of and compliance with our security standards for employees' areas of responsibility.

Policy Enforcement

All employees are made aware of the actions that will be taken in the event of a violation of our policies and procedures. Formal disciplinary and sanction policies are in place for employees who violate security protocols.

Policy Changes & Reviews

As a result of recurring risk assessments and the general evolution of technology, Posh Tech may need to adjust existing privacy and security policies. When making changes to any of our published policies, we take care to inform our tenants of the changes to these policies, procedures, standards, and controls to ensure they remain relevant and useful.

Risk Management

Posh adopts the NIST Risk Management Framework guidelines as a manner of guiding us through the risk process. Additional models like Octave Allegro are also used to provide a broad, in-depth risk profile of internal assets, internal systems, data stored, users and third-party risk assessments (if applicable). For risks which lacked identification during a risk assessment review, a risk treatment plan is adopted to ensure a gap/identification failure is not found. Using the NIST approach a risk ranking profile is assigned to all critical assets and third parties who are sub-processors of data.

Interoperability & Portability

Network Traffic

Posh segmented firewalls are built on a zero-trust architecture which prohibits administrators being able to laterally move through the network without re authenticating. As part of our architecture explicit firewall rules are “allowed” based on ingress/egress traffic. Insecure ports and protocols are disabled, in addition to deprecated ciphers.

Virtualization

Windows Operating Systems are not used across the platform. Our shared responsibility model is a combination of IaaS and PaaS services from Google. Due to the confidentiality of the platform and our security landscape, additional information is not disclosed at this time, but our SOC-2 audit does provide some additional information regarding our virtual environment. We do not host physical datacenters.

Additional Security Measures

Incident Response Plan

We aim to ensure Posh customers do not experience an outage or a security incident. However, an Incident Response Plan outlines the roles and responsibilities of Posh Tech and its users during such an event. Each plan is tailored to a specific incident type and is issued to account owners should a security incident occur. Our process is based on NIST guidelines. Additional information can be found in our SOC-2 report. We do not share the plan or policy externally due the confidential nature of the exercises we perform when attempting to deconstruct the cyber kill chain. In order to regularly test the plan, we may perform table-top exercises or purple team events.

Logging & Tracking

The Posh engineering and security teams log, monitor and alert on application, system, and security events daily. Internal audit reviews are conducted on a quarterly basis.

Customer-initiated security testing

Due to security tools proactively monitoring the platform, we do not allow security scans or penetration tests to be performed on the platform. Any such tests may be conceived as a potential threat and the ingress IP’s may be blocked from our platform.

Threat and Vulnerability Management

External and internal software security testing

Our security team performs automated and manual software security testing, as well as network vulnerability testing on an on-going basis to identify and resolve potential security vulnerabilities and bugs in our software.

Application security scanning is done as part of our development and release processes as well as being performed periodically in isolated environments during the lifecycle of the application.

Vulnerability management is done continuously with scans occurring at regular intervals across our entire infrastructure. At a minimum, this happens weekly, but for most systems, it happens several times a day.

Vulnerability & Patch Management

Policies and procedures have been established and supporting processes and technical measures implemented, for timely detection of vulnerabilities, infrastructure network, and system components to ensure the efficiency of deployed security controls.

A change management process is in place for all patches, configuration changes, or changes to Posh Tech software.

We patch continuously as soon as we are made aware of an issue or as soon as it is administratively feasible.

Questions

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