Demostack Privacy & Security

Jan, 2024

demostack

[External]

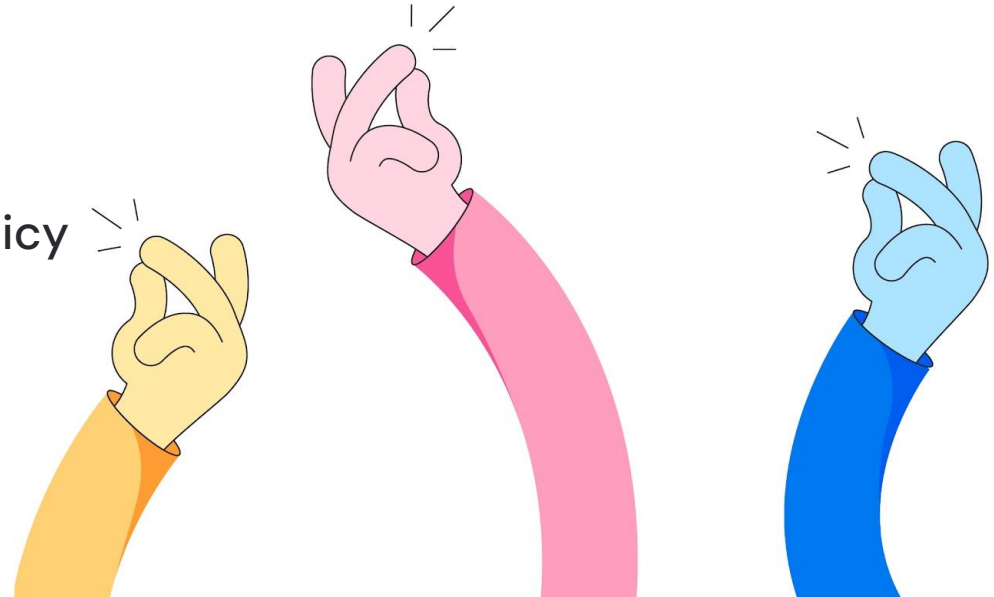
Agenda

01 Demostack Commitment to Privacy and Security

02 Security and the SOC 2

03 Privacy, GDPR and HIPAA

04 Security Assurance and Policy



Demostack Commitment to Privacy and Security

Demostack is committed to Privacy and Security as core values, and competitive differentiators.

Security is very much part of our DNA

Broad security experience and skills within staff

Strategic Priorities

Security and the SOC 2

Privacy, GDPR and HIPAA

We don’t sell customer data / personal information to any third party.

demostack

[External]

Security and the SOC 2

Earned SOC 2 Type 2 with PWC for period ending October 31, 2023

- Covers Security and Confidentiality Trust Services Criteria
- “Unqualified” Attestation: no control gaps identified

Security “defense in depth” strategy

- Data Center and Network Security
- App Security and Data Security
- Independent Penetration Testing and Code Review Testing

[External]

Data Center and Network Security

We run in Google Cloud Platform, in US

- Google Kubernetes Engine (GKE)
- Cloud CDN (Content Delivery Network)
- Cloudflare for frontend assets
- Key Management
- Nothing “on-prem”
- Environments separation (dev, testing, production)

We use Google Security Command Center to monitor assets, identify vulns / misconfigurations, detect threats, and assess compliance against security standards.

[External]

Application and Data Security

All customer data is encrypted at rest and in transit

Authenticate with Okta Identity Providers-support SAML, SSO, OID

OSS compliance reviews

Use a variety of external security services to monitor and alert

- SonarCloud for vulnerability detection and mgmt - SAST, 3rd parties
- OneTrust for Continuous Compliance Monitoring
- Security Scorecard rates Demostack on 10 dimensions, an “A”, Intruder.io scans

Domain security and Email security implemented

- Full DMARC deployed (Domain-based Message Authentication, Reporting and Conformance)
- BIMI deployed and enforced

Roles-based security awareness and training for Engineers, All Staff

Application and Data Security (continued)

- Substantial Security expertise and certifications among engineers
- External Pen tests semi-annually (“black / gray box testing”)
- External Code Review program throughout the year (“white box testing”)
- Deployed automated Test-driven development (TDD) methodology
- Active, monthly security and data privacy meetings - conducted and reported to highest levels in Org

[External]

Privacy by Design

Thinking strategically about how privacy practices fit into Demostack's overall business strategy makes privacy a core part of the Demostack business model.

Competitive differentiator.

[External]

Privacy and Data Protection Frameworks

GDPR

EU-UK Data Processing Agreement and SCCs complete

Working with Privacy Consultancy to audit, continually improve Policy processes and tools

HIPAA

Demostack is compliant with the HIPAA Privacy and Security standards as a Business Associate

CCPA/CPRA

Not yet subject to CCPA, but working toward compliance

Expanding capability to remove PII *before* being stored -"PII Shield"

[External]

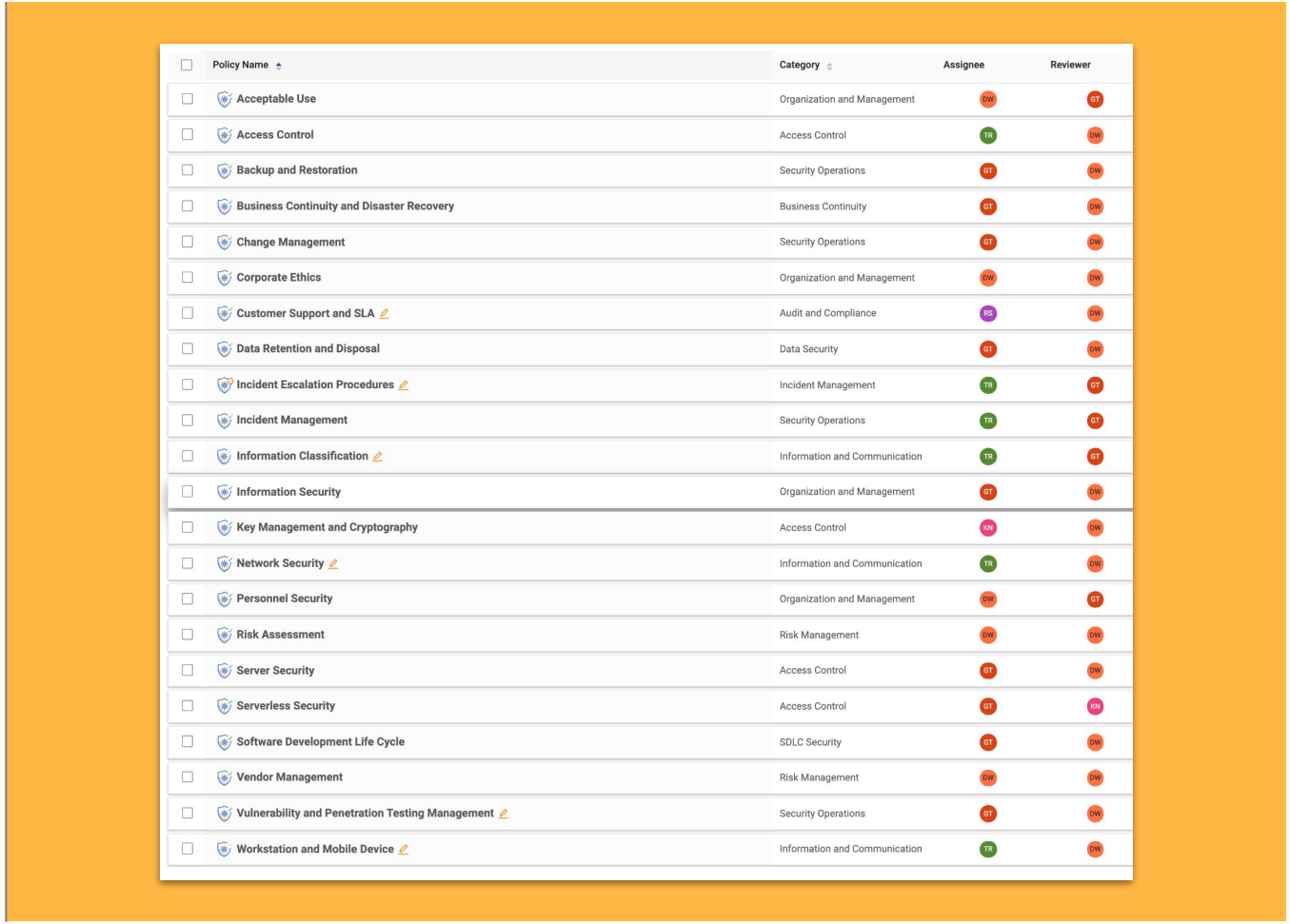
Security Assurance with OneTrust and Tugboat Logic

- Deployed Continuous Monitoring and Assurance
  - Example: GCP Integration
  - Integration supports automated evidence collection for many security controls: cloud IAM configuration, cloud firewall rules, cloud data at rest encryption, system event logging, and system performance and capacity monitoring.
- InfoSec Policy Mgmt and Controls
- Vendor Risk Management
- Security Awareness and Training

[External]

Information Security Policies

.



Policy Name	Category	Assignee	Reviewer
Acceptable Use	Organization and Management	DW	GT
Access Control	Access Control	TR	DW
Backup and Restoration	Security Operations	GT	DW
Business Continuity and Disaster Recovery	Business Continuity	GT	DW
Change Management	Security Operations	GT	DW
Corporate Ethics	Organization and Management	DW	DW
Customer Support and SLA	Audit and Compliance	RS	DW
Data Retention and Disposal	Data Security	GT	DW
Incident Escalation Procedures	Incident Management	TR	GT
Incident Management	Security Operations	TR	GT
Information Classification	Information and Communication	TR	GT
Information Security	Organization and Management	GT	DW
Key Management and Cryptography	Access Control	KN	DW
Network Security	Information and Communication	TR	DW
Personnel Security	Organization and Management	DW	GT
Risk Assessment	Risk Management	DW	DW
Server Security	Access Control	GT	DW
Serverless Security	Access Control	GT	KN
Software Development Life Cycle	SDLC Security	GT	DW
Vendor Management	Risk Management	DW	DW
Vulnerability and Penetration Testing Management	Security Operations	GT	DW
Workstation and Mobile Device	Information and Communication	TR	DW

[External]

Contacts

Privacy: Aaron Hakim, CTO and DPO
Legal: Gal Bruck

privacy@demostack.com

Security: Gonen Tiberg, Director of Engineering and CISO

- *CISM, CDPSE, Member ISACA*
- *Reports to CTO, member of Leadership team.*
  Former Security Officer for FCA-regulated fintech startup Covercy

security@demostack.com

Our Trust Center resources

- *https://www.demostack.com/trust-center*
- *https://www.demostack.com/privacy*
- *https://www.demostack.com/security*

[External]

Thank You!

demostack

[External]