Vitamin Software's

Commitment to Security

Introduction

Working responsibly with people's private data and companies' sensitive information is not easy. The world is more connected than ever, and cyberthreats are constantly evolving. We at Vitamin Software believe that our customers thrive in environments made safe and secure by trusted partners.

Our customers' success is what drives us forward, and we work hard to achieve this goal. Information security is one of our top priorities. All of our products and processes include security controls, from software development and systems architecture to hiring and operational procedures.

This paper describes the enterprise security principles and practices implemented by Vitamin Software to protect our and our customers' assets.

Values and Security Leadership

Vitamin Software is built on four core values: **Empathy, Entrepreneurial Mindset, Transparency, and High Standards.** These values guide our every step, and customers

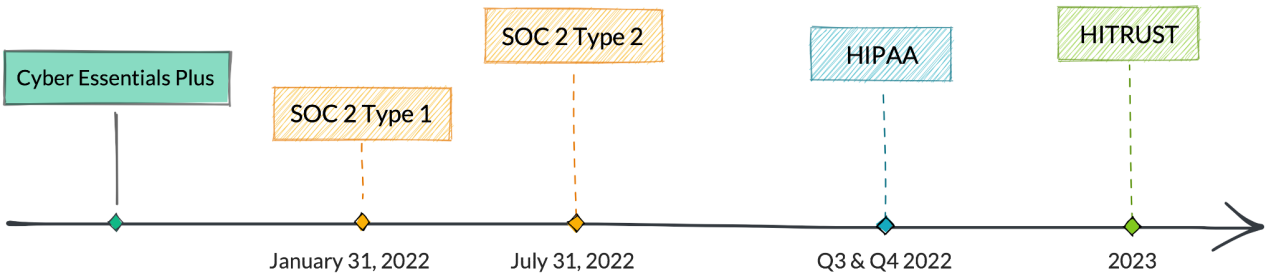
trust us to uphold them as a promise. We embed these values in everything we do to ensure our customers' success.

Our focus on security starts at the highest level Our Chief Information Officer (CIO) and Chief Information Security Officer (CISO) develops our information security strategy and implements measures that protect our customers and us against current and potential security threats.

Our CIO (also acting as our CISO) is Catalin Andrei. Catalin has held technology leadership roles for the past 15 years. Previously Senior Director of IT at Development Gateway, his expertise in information security is based on the design and implementation of information systems and data portals for UN agencies, country governments and international organizations like the World Bank, AfDB, AFD, etc. With each organization mandating an Information Security Policy to be followed when building any system that accessed or stored their information (like the World Bank's Information Security Policy for Contractors), Catalin gained hands-on experience with some of the world's toughest information security controls.

Catalin ensures that all technology created by Vitamin is created through secure processes, using secure resources, and meets customer expectations.

Certification Roadmap



To demonstrate our adherence to strict security standards, we are working to obtain relevant information security certifications. As a first step, we obtained the ***Cyber Essentials Plus*** certification. Supported by the UK Government, Cyber Essentials helps organizations protect themselves against common online threats.

We anticipate obtaining the SOC 2 Type 1 certification by January 31, 2022 and SOC 2 Type 2 certification by July 31, 2022.

In Quarters 3 & 4 of 2022 we will work on obtaining a HIPAA compliance certification, and in 2023 we aim to become HITRUST certified.

> *In the following sections, you'll read how we implement these security standards across our entire workflow. The content of this document is regularly updated to reflect the current status of the security controls we employ. This document should be used as a starting point for more in-depth conversations on our security approach.*

Contractual Framework for Information Security

When we engage with a prospective customer, we make sure that any information shared during the discovery process is well protected by signed agreements. Documents we typically use while engaging with potential customers include:

- A Non-Disclosure Agreement (NDA), because we never discuss private information – including a customer's business needs – without making sure it's protected.
- We describe our security controls in detail by completing client security questionnaires.

- When appropriate, we sign a Business Associate Agreement or Business Associate Subcontractor Agreement.

Prior to starting a customer engagement, we also sign a Master Services Agreement that reinforces our commitment to security. Our engagements are backed by professional liability insurance from ***The Hartford*** and ***Groupama***, both of which have explicit coverage for cybersecurity risks.

Trusted Vitamin Personnel

To mitigate risks related to intentional or unintentional security breaches, Vitamin Software enforces a number of human resource and operational protocols. We decrease the risk of insider threats by performing background checks, and ensure our practices are in line with our team members' legal jurisdictions. We remove any reliance on manual controls by enforcing our Information Security Policies through centrally managed solutions. And we ensure our staff stay up to date with the latest security risks and mitigation measures through continuous training.

Background Check

All new Vitamin Software employees will be based in the United States or Europe. Our recruitment process includes signing an NDA with the candidate before discussing positions in detail, and a criminal and financial background check conducted by the international service ***Certn***.

Location

Vitamin Software is headquartered in Delaware, US and our team members are based in the United States and Europe. Our customers work with Personal Identifiable Information (PII), Protected Health Information (PHI), and other types of sensitive data. Because our team members sometimes have access to that data, we implement all relevant HIPAA,

GDPR, and other necessary information protection requirements throughout our workflows.

Adherence to Information Security Policies

All Vitamin Software employees must acknowledge and adhere to the Information Security Policies:

- Acceptable Use Policy
- Asset Management Policy
- Backup Policy
- Business Continuity/Disaster Recovery Plans
- Code of Conduct
- Data Classification, Deletion, and Protection Policies
- Encryption and Password Policies
- Incident Response Plan
- Physical Security Policy
- Responsible Disclosure Policy
- Risk Assessment Policy
- Software Development Life Cycle Policy
- System Access Management Policy
- Vendor Management Policy
- Vulnerability Management Policy

Vitamin Software employees work on company-owned computers and must comply with the requirements of the above Information Security Policies. Our suppliers must also comply with the same control measures, or prove they implement comparable control measures.

To ensure that measures are properly implemented, we use the following solutions:

- A centrally-managed system configuration to enforce strong password policies, auto-lock with password prompt when the user is away, and push operating system automatic updates

- Tenable.io for daily vulnerability management and automatic patch rollout via Desktop Central
- Drata Agent to monitor device compliance with information security policies
- 1Password for secure credential storage
- Named accounts

In addition:

- All devices must use a firewall to block incoming connections
- Workstation and external (e.g. backup disk) hard drives must be encrypted
- Day-to-day work is completed through non-privileged user accounts
- Anti-malware and antivirus software monitors all accessed files and visited websites

New employees acknowledge and implement information security policies as part of the onboarding process. Existing employees must acknowledge and adhere to any policy updates.

All employees undertake mandatory annual security training, and any additional training deemed necessary by our CISO.

Secure Software Development Lifecycle

Vitamin Software solutions are secure because we make them that way. From design to implementation, we protect our customers' data at all stages. After determining the security requirements of each project, we "buff up" system infrastructure with all relevant countermeasures for potential vulnerabilities. We proactively prepare solutions for

possible issues and enforce secure coding principles to eliminate trivial vulnerabilities. This allows our engineers to focus on building a market-ready solution.

Development Environment Setup

When onboarding new customers or projects, we apply the following strict infrastructure security measures:

- Operating system (OS) updates are installed automatically
- Web application firewalls are put up to detect and prevent attacks like SQL injection, cross-site scripting (XSS), denial-of-service, low reputable IPs, etc.
- Network intrusion detection systems (NIDS) are set up to receive alerts for any suspicious activity
- Tight security groups are built when defining who can access services
- Resource monitoring and alerting systems are configured to detect any unusual usage patterns

In addition, we try to use infrastructure as code wherever possible. This allows for quick and easy resource management in case of emergencies.

We favor browser-based shells (e.g. AWS Session Manager, AWS CloudShell, GCP Cloud Shell) as they already require Two-Factor Authentication to access the cloud provider's management console. When such services are not supported, we use a bastion host for SSH access to servers.

For password management, we actively encourage our customers to apply the same principles that we do (e.g. trusted password management solutions, named accounts).

Contributing code

The software development process is based on a series of principles that put information security first:

- Our engineering team is trained on the OWASP Top 10 web application security risks on a regular basis, for awareness when developing and reviewing code

- Code reviews are mandatory before code reaches the mainstream branch
- Secrets (e.g. user credentials) are kept in trusted services (e.g. AWS Secrets Manager)
- Principle of Least Privilege is applied when developing code and configuring services

Deployment to production and monitoring

Our responsibility to keep our customers' assets safe does not end when we've built the solution. Our Quality Assurance process keeps any issues from slipping into production, avoiding unauthorized information disclosure and regressions. We also keep an eye out for unexpected events and usage patterns to ensure a timely response to security threats or functional failures.

The final stages of releasing code into production and monitoring software performance makes use of information security best practices:

- Before releasing code to production, functional testing is performed and edge cases are tested
- Automated continuous integration and continuous delivery (CI/CD) is used for build and deployment
- Automated reviews are performed to identify vulnerabilities in dependencies (e.g. Dependabot)
- Unexpected events in the software are monitored using Sentry
- Log alerts are set up for exceptions or for specific security incidents

Suppliers

We apply the same standards with our suppliers as with our clients and employees. No information is exchanged without an NDA. When we work under a BAA, we request our contributing project partners to also sign a BAA.

Depending on the type of service a supplier provides and the nature of our relationship, our CISO may decide additional measures are needed. For example, our CISO may assess a consultant's compliance with security standards, and may require the consultant to employ synthetic data when testing changes on local development environments.

Conclusion

We at Vitamin Software care about our customers' success. We strive to deliver secure, high-performing solutions that meet our customers' needs and empower them to move forward. Keeping data safe is our top priority and that is visible in every aspect of our work. We embed information security measures and best practices into everything we do, becoming trusted, reliable partners to companies from highly regulated industries.

Vitamin Software builds bridges: from problem to solution, from difficult to feasible, from impossible to outstanding.