SECURITY OVERVIEW

datasheet version 4.0.2

Vanilla

VANILLA FORUMS INC

Document Change History

4.0 Tim Gunter <tim@vanillaforums.com>
JUNE 2018
Updated network diagram, updated hosting, GDPR.

3.1 Tim Gunter <tim@vanillaforums.com>
APRIL 2016
Updated network diagram, added cluster diagram.

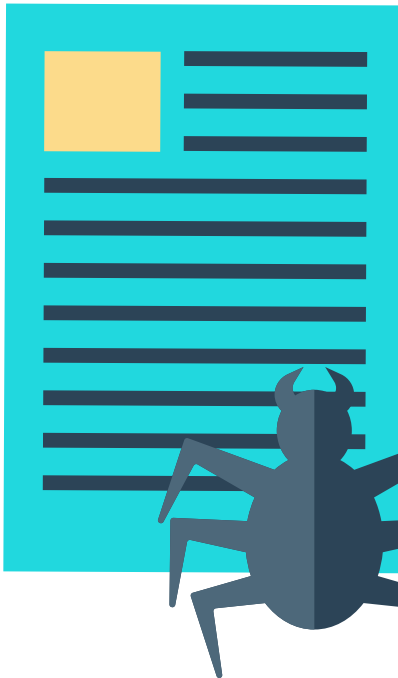
3.0 Tim Gunter <tim@vanillaforums.com>
AUGUST 2015
Updated to reflect new DDoS and Trust policies.

2.1 Tim Gunter <tim@vanillaforums.com>
DECEMBER 2014
Updated to clarify backup/restore SLA and IDS SLA.

2.0 Tim Gunter <tim@vanillaforums.com>
JUNE 2014
Updated to reflect new policies as of the deployment to RPC in Chicago.

1.1 Tim Gunter <tim@vanillaforums.com>
FEBRUARY 2013
Updated to reflect new policies as of internal security review.

1.0 Tim Gunter <tim@vanillaforums.com>
AUGUST 2012
Document created.



Security is a top concern for companies selecting 3rd party externally hosted software platforms that will contain customer information. Vanilla takes security very seriously and has adopted industry best practices to ensure that our customer's data stays safe.

Vanilla is committed to the security of our products from the ground up. Security is crucial to our process from product development to deployment, and all our products and services are tested rigorously before hitting production. In order to ensure compliance with our strict security standards, we conduct regular security audits and vulnerability testing on our products and our hosting environments

The following is a walkthrough of security and compliance policies in place at Vanilla Forums.

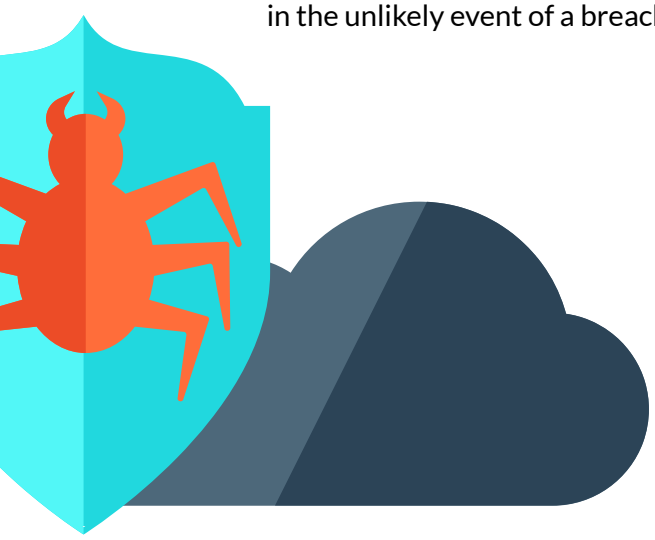
Table of Contents

Application Security

Security is a major consideration when designing, building, and supporting our application. From password encryption to the rendering of uploaded images, significant effort is put into outthinking malicious exploits.

Application security includes:

- **Granular permissions**, using Role Based Access Control (RBAC), to ensure that access to functionality is restricted and controlled. Our permission system aims to be extremely straightforward and easy to understand which has been shown to reduce the frequency of accidental misconfiguration.
- **Robust validation** of user generated content to prevent the insertion of malicious code. All input to the application is sanitized and validated prior to being considered actionable. All user interaction with the application is considered hostile until proven otherwise, on a request-by-request basis in order to prevent Access Control Failures (ACF).
- **Password hashing**, using industry standard multi-pass methodologies with blowfish for the block level cipher.
- **Transient Key cryptography**, which is used to generate single use numbers (or “nonces”) that must match up in order for form submissions to be valid.
- **Penetration testing** by leading security firms helps us to find things we’ve missed and respond to new vulnerabilities in real time.
- **Bug Bounty** campaign through HackerOne, where experienced white-hat hackers and exploiters attempt to defeat our security in exchange for rewards. We then patch the vulnerabilities they discover, making us more and more secure.
- **Logging and backups** allow us to investigate and restore data that may have been damaged in the unlikely event of a breach or loss.



Questions and Answers

	Application Stack
Development	PHP 7
Database Technology	Percona MySQL
Session Management	UserID in HMAC-signed cookie

	IO Validation
How does Vanilla receive input?	Input is provided by the end user through their web browser. Vanilla also supports an API that can accept calls from automated agents. Users are able to upload files if the file upload feature is enabled.
What kinds of files can users upload?	This is configurable, and we sanitize image uploads to eliminate malicious gif/jpg/png exploits. Other file types are uploaded and stored as-is. Files are not stored on application servers and cannot infect our network.
How does Vanilla determine the file type?	By file extension and mimetype inspection.
Can users generate arbitrary HTML?	Vanilla supports several markup formats, including BBCode, Markdown and WYSIWYG. There is no need to allow arbitrary HTML.
How does Vanilla mitigate XSS?	User input is aggressively sanitized by an intelligent mixed type input parser which removes active elements including scripts.
How does Vanilla mitigate XSRF?	Most URLs that have consequences are shielded by POSTs, and those that are not are protected by a dynamic transient key.
How is SQLi addressed?	Queries are generated by chained method calls against our data access layer abstraction. This layer aggressively sanitizes input and prevents premature query termination and tampering.

	Incident Response
How does Vanilla monitor customer forums?	Forums are monitored using Panopta to ensure that they are consistently returning expected response codes.
What happens if a forum goes down, or something else happens?	Vanilla has a status page at https://status.vanillaforums.com which is updated when something goes wrong. VIP customers are directly notified of serious outages that affect their SLA.
Are there other options?	Customers on higher tier plans have access to an emergency support number that is available 24/7.

Data Handling / Security

During the course of normal operations, some Vanilla Forums staff will have cause to interact with customer data from time to time.

- This data will be accessed only for the purposes of fulfilling Vanilla Forums' responsibilities as a hosting and service provider for the customer.
- When stored on our servers, customer data is protected by firewalls and access is limited to users with explicit authority to log in to those servers. These users are constrained to Operations staff only.
- Servers containing customer data are patched and updated regularly, automatically.
- When stored on employee computers, customer data resides on whole-disk encrypted drives to protect the data against unauthorized access in the event of loss or theft of those devices.
- Access to customer data will not be granted to third parties without the explicit consent of the customer, or at their specific direction.
- When stored on employee computers, customer data will be removed when it is no longer being used for its original purpose (data migration, usually).

Staff Security Policy

Vanilla's operations team and staff undergo security training and must abide by our security policies which are designed to ensure the protection of customer information. Our security policy covers:

- Password management & system access
- Building access
- Data handling
- Incident response / management
- Disaster recovery procedures
- Device security

Questions and Answers

	Data at Rest
What kind of data does Vanilla store?	Vanilla is a forum, so we store user records and user generated content. Some of it is access-restricted based on application RBAC ACLs. PII can be shielded from accidental access.
Can this data be encrypted at rest?	Yes. Vanilla can use Full Disk Encryption (FDE) on its database servers at higher plan levels.
How is FDE achieved?	Vanilla uses dm-crypt with Linux Unified Key Store to create an encrypted volume that contains the stored data.
How are passwords stored?	We hash all passwords using salted CRYPT_BLOWFISH before they are saved to the database.
Are any fields encrypted?	No. Our data needs to be searchable. When higher data security is required, we rely on Full Disk Encryption.
How is data and media decommissioned?	Virtual instances that house the data are destroyed.
Where is Vanilla's data stored?	Vanilla operates private cloud environments in both the US (Chicago) and Canada (Montreal).
Who has access to our data?	Vanilla Operations team members have access to database servers for maintenance and repair purposes. Access is carefully monitored and logged.

	Data in Transit
What kind of transit security does Vanilla use?	Forums on our network can be made available over HTTPS using TLS 1.0, 1.1 and 1.2, and a secure cipher.

Redundancy and Backups

Redundancy

The hosting infrastructure at Vanilla's hosting providers are designed with multiple redundancies for maximum uptime.

- We host in Tier 3+ data centers. These have redundant, concurrently maintainable UPS power subsystems with instantaneous failover, and routinely tested diesel backup generators with at least 72 hours of fuel, for ironclad power delivery.
- Our primary facility is extremely green, using air cooling-only in the winter and achieving a PUE of less than 1.15.
- Vanilla hosts in carrier-neutral data centers with multiple carriers for fast, reliable, redundant Internet connectivity, with automatic failover.
- Beyond the network edge, each critical system in the Vanilla architecture is set up in a redundant manner to eliminate single points of failure. This includes redundant load balancers, firewalls, switches, and routers.
- At the system layer, servers are deployed with redundant power supplies, redundant network cards, and redundant self repairing disk storage.
- At the database layer, regular backups are made and stored offsite in multiple redundant secure locations, on a daily basis.

Backups

Vanilla's backup system uses binary replication to copy database data on a daily basis. This method is fast, non-intrusive, and does not cause a performance penalty to the live site.

	Backups
Is data backed up regularly?	Yes. Incremental backups are run daily. Full backups are run each week as a basis for incremental backups. Backups are cycled on a 2 week basis.
Where is backup data stored?	We store compressed and encrypted backups in our hosting provider's cloud based redundant file storage service.
How can data be restored?	In the case of data loss due to hardware malfunctions or failures (not user error), the restoration SLA is 24 hours and there is no cost. In the case of user error (accidental deletion of data by users, moderators or admins), there is no SLA and restoration hours are billable.

Host Security

Vanilla is hosted on Openstack powered private clouds, using virtual machines within logical web clusters. This allows us to allocate resources as and when they are needed, ensuring high availability and consistently high performance.

Questions and Answers

	Instance Configuration
What operating systems does Vanilla use?	Vanilla is hosted on Ubuntu at the Virtual Machine level.
Are VMs individually firewalled?	Yes. Each VM has a stateful firewall installed which is customized to its workload.
Are unnecessary services and ports disabled?	Yes. Each VM has a specific workload according to its class, and all other ports and processes are locked down.
Are any services allowed to use default credentials?	No. All services on the Vanilla network have been customized and access credentials have been changed.
How is patching handled?	Proprietary automation software ensures that security patches are applied automatically on a daily basis

	Access Control
How are VMs managed?	We use public/private key based SSH access only, plaintext access is disabled. Our servers use non-standard SSH ports.
What kind of authentication is used?	We use local OS accounts that are managed through an active centralized configuration management system that uses Role Based Access Control rules to grant access.
How is access restricted?	Our environment is protected by a perimeter VPN and our internal servers are granted private, non internet routable IPs.

Network Security

Our hosting environment's network is designed from the top down to be secure:

- Protected by Openstack's security layer.
- Vanilla uses discrete Octavia load balancers for each cluster, with automatic failover.
- Origin certificates are securely stored in the Barbican keystore.
- No direct access to workload servers from the internet.
- Server-to-server API communications are secured using SSL.
- Daily vulnerability scanning by a 3rd party service.

DDoS Mitigation

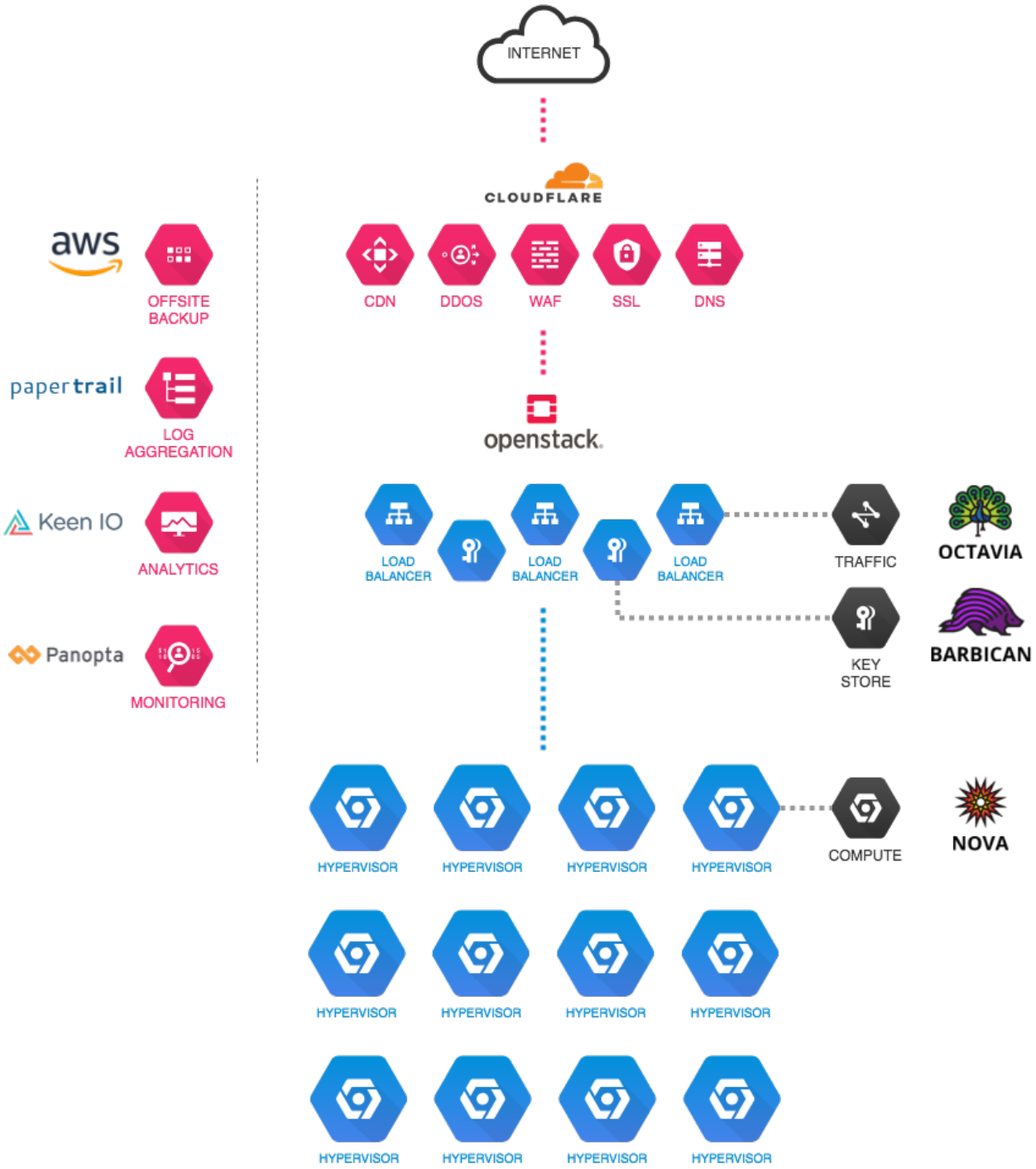
Vanilla is protected by Cloudflare, which uses automated traffic scrubbing tools that monitor incoming traffic and filter out malicious volumetric attacks. This system allows us to withstand the largest attacks on the internet, while continuing to service legitimate requests without interruption.

Questions and Answers

	Cloud Instances
What kind of cloud does Vanilla use?	Vanilla operates private clouds running on Openstack.
How are instances networked?	We use a flat network layout with firewalling and specific ACLs to segregate traffic and access.
Does Vanilla have monitoring, alerting, and auditing?	Yes. We have active monitoring systems connected to distributed alerting tools and all our logs are aggregated and searchable.
Are VMs individually firewalled?	Yes. Each VM has a stateful software firewall installed which is customized to its workload. Repeated failed SSH access results in throttling.
Does Vanilla use IDS (Intrusion Detection)?	Our hosting partner monitors our edge network and devices for intrusion.
What happens if an intrusion is detected?	Customers are notified within 24 hours of Vanilla's detection of a network intrusion. Upon detection, Vanilla will work with its upstream hosting provider to assess the extent of the intrusion and determine the scope of data theft, if any.

Private Cloud

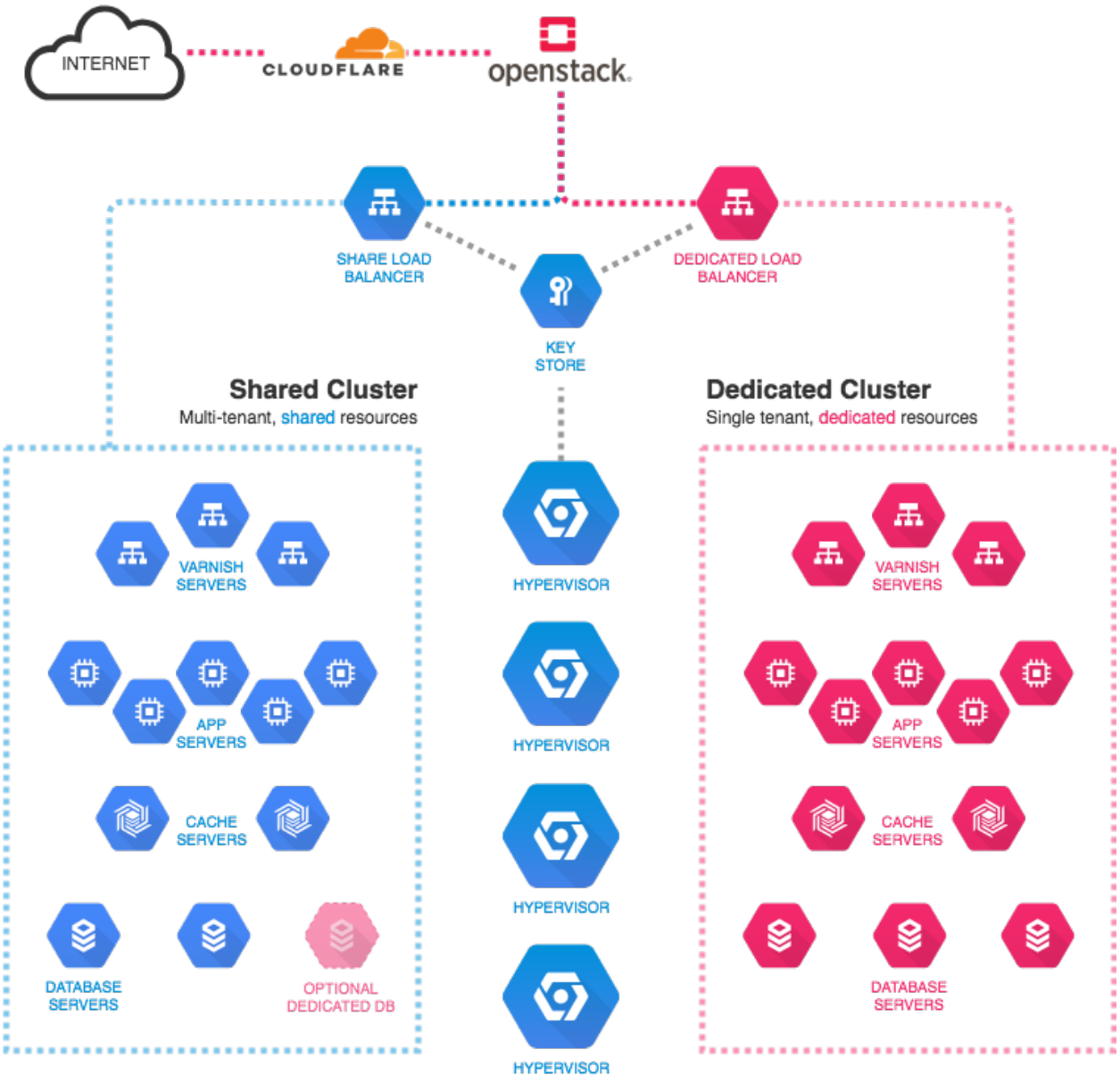
Vanilla is hosted in a Private Cloud which is fully dedicated to Vanilla's use. Customers are deployed to Virtual Machines within this Private Cloud.



Clustered Virtual Layer

Each Vanilla forum is hosted on one of our purpose-built cluster. Each cluster is comprised of a number of virtual machines that work together to deliver page requests to end users.

The following diagram outlines the high level layout of a cluster, as well as illuminating the difference between a dedicated “VIP” cluster and a shared cluster.



Physical Security

Vanilla's application is hosted in SSAE 16/ISAE 3204 Type II (SOC1 or SOC2) compliant facilities that offer world class network, physical and environmental security:

- 24/7 security personnel and biometric security to access physical servers
- Access limited to only authorized personnel and on a needs basis
- Personnel are security certified and background checked
- Redundant bandwidth providers, UPS, HVAC, etc.
- Redundant network providers

SSAE 16 / ISAE 3204
TYPE II

AICPA Service Organization Control Reports
AICPA
SOC
aicpa.org/soc
Formerly SAS 70 Reports

Questions and Answers

	Physical Access
Who has access to physical hosts?	Only our hosting partner's technical and operations staff have physical host access.

Compliance

- Vanilla data centers are SSAE16/ISAE 3204 Type II (SOC1 or SOC2) compliant.
- Vanilla has EU Model Clauses to bridge the gap between Safe Harbor and Privacy Shield.
- Vanilla maintains Data Processing Addenda with its suppliers in order to ensure EU GDPR compliance.
- Vanilla conducts annual security vulnerability and penetration testing using independent third party auditors.

EU Model Clauses

During the interim period between the dissolution of the Safe Harbour agreement and the establishment of Privacy Shield, Vanilla has executed model clauses with its US-based hosting providers to ensure that data is handled securely and in accordance with EU privacy standards.

PIPEDA

Vanilla is a Canadian company. We are bound by the Canadian privacy and information law known as PIPEDA (**Personal Information Protection and Electronic Documents Act**).

PIPEDA is recognized by the EU as being compatible with EU laws, and therefore the transfer of data from an EU to a Canadian company is legal in Europe. Read more **here**.

Audit Trails

Vanilla software contains comprehensive auditing features that allow site administrators to monitor administrative actions taken by staff. In the event of a security breach, this can be used to troubleshoot and identify the source of the breach. Administrative auditing also simplifies the resolution of moderator disputes, allowing administrators to review moderator behaviour and develop better workflow and practises.