VineCode

VINE CODE LIMITED SECURITY POLICY

Vine Code uses Amazon Web Services (AWS) to deliver a scalable cloud computing platform with high availability and dependability. We use AWS services to help protect the confidentiality, integrity, and security of our customers' systems and data as this is of the utmost importance to us, as is maintaining customer trust and confidence. Vine Code is also PCI/DSS Level 2 compliant and maintains the highest standards of best practice with regards to security.

Network Access & Security

Network access to the devices used to provide the Services is facilitated through named user accounts protected by a VPN accessible by username, password and two factor authentication devices. Personnel are issued with VPN user accounts upon commencement of their employment and successful background screening. VPN user accounts are terminated when personnel leave Vine Code Limited.

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services.

Vine Code devices are tracked, password protected and encrypted with passwords changed a minimum of every 90 days. Access to sensitive services is by two-factor authentication whenever possible. Access points to AWS are via secure VPN and secure HTTP access (HTTPS), which allows us to establish a secure communication session with our storage or compute instances within AWS.

Network Monitoring & Protection

Vine Code utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. Our monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts.

Secure by Design

Vine Code's development process follows secure software development best practices, which include security design reviews, threat and risk assessment. Code analysis tools are run as a part of the standard build process, and all deployed software undergoes recurring penetration testing. Our security risk assessment reviews begin during the design phase and the engagement lasts through launch to ongoing operations.

Vine Code applies a systematic approach to managing change so that changes to customer-impacting services are thoroughly reviewed, tested, approved, and well-communicated. The Vine Code change management process is designed to avoid unintended service disruptions and to maintain the integrity of service to the customer. Routine, emergency, and configuration changes to existing Vine Code infrastructure are authorised, logged, tested, approved, and documented in accordance with industry norms for similar systems.

Physical Security

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Personnel Security

Vine Code has established procedures to delineate the minimum standards for logical access to our software platform and infrastructure. Where permitted by law Vine Code conducts background checks as part of pre employment screening practices for employees and commensurate with the employee’s position and level of access. The procedures also identify functional responsibilities for the administration of logical access and security.

To help ensure that only authorized users and processes access our system services, we use several types of credentials for authentication. These include passwords, cryptographic keys, digital signatures, multi-factor authentication and certificates.

Reports of and Response to Security Breach

Vine Code Limited will immediately report to you any unauthorised access or release of your information of which we become aware. Upon request, we will promptly provide to you all information and documentation that we have available to us in connection with any such event.

Business Continuity

Vine Code’s infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. We have designed our systems to tolerate system or hardware failures with minimal customer impact.

Reviewed Feb 2025
Vine Code Limited, Registered Office: 80 West View, Barlby Road, Selby YO8 5BD.
Email: privacy@vinecode.uk