INFORMATION SECURITY POLICY

Codenvy has a security program designed to provide high quality services for our customers and to protect intellectual assets. The objective of this document is to address questions that prospective and existing customers may have regarding our security program.

Hosting facilities used by Codenvy maintain SAS70 compliance for physically secure environments. Codenvy integrates with services providers that maintain PCI merchant level certification for any credit card or financial data management.

Codenvy staff maintains security by internal and external monitoring of critical systems, in addition to continuous threat and vulnerability auditing. The following controls are in place to ensure customer and corporate information remains protected.

Questions? We welcome any questions, comments or suggestions you may have about this Information Security Policy or any other material on Codenvy. Please send your questions, comments or suggestions to info@codenvy.com. PLEASE DO NOT SEND ANY SENSITIVE INFORMATION TO US VIA UNENCRYPTED EMAIL.

Effective Date: February 13, 2013

Network Security

- Access Control via Network Segmentation, Firewalls, and VLANs
- Network Intrusion Detection
- Regular audits and physical security checks
- Disabling of commonly weak protocols and services (ex. telnet, FTP, r* commands)

Application Security

- Secure development cycle incorporating multiple test/staging environments
- Anti-DDoS measures to ensure application uptime

Data Protection

- Encryption via Secure Sockets Layer (SSL/TLS) for data in transit
- Database Encryption (Hashing) for passwords

Physical Security

- No sensitive data at the office (no servers)
- Servers with sensitive data hosted in Amazon AWS data centers - https://aws.amazon.com/privacy/
- Corporate data on Google App - https://www.google.com/policies/privacy/
- Staff are trained to counter attempts of illegal capture of physical data carriers

Through these and other measures, Codenvy's staff strives to maintain a strong security posture. The Codenvy Information Security Team works with all business units to ensure that they are all properly educated on best practices and that approved processes are being followed. In addition, our technology operations staff maintains 24/7/365 on-call coverage.

Codenvy takes information security and the protection of our customer's data very seriously. Our staff works to discover and remediate security issues as quickly and thoroughly as possible. A large part of running a world-class Software as a Service (SaaS) platform requires that any information security threat be dealt with swiftly. To this end, we are always looking to advance and improve our technology and process so that Codenvy Corporation and its customers can be secure.