Cytobank Security Overview

Cytobank is committed to protecting the confidentiality, integrity and availability of our customers' information.

The Cytobank platform has been designed to include multiple layers of security to mitigate security threats and to meet the expectations and regulatory requirements of our customers.

Physical and Environmental Security

Cytobank operates its systems in high-security data centers that meet SSAE-16 and ISAE 3402 standards. Cytobank data centers are designed to minimize the impact of disruptions to operations and are physically secured to prevent theft, tampering, and damage. Data centers include perimeter security, redundant power, climate control, fire suppression, and redundant network connectivity.

Logical and Network Security

Cytobank employs best practices in security techniques, server hardening, firewalls, network monitoring, intrusion detection, data isolation, and session control to protect customer systems and information. Transmissions to the Cytobank servers are encrypted using SSL/TLS connections.

Development and Maintenance

Cytobank has a robust software development lifecycle that includes secure software development practices, secure design and coding, source-code control, and quality testing. Cytobank uses an automated deployment platform that facilitates platform updates and efficient securi.ty patching.

Security Training and Awareness

All Cytobank personnel receive security awareness training and education at hire and annually thereafter. Employees are trained on Cytobank security policies, procedures, and threats and instructed to immediately report any suspected security issue or incident.

Disaster Recovery and Business Continuity

Cytobank has procedures and systems in place to back up data to an offsite location on a daily basis. Cytobank also has automated monitoring tools to detect and respond to disruptions, capacity issues, and system failures. Cytobank services are designed to deliver reliability, availability, and performance with a guaranteed 99% uptime, financially-backed service level agreement (SLA).

Network Monitoring and Incident Response

Cytobank operations uses centralized log monitoring tools and systems to detect failures, anomalous activity and incursions to the Cytobank network, resources, and computer hosts. Cytobank has incident response procedures in place to investigate, isolate, disable, or shut down suspicious activity when detected.

Authentication and Access

Cytobank requires authorized credentials for access to its network and services, has separated its production network from the corporate network, and has implemented administrative and technical controls to authenticate individuals, ensure strong passwords, one-way password encryption, and periodic review of access roles.

Data Retention and Return

Cytobank retains and protects customer data for the duration of the service agreement. Upon request Cytobank will assist in returning data to the customer in industry standard format and remove remnants of the information. Cytobank policies ensure that remaining data is overwritten and physical media is degaussed, shredded, or otherwise destroyed.

Please contact us at sales@cytobank.org for more information and a copy of our detailed Security Whitepaper.