Overview of Security Systems and Processes

July 2018

Cytobank provides a cloud-based platform for the management, sharing, and analysis of single cell data. The Cytobank platform includes data visualization, advanced algorithms, and collaboration tools that enable communication between clinical researchers, scientists, and informaticians.

Cytobank is committed to protecting the confidentiality, integrity and availability of our customers' information. The Cytobank platform includes multiple layers of security to mitigate security threats and meet the expectations, regulatory, and trust requirements of our customers.

This document describes our security practices, operational processes, and security technology that protects the information you entrust to us.

Table of Contents

Introduction

Cytobank's information security governance is aligned with the International Organization for Standardization (ISO) 27001, the Federal Information Security Management Act (FISMA), Federal Information Processing Standards Publications FIPS 199/200, the National Institute of Standards and Technology (NIST) Special Publications 800 Series.

Based on these frameworks, Cytobank has developed and implemented an information technology security and privacy program that includes a set of written policies, procedures, and security controls designed to ensure the privacy and security of information. Cytobank monitors its security program and controls on a continuous basis and is committed to ongoing security improvement.

Cytobank has categorized the information it manages and performs periodic assessments of vulnerabilities, threats, and risks to operations, systems, and data. Cytobank actively monitors reports of new security issues and threats and has implemented reasonable and appropriate physical, administrative, and technical safeguards to mitigate these security risks to acceptable levels. Development of the Cytobank platform and processes embody "privacy-by-design" and "security-by-design" principles for the protection of personal information.

Cytobank uses a combination of people, process, and technology, as well as a multi-layered defense-in-depth strategy that ensures that information assets are consistently protected, configured, maintained, and monitored. Cytobank trains its staff to respond to potential incidents and take steps to assess, contain, investigate, and remediate security issues in a timely fashion.

Cytobank operates its platform and systems in high-security data centers that meet SOC 2 Trust Services Criteria, ISO 27001 Security Management Controls, and ISO 27018 Personal Data Protection codes of practice for security, availability, processing integrity, confidentiality, and privacy.

Physical and Environmental Security

Physical and environmental systems at Cytobank data centers are designed to minimize the impact of disruptions to operations and are physically secured to prevent theft, tampering, and damage.

> **Physical Security** – Physical access to data centers is controlled both at the perimeter and at building ingress points using video surveillance, two-factor access control systems, and other electronic systems. Data centers are staffed 24/7/365 by trained

security guards, access is authorized on a least privileged basis, and all visitors are signed in and escorted by authorized staff. All physical access to data centers is logged and audited routinely.

Redundant Power – Electrical power systems in the data center are designed to be redundant. Uninterruptable power supplies (UPS) and generators provide back-up power in the event of an electrical failure.

Climate Control – Redundant air cooling systems ensure a constant operating temperature is maintained for servers and other hardware. Personnel and systems monitor and control temperature and humidity to appropriate levels.

Fire Suppression – Automated fire detection and protection equipment has been installed to reduce risk. The fired detection system uses smoke detection sensors and wet-pipe, pre-action, or gaseous suppression systems to safely extinguish fires.

Resilient Network – Internet connectivity and bandwidth is provided by multiple providers over diverse fiber circuits. The data center network includes redundant components to provide continued access in the event of network equipment outage.

Logical Security

Cytobank uses security architecture techniques, data isolation, server hardening, access control lists, network monitoring, and intrusion detection and prevention systems to protect customer systems and information.

Data Isolation – The Cytobank platform is designed to host multiple customers in a secure manner using an appropriate combination of physical server separation, instance isolation using virtual resources allocated per customer, private subnets, and data isolation techniques to partition access and reduce the threat of compromise by other customers or outsiders.

Network Security – Cytobank uses firewalls with Stateful Packet Inspection (SPI) that are configured in a default deny mode. Only ports required for inbound traffic are opened. Traffic is restricted by protocol, by service port, and by source when required. Cytobank also uses private network segments, external gateways, security group rules, and Access Control Lists (ACLs) to provide strict control over inbound and outbound network traffic.

Transmission Security – External communication to the Cytobank platform and application servers only allow connections using Hypertext Transfer Protocol Secure (HTTPS). Cytobank uses end-to-end traffic encryption and SSL-terminating load balancers to ensure session traffic is encrypted using Transport Layer Security (TLS). A 2048-bit SSL certificate is used for secure communications between the user's web-browser and the Cytobank servers.

Intrusion Detection and Prevention – Cytobank has implemented log monitoring and alerting tools to detect failures, anomalous activity, and incursions to the network or to computer hosts on the network. Cytobank systems blocks incoming traffic if multiple invalid or malicious access attempts are detected.

Malware Prevention – Cytobank uses industry standard anti-virus systems to detect and eliminate viruses on production servers as well as on the laptops and desktops of its employees.

Vulnerability Management – Cytobank uses automated vulnerability scanning tools and software testing tools on a regular basis to inform its risk assessment and prioritize mitigation activities of servers and software. Additionally, Cytobank performs third-party penetration tests to find security vulnerabilities that could be exploited. Cytobank systematically addresses any issues discovered in these assessments.

Session Control – Cytobank web-based applications that contain confidential information issue a session-specific key and cookie that expire after a certain period of inactivity set by the administrator after which the user must re-authenticate.

Development and Maintenance

Cytobank's software development lifecycle and system operations include secure software development practices, secure design and coding, source-code control, and configuration management.

Risk Assessment – Cytobank maintains a list of all computer systems and the data and customer associated with each system. Cytobank identifies and categorizes threats and vulnerabilities to the loss, modification, or theft of confidential information, estimates the frequency of the potential threats, and the likelihood of a threat occurring.

Change Management – Cytobank applies a systematic approach to managing change and uses commercial source control systems, version numbers, and branching

strategies to maintain and track revisions of the software and platform elements. Cytobank uses a robust defect tracking system to track issues identified in production software and systems.

Secure Coding – Cytobank performs code review and security testing of the applications of applications it develops. Cytobank secure software coding principles include but are not limited to: input validation, output encoding, session management, error handling, logging, access control, encryption, database security, and protection from cross-site scripting attacks.

Testing – Cytobank performs multi-layered threat modeling, security testing, and quality assurance of its systems including peer review, unit tests, automated tests, manual tests, security tests, and performance tests.

Deployment – Cytobank manages all source-code in an industry-standard source-control repository. Cytobank versions its software changes and pushes them to production using a staged deployment strategy. Cytobank prohibits changes to production until a proposed change has been tested and approved through the development review and quality assurance process.

Security Training

All Cytobank personnel receive training, education, and awareness training at hire and annually thereafter about Cytobank security policies, procedures, and threats.

Training – Cytobank personnel receive Security Awareness training to understand the potential risks to sensitive information as well as Social Engineering Awareness training to protect from human hacking techniques such as phishing.

Incident Reporting – All personnel are trained to immediately report any suspected security issue, loss of device, suspicious e-mail, or security incident to the Security Officer or operations team.

Disaster Recovery and Business Continuity

Cytobank has procedures and systems in place to respond to and restore damage to computer equipment and data loss within a short period of time.

Data Backups – Cytobank customer data are backed up on a daily basis. Automated backups and data snapshots are encrypted using Advanced Encryption Standard

(AES256) and stored and retained at a secondary data center. The success of backup operations is monitored by automated systems and Cytobank personnel.

Availability – Cytobank uses automated monitoring tools to detect and respond to disruptions, capacity issues, and failures to systems. Cytobank uses auto-scaling techniques to scale capacity up and down to maintain performance. Cytobank has a systematic written Disaster Recovery (DR) plan to respond to disasters, restore data, and resume operations with an established Recovery Time Objective (RTO).

Business Continuity – Cytobank maintains data centers in multiple locations in the United States, Europe, and Asia. In the event of a regional disaster or complete data center failure, Cytobank has processes to re-establish services and remote operations using an alternate data center location.

Storage Redundancy – Cytobank stores all data on storage systems that use redundancy technology such as RAID, checksums, and/or object duplication to ensure the high durability of data and prevent corruption of stored data.

Service Level Commitment – Cytobank services are designed to deliver reliability, availability, and performance with a guaranteed 99% uptime, financially backed service level agreement (SLA).

Network Monitoring

Cytobank operations uses monitoring tools and systems to detect failures, anomalous activity, and incursions to the Cytobank network, resources, and computer hosts.

Event Logging – Cytobank systems are instrumented to log key security and operational metrics and events. Log sources are synchronized with a centralized time-server. Authentication events, web access, security events, resource modification, operating system events, and errors are recorded. Logs include information such as the time, date, user identifier, originating IP address, and other device information.

Log Management – Cytobank employs a centralized log management and alerting system to record, investigate, and retain log records and detect anomalous activity. System logs are encrypted in transit and at rest. Cytobank retains backups and archives of log files in order to facilitate investigation and troubleshooting.

Incident Response – Cytobank has procedures in place for personnel to take steps to investigate, isolate, disable, or shut down suspicious activity. Cytobank security

personnel conduct and document investigations in collaboration with external security advisors, law enforcement, and legal counsel. Cytobank takes steps to mitigate security incidents or information breaches to prevent further use or disclosure of the information.

Communication – Cytobank is committed to notifying its customers in a timely fashion regarding security incidents or improper use or disclosure that impact a customer's confidential information. Cytobank has multiple methods for internal communication to employees and external communication to its customers, service providers, and partners.

Authentication and Access

Cytobank requires authorized credentials for access to its network and services, has separated its production network from corporate and development networks, and has implemented administrative and technical controls to authenticate individuals and review access.

User Security – Each user of the Cytobank system receives a unique login and role based access rights managed by their site administrator. Users invited to the Cytobank platform are able to set their password upon registration.

Password Policy – The Cytobank software platform allows configuration of password policies including password length. Users will be challenged with a captcha after multiple failed login attempts. Users who have forgotten a password are sent a unique one-time password reset token with a fixed expiration time. The platform supports Single Sign On (SSO) for Enterprise Users.

Password Security – Passwords are encrypted using an industry standard FIPS compliant one-way hash function. The one-way hash function output cannot be reworked to discover the original password. In addition, passwords are concatenated with a random salt to ensure that identical passwords are encrypted uniquely.

Administrative Security – All Cytobank personnel are assigned a unique user identifier and access to applications, systems, and servers. Access is limited by employee role, and access to customer information for troubleshooting purposes is on an as-needed and minimum necessary basis. Cytobank has policies in place for Acceptable Use.

Administrative Access – Access to customer servers is only by approved Cytobank personnel and is performed using Secure Shell (SSHv2). Administrator access requires

Multi-Factor Authentication (MFA) in addition to a password to gain access. All such administrative access is through a secure bastion host and is logged and monitored. Access to sensitive information and confidential information is restricted and account escalation is required to perform certain administrative functions and changes.

Single Sign-On – Cytobank supports Single Sign-On (SSO) using Security Assertion Markup Language, SAML 2.0 and partner integrations with leading identity management solutions. SSO allows businesses to seamlessly integrate Cytobank into their existing authentication workflow.

Account Termination, Review and Audit – Cytobank has processes in place to ensure that access is immediately revoked when personnel no longer work for the company. Administrative access to customer systems is reviewed and audited on a periodic basis.

Data Retention

Cytobank retains and protects customer data for the duration of the service agreement. Upon request and for a fee, Cytobank will assist in returning data to the customer. Cytobank supports the requests of customers to have any "Personal Information," defined as user contact information and pseudonymized data about individuals, removed from its systems.

Data Removal – Authorized customer users are able to mark data as deleted from the Cytobank system using the user interface. Customers may request such data to be permanently removed.

Data Return – If a customer wishes to terminate their Cytobank services, Cytobank will, upon request and for a fee, return the data in an industry standard format and remove the data permanently as described above. Cytobank will facilitate the deletion or return of Personal Information at the end of the service contract except for necessary record-keeping purposes and as required or authorized by law.

Disposal – Cytobank data center operations policies ensure that physical media containing client data is overwritten, degaussed, and physically destroyed, or otherwise rendered un-accessible before the media is removed for disposal in accordance with NIST 800-88 ("Guidelines for Media Sanitation") and industry-standard practices.

Standards and Compliance

EU General Data Protection Regulations – GDPR

The General Data Protection Regulation (GDPR) (EU) 2016/679 aims to protect European citizens' personal data, ensure the lawful processing of data, and safeguard data subjects' data privacy rights and freedoms. The processing of data by Cytobank may include "Personal Information" including user contact information and pseudonymized data about individuals who reside the European Union (EU) and European Economic Area (EEA). As a data processor, Cytobank has implemented policies and procedures that meet the required principles for personal data protection including lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, integrity, and confidentiality.

Cytobank has implemented appropriate administrative, technical, and continuous monitoring safeguards to ensure the security and protection of Personal Information. Cytobank enters into confidentiality and data protection agreements with its sub-processors that include standard contractual clauses for data transfers to the United States.

US Government – FISMA

The United States Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.) defines a comprehensive framework to protect government information, operations, and assets against natural and man-made threats. In accordance with FISMA, the National Institute of Standards and Technology (NIST) has developed standards, guidelines, associated methods, techniques and guidelines for providing adequate information security for organizations.

Federal agencies, departments, and their contractors are required to implement the FISMA framework and meet the requirements and controls specified in Federal Information Processing Standards (FIPS) 199, FIPS 200, and NIST Special Publication 800-53. To the extent that Cytobank may serve as a contractor to government entities, Cytobank has categorized its systems, documented its security processes, and has implemented the set of controls necessary and appropriate for the FISMA Moderate level.

Cytobank policies and security controls and monitoring cover the areas of Information System Inventory, Risk Assessment, Security Planning, Configuration Management, System and Communication Protection, Personnel Security, Awareness and Training, Physical and Environmental Protection, Media Protection, Contingency Planning, Maintenance, System and Information Integrity, Incident Response, Identification and Authentication, Access Control, Accountability and Audit.