Overview of Security Systems and Processes

March 2021

protocols.io platform is a cloud-based platform for developing and publishing science protocols, methods and checklists.

The protocols.io platform provides online tools that enable collaborative editing of protocols and communication between researchers.

protocols.io is committed to protecting the confidentiality, integrity and availability of our customers' information. The protocols.io platform has been designed to include multiple layers of security to mitigate security threats and meet the expectations and regulatory 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

protocols.io's information security governance is aligned with the International Organization for Standardization (ISO) 27002, 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, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Based on these frameworks, protocols.io 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. protocols.io monitors its security program and controls on a continuous basis and is committed to ongoing security improvement.

protocols.io has categorized the information it manages as part of its periodic assessments of vulnerabilities, threats, and risks to operations, systems, and data. protocols.io actively monitors for 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.

protocols.io 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. protocols.io trains its staff to respond to potential incidents and take steps to assess, contain, investigate, and remediate security issues in a timely fashion.

Physical and Environmental Security

protocols.io operates its systems in high-security data centers that meet SSAE-18 and ISAE 3402 standards. Environmental systems at the 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 the data center is controlled both at the perimeter and at multiple access points using video surveillance, multi-factor access control systems, biometrics, 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 require escort.
>
> Redundant Power – Electrical power systems in the data center are designed to be redundant. Uninterruptable power supplies (UPS) and diesel 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 protection equipment detects smoke and suppression systems are designed to safely extinguish fires. Fire extinguishers are located throughout data centers for human intervention.

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

Logical Security

protocols.io uses security architecture techniques, data isolation, server hardening, network monitoring and intrusion detection and prevention systems to protect customer systems and information.

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

Network Security – Firewalls with Stateful Packet Inspection (SPI) are configured in a default deny mode. DDoS protection and scalable load balancers operate at the edge. Segmented front-end and back-end networks separate web services from database and file data. Only ports required for inbound traffic are opened. Traffic is restricted by protocol, by service port, and by source when required.

Transmission Security – Communication to the platform and application servers only allow connections using Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSHv2). Session traffic is encrypted using Secure Sockets Layer (SSL v3) or Transport Layer Security (TLS v1.2+). Upon logging in to protocols.io, users will see a commercial 2048-bit SSL certificate issued by CA GeoTrust for secure communications between their web-browser and the protocols.io servers.

Intrusion Detection and Prevention – Log monitoring tools detect failures, anomalous activity, and incursions to the network or to computer hosts on the network. protocols.io systems block the IP addresses of incoming traffic if they attempt multiple invalid or malicious access attempts.

Endpoint Protection – protocols.io 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. All staff laptops are encrypted with AES full-diisk encryption.

Vulnerability Management – protocols.io uses automated vulnerability scanning tools and software testing tools that detect known common vulnerabilities and exploits (CVEs) on a regular basis to inform its risk assessment and prioritize mitigation activities of servers and software.

Session Control – protocols.io 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

protocols.io's software development lifecycle includes secure software development practices, secure design and coding, source-code control, and configuration management.

Risk Assessment – protocols.io maintains a list of all computer systems and the data and customer associated with each system. protocols.io 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 – protocols.io 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. protocols.io uses a robust defect tracking system to track issues identified in production software and systems.

Secure Coding – protocols.io performs code review and security testing of the applications it develops. protocols.io 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 – protocols.io performs multi-layered threat modeling, security testing, and quality assurance of its systems including peer review, unit tests, automated tests, manual tests, static and dynamic security tests, and performance tests.

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

Security Training

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

Training – protocols.io personnel receive Security Awareness training to understand the potential risks to sensitive information, protected health information training, 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

protocols.io 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 – protocols.io customer data is backed up on a daily basis using snapshot technology. Backups are encrypted using Advanced Encryption Standard (AES-256) and stored and retained at a secondary data center. The success of backup operations is monitored daily by protocols.io personnel.

Availability – protocols.io uses automated monitoring tools to detect and respond to disruptions, capacity issues, and failures to systems. protocols.io has a systematic written disaster recovery (DR) plan to respond to such disasters, restore data, and resume operations with an established Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

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

Storage Redundancy – protocols.io 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 – protocols.io services are designed to deliver reliability, availability, and performance with a guaranteed 99% uptime, financially backed service level agreement (SLA).

Network Monitoring

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

Event Logging – protocols.io systems are instrumented to log key operational metrics and events. Log sources are synchronized with a centralized time-server. Authentication events, web access, security events, 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 – protocols.io employs a centralized log management and alerting system to record, investigate, and retain log records and detect anomalous activity. Log data is encrypted in transit and at rest. protocols.io retains backups and archives of log files in order to facilitate investigation and troubleshooting.

Incident Response – protocols.io has procedures in place for personnel to take steps to investigate, isolate, disable, or shut down suspicious activity. protocols.io security personnel conduct and document investigations in collaboration with external security advisors, law enforcement, and legal counsel. protocols.io takes steps to mitigate security incidents or information breaches to prevent further use or disclosure of the information.

Communication – protocols.io 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. protocols.io has multiple methods for internal communication to employees and external communication to its customers, service providers, and partners.

Authentication and Access

protocols.io 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 and review access.

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

Password Policy – The protocols.io software platform allows configuration of password policies including password length, complexity. Users who have forgotten a password are sent a unique one-time password reset token with a fixed expiration time.

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 the original password. In addition passwords are concatenated with a random salt to ensure that identical passwords will be encrypted differently.

Administrative Security – All protocols.io personnel are also 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. protocols.io has policies in place for Acceptable Use.

Administrative Access – Access to customer servers is only by approved protocols.io personnel and is performed using Secure Shell (SSHv2) and multi-factor authentication (MFA). Access to sensitive information and confidential information is restricted and account escalation is required for administrators to perform certain administrative functions and changes. protocols.io has processes in place to ensure that access is immediately revoked when personnel no longer work for the company.

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

Account Review and Audit – Administrative access to customer systems is reviewed and audited on a periodic basis.

Data Retention

protocols.io retains and protects customer data for the duration of the service agreement. Upon request protocols.io will assist in returning data to the customer and remove remnants of the information.

Data Removal – Authorized customer users are able to mark data as deleted from the protocols.io system using the user interface. Customers may request such data to be permanently removed upon request and have the data overwritten with random patterns that render the data unretrievable.

Data Return – If a customer wishes to terminate their protocols.io services, protocols.io will, upon request, return the data in an industry standard format and remove the data permanently as described above.

Disposal – protocols.io data center operations policies ensure that physical media containing client data is overwritten, degaussed, shredded, or otherwise rendered un-accessible before the media is removed for disposal.

Organizational Controls

Written Contracts – protocols.io maintains written Business Associate Agreements with its vendors who manage PHI that require they implement appropriate safeguards and provide notification of security incidents and information breach in a timely fashion.

Vendor Assessments – protocols.io qualifies the vendors it uses to manage PHI to ensure their practices have an appropriate level of administrative, physical, and technical safeguards and they have necessary security management and training processes.

Standards and Compliance

HIPAA

protocols.io is a "Business Associate" and is subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA" Public Law 104-191) which establishes national standards for electronic health care transactions and code sets, unique health identifiers, and security.

Pursuant to HIPAA, protocols.io is required to comply with the Department of Health and Human Services (HHS) regulations, 45 CFR Parts 160 and 164, including the "Privacy Rule", the "Security Rule", the "Breach Notification Rule" and the "Enforcement Rule".

protocols.io must ensure the privacy, confidentiality, integrity, and access to the Protected Health Information (PHI) it receives, generates, maintains, and transmits. protocols.io has also implemented procedures to ensure proper de-identification of information that is used for research. protocols.io must ensure its "business associates," as defined under HIPAA, meet certain requirements to ensure the security and privacy of PHI they receive, manage, maintain, or transmit on protocols.io's behalf.

ISO 27001/27002

ISO 27001 was established by the International Organization for Standardization. It is an internationally-recognized management standard that describes best-practices and a holistic approach for an "Information Security Management System (ISMS)".

The ISO 27001 standard requires management commitment to security and provides a model for "establishing, implementing, operating, monitoring, reviewing, maintaining and improving" an ISMS including:

- Systematic evaluation of the risks to the security of its information systems
- Design and implementation of a comprehensive set of security controls to address those risks; and
- Management processes for planning, implementing, monitoring and improving those controls.

ISO 27001 is supported by control objectives and definitions defined in ISO 27002.