Girls Who Code Security Whitepaper

Protecting data privacy and security is a top priority for Girls Who Code. We regularly evaluate our policies and practices to improve security and to keep up with the latest practices in the security industry.

This document is designed to provide a high-level overview of the information security program at Girls Who Code. While this document is written for technology experts who often play a key role in assessing our policies, we recognize that data security is just as important to families, teachers, and students as it is to school officials.

The scope of this document includes the services provided by the platforms managed directly by Girls Who Code: **Girls Who Code Clubs HQ**, **Girls Who Code HQ**, and the internal data warehouse system used for business analytics. These will be collectively referred to as "Services" throughout this document. Capitalized terms not defined in this document, such as "**Student Data**," are defined **here**.

I. Audits and Certifications

The following security-related audits and certifications are applicable to the Services, as described below.

Overall, the security program is built on the foundation of the **NIST Cybersecurity Framework**, a widely adopted and leading framework for organizing and measuring security programs. This overarching framework is complemented by various privacy regulations, modern engineering practices, and a continuous push for innovative security approaches to data and systems.

Additionally, the Services undergo security assessments by internal personnel and third parties, which include annual penetration tests and application security assessments (BSIMM), on at least an annual basis.

As further described in our **Third-Party Service Providers Chart**, and below, Girls Who Code uses infrastructure provided by Amazon Web Services, Inc. ("AWS") to host or process **Student Data** as well as all other **User Data** submitted to the Services. Information about security and privacy-related audits and certifications received by AWS, including ISO 27001 certification and SOC reports, is available from the **AWS Security website** and the **AWS Compliance website**.

II. Key Security Policies and Procedures

Security Policies and Procedures

The Services are operated in accordance with the following key policies and procedures to enhance security:

- User passwords are stored using a one-way salted hash. Passwords are not logged, not transmitted as plain text, and neither are they stored as plain text. Girls Who Code applies the industry's best practices for handling user passwords.
- Multi-factor authentication and/or a Virtual Private Network (VPN) is required for key systems, including hardware tokens for administrators, and access to data and systems is limited based on role and job responsibilities
- Single Sign-on is enabled for third-party applications wherever possible.
- Data is encrypted at rest and in transit using TLS 1.2 and newer
- Application Security and testing practices such as code reviews, third-party library security assessments, container security, continuous integration testing, correctness testing, and more are enabled and optimized.
- Operational monitoring and processes have been established to quickly identify, recover, and improve to build resilience in everything we do.
- User access log entries will be maintained, containing the date, time, user ID, URL executed, or entity ID operated on, the operation performed (created, updated, deleted), and source IP address. Note that the source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by a customer or its ISP.
- System infrastructure logs, and application logs with user activity will be kept for a minimum of 30 days. Logs will be kept in a secure area to prevent tampering. Girls Who Code does not operate data centers directly and utilizes cloud infrastructure providers - mainly Amazon (AWS) who have their own monitoring and logging systems in place, such as for physical data center access. This information can be found here: **https://aws.amazon.com/compliance/data-center/controls/**
- Certain administrative changes to the Services (such as password changes and adding custom fields) are tracked and are available for viewing by internal system administrators only.

For more details on each of the Key Security Policies and Procedures, please see the relevant sections below.

Testing and Backup Controls

We have data backup and recovery capabilities that are designed to provide timely restoration of the Girls Who Code Services, with minimal data loss, in the case of catastrophic failure. These backups are encrypted and stored in multiple availability zones. Technical and organizational measures to ensure the integrity, availability, and resilience of the processing systems, and that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Regular patching and deployment of various systems into production;
- Uninterruptible power supply (UPS) - While Girls Who Code does not operate their own Data Centers, Cloud providers such as **Amazon** supply power backups to the servers utilized by Girls Who Code in their data centers;
- Remote storage - all **User Data** and operational data are stored remotely and securely on our cloud provider's servers;
- Antivirus/firewall systems; and
- Disaster recovery plan, in the event of a physical or technical incident

To test, assess, and evaluate the effectiveness of the measures described above, we implement the following technical and organizational measures:

- Testing and evaluation of software updates before they are installed;
- Annual Penetration tests and BSIMM reviews.

III. IT Governance

Technical and organizational measures to improve the overall management of IT and ensure that the activities associated with information and technology are aligned with the compliance efforts include:

- Processes for data minimization;
- Processes for data quality;
- Processes for limited data retention;
- Processes for ensuring accountability; and
- Data subject rights policies.

Separation control

Technical and organizational measures to ensure that **Personal Information** collected for different purposes can be Processed separately include:

- Separation of databases;
- Segregation of functions (production/testing); and
- Procedures for storage, amendment, deletion, and transmission of data for different purposes.

IV. Infrastructure Security

A. Encryption at Rest and In Transit

User Data (including **Student Data**) is stored at our Service Provider, Amazon Web Services (AWS) and the following applies to their technical and organizational measures. In addition, we secure employee computers. All personally identifiable information is encrypted at rest using modern encryption algorithms.

Access to the Girls Who Code Service occurs via encrypted connections (TLS 1.2 and newer), which encrypts all data before it leaves the Girls Who Code Service's servers and protects that data as it transits over the internet. We primarily use Amazon AWS to run servers and other infrastructure for our Services. We follow the best practices for both Amazon AWS and all other third-party services and integrations. We use HTTP Strict Transport Security to ensure that pages are loaded over HTTPS connections.

B. Network Security

The Girls Who Code Services use AWS to host the server infrastructure. AWS undergoes strict ongoing security assessments from external audit firms to ensure compliance with security standards, including ISO 27001, SOC 2, PCI DSS Level 1, and FISMA. See **https://aws.amazon.com/compliance/programs/** for more details.

Network access to the Girls Who Code Services infrastructure is highly restricted to only staff who require access. Multi-factor authentication is required for administrative access to servers hosted in AWS.

C. Patching

We use automated processes to regularly install security updates on the infrastructure that powers the Girls Who Code Services, these processes include:

- AWS Managed Services (e.g., Relational Database Service): AWS proactively notifies our engineering team when updates are available, and we apply them in a timely fashion.

- Girls Who Code HQ Application: Application code is peer-reviewed and penetration tested.

D. Monitoring

Girls Who Code monitors the Services through the use of extensive logging. AWS CloudWatch is used for any workload deployed to AWS. At the same time, for better Application Performance Monitoring capabilities GirlsWhoCode uses Elastic APM, with opentrace and open telemetry enabled. Incident Response Plans and internal processes are in place to guide the response to any security alerts or security investigations.

Within the application, Girls Who Code may analyze data collected by users' web browsers for security purposes, including detecting compromised browsers, preventing fraudulent authentications, and ensuring that the Services function properly.

E. Security Logs

All systems used in the provision of the Services, including firewalls, routers, network switches, and operating systems, log information to their respective system log facility or a centralized logging server (for network systems) in order to enable security reviews and analysis.

V. Disaster Recovery and Incident Management

Disaster Recovery

Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. The Services utilize isolated, fault-tolerant zones within the primary data center region to replicate, backup, and distribute the workload over the required hardware, and software components needed to continue providing the service to users in the event of failures.

Girls Who Code has disaster recovery plans in place and tests them at least once per year. The scope of the disaster recovery exercise is to validate the ability to failover a production instance from the primary data to the secondary data center utilizing developed operational and disaster recovery procedures and documentation. The Services’ disaster recovery plans target the most expedient recovery with minimal disruption to users. However, these targets exclude a disaster or multiple disasters causing the compromise of the entire data center region and exclude development and testbed environments.

Incident Management

Girls Who Code maintains security incident management policies and procedures that set out roles, responsibilities, and procedures for reporting, investigation, containment, remediation, and notification of security incidents. Girls Who Code notifies impacted users without undue delay of any unauthorized disclosure of their respective **Student Data** or **Personal Information** by Girls Who Code or its agents, of which Girls Who Code becomes aware to the extent permitted by law.

VI. Physical Security

Physical Access Controls

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers, and related hardware), where **User Data** is Processed, include:

- Establishing security areas, and restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card, hardware keys);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system; and
- Securing decentralized data processing equipment and personal computers.

> *Note: The Girls Who Code Services are currently hosted in AWS, and* ***User Data*** *(including Student Data) is stored at our Service Provider - currently AWS – which employs industry-leading physical security measures to protect their data centers, and the above applies to their technical and organizational measures. These security features are regularly audited by third party auditors. You can learn more about AWS' physical security* ***here.*** *In addition, we secure decentralized data processing equipment and personal computers.*

Virtual Access Control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous password attempts; and
- Creation of one master record per user, user-master data procedures per data processing environment;

Data Access Control

Access to the Girls Who Code Services infrastructure is highly restricted. We limit access to individuals who need access to do their jobs, such as engineers, data analysts, product managers, and support personnel. All-access to our infrastructure is logged. All-access to our infrastructure requires the use of strong passwords and multifactor authentication.

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such **User Data** (including **Student Data**) in accordance with their access rights, and that **User Data** (including **Student Data**) cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access **Personal Information** without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure;
- Default configuration; and
- Encryption

Disclosure Control

Technical and organizational measures to ensure that **Personal Information** cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport, or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities **Personal Information** are disclosed, include:

- Encryption/Pseudonymization/tunneling;
- Logging
- Transport security

Entry Control

Technical and organizational measures to monitor whether **Personal Information** has been entered, changed, or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems; and
- Audit trails and documentation.

VII. Architecture and Data Segregation Security

The Services are designed to separate and restrict **Student Data** access based on business needs. The architecture provides an effective logical data separation through a separate database for Club Services and via school-specific “Organization IDs.” This enables user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.