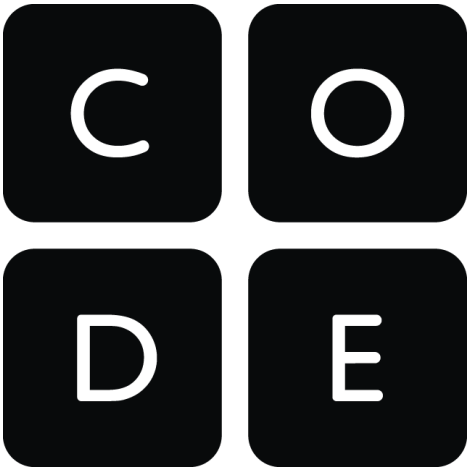

Code.org
Information Security Policy

Last Updated: April 2020

1 Introduction

1.1 Purpose

This document specifies security policies and practices relating to all data collected, processed, transmitted or stored by Code.org ("**Code.org data**").

1.2 Document control

The Code.org Leadership Team will periodically review this document and will be responsible for any modifications deemed necessary.

2 General Security Policy and Standards

2.1 Objectives

To establish and maintain adequate and effective information security safeguards for Code.org employees and contractors to ensure that the confidentiality, integrity and operational availability of Code.org data is not compromised. Code.org data must be safeguarded against unauthorized disclosure, modification, access, use, destruction, or delay in service.

2.2 Sensitivity of information

Code.org data, whether personally identifiable or not, is considered sensitive. A breach of any Code.org data would be considered severe.

3 Personnel Security

3.1 Data access

Access to Code.org data should be granted to Code.org employees on an individual basis as determined by business need. Code.org data access policies and procedures will be overseen by the CTO.

3.2 Non-disclosure information and security agreement

All Code.org employees must sign a non-disclosure information and security agreement, and pass a background check.

3.3 Training

All Code.org employees are to receive appropriate training and regular updates in information security and privacy policies and procedures, including security requirements, legal responsibilities and business controls.

3.4 Disciplinary process

An appropriate disciplinary process is to be in place to cover both employees and contractors who may knowingly disregard a particular policy requirement.

4 Physical Security

4.1 General Requirements

Areas in which Code.org data is stored are to be physically secure and access restricted to authorized personnel only. Production data storage should be in a facility audited to a modern security standard such as SOC 3.

4.2 Equipment Protection

All items of data center equipment are to be sited or protected to minimize the risks from environmental threats and hazards, and opportunities for unauthorized access. Data center equipment must be sufficiently robust and redundant to survive a normal rate of hardware failure. Code.org data must be stored with enough redundancy such that the loss of a single hard drive does not lead to loss of any Code.org data.

4.3 Data Backup

Code.org data in production must be regularly backed up so that it can be restored if or when necessary.

4.4 Disaster Recovery

A disaster recovery system must be implemented such that in the event of a major catastrophe (such as loss of primary data center), Code.org site and data may be restored. In the event of a major disaster that leads to the loss of production Code.org data, it is expected that up to 24 hours of data may be lost after restoring from disaster recovery backups, and recovery time may be up to 48 hours.

4.5 Encryption at Rest

All Code.org data containing personally identifiable information (PII) should be encrypted at rest (in storage). All non-PII Code.org data should be encrypted at rest whenever commercially feasible.

4.6 Destruction of information

Code.org data must be destroyed according to policies including the Code.org Privacy Policy and applicable regulations including GDPR.

5 Network Security

5.1 General Requirements

Code.org data must be securely stored on networks with controls to prevent unauthorized access. Controls should include firewalls and secure access by authorized Code.org employees.

5.2 Encryption in Transit

Code.org data must be encrypted in transit over the public Internet.

6 Information Security Incident Response

6.1 Priority 0 incidents

Priority 0 incidents include leak of personally identifiable information (PII); critical server vulnerabilities; and spamming.

Target action/resolution time: Immediate.

Examples:

1. A user can obtain the PII for another user. (P0 if leaks have happened; P1 if no evidence this has been exploited)
2. A user (besides approved employees) can assume the credentials of an admin or teacher. (Always P0)
3. Users are able to ssh into and execute commands on our servers. (Always P0)
4. SQL injection allows the user to run arbitrary queries or updates. (Always P0)
5. Our servers are being used to send spam. (Always P0)
6. Script injection (XSS) allows a user to run arbitrary Javascript in our pages. (P1 if not exploited)
7. CSRF (cross-site request forgery) bug. (P1 if not exploited)
8. Our servers are being used to issue DOS or SPAM attacks. (P1 if not exploited)

Action: Escalate urgently according to the following process:

1. Immediately escalate to all engineers if during the day. On nights and weekends, page the dev on call by sending a message to the email list with the word URGENT in the subject line. Text or call the CTO. Escalate further to additional Leadership team members if no response.

2. Do not close any security or privacy leak bug without approval of the CTO.

3. After the fix is done: hotfix or push it immediately to production. This is a top priority fix - more important than all other fixes or work in progress. Taking down the website or closing access to AWS resources is a possible mitigation step if that prevents further data exposure during investigation and fix.

4. Keep engineers, CTO and Leadership team up to date as to status and resolution.

5. Director of Marketing, CEO and CTO to decide and execute on an external communication plan. CTO executes Data Breach Notification Plan as appropriate.

6. Be aware that Code.org's GitHub repo is public; be careful about how change is discussed in GitHub pull requests.

6.2 Priority 1 incidents

Priority 1 incidents include serious server vulnerabilities; XSS/XSRF bugs; and unexploited issues classified as P1 above.

Target action/resolution time: within 24 hours.

Examples:

1. A network configuration issue allows users to issue hits against internal servers or ports without going through the firewall.

2. One non-admin user can assume the credentials of another non-admin user.

3. An XSRF bug exists but has not yet been exploited.

4. An unpatched security hole in an Ubuntu service or executable exists.

5. Our servers could potentially be used to send spam.

6. Users can DOS our site by hitting expensive pages.

Action: Alert Developer of the Day and CTO. CTO and engineering team plans and executes fix. The Director of Marketing, CTO and CEO decide and execute on an external communication plan as appropriate. CTO executes Data Breach Notification Plan as appropriate.

6.3 Data Breach Notification

If Code.org finds evidence of a breach or unauthorized release of any personally identifiable information, we will notify the impacted users via email. To protect student privacy, we do not store any student email addresses, so we will contact their teacher (if they are in a teacher's section) or parent (if parent email is provided). If we believe the breach resulted from criminal conduct, we will also report to law enforcement.

6.3.1 Notification Requirements under GDPR

Notification to the Supervisory Authority

In case the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the event shall be notified to the Supervisory Authority (SA). Code.org shall use ICO, the UK's Supervisory Authority for GDPR, as SA for notifications unless otherwise decided by the CTO. This notification shall take place without undue delay not later than 72 hours after becoming aware of the data breach. Notification is the responsibility of the CTO. Provided documentation will serve as an element of proof and will be investigated by the SA to determine whether or not Code.org complies with legislation concerning personal data breaches.

This notification shall at least contain the following information:

- A description of the nature of the personal data breach, including where possible:
    - The categories and approximate number of data subjects concerned, and
    - The categories and approximate number of personal data records concerned.
- Contact details for Code.org CTO where more information can be obtained
- Description of likely consequences of the personal data breach
- Description of measures taken or proposed by Code.org to address the personal data breach, including, where appropriate, measures to mitigate possible adverse effects.

Code.org must document all personal data breaches, including the circumstances and facts of the breach, the consequences, and corrective measures taken to solve the breach. By means of this documentation, the SA can verify compliance with the GDPR.

Cases in which the SA does not need to be notified

Code.org does not need to notify the SA concerning a data breach if the circumstances of the data breach indicate that the breach will not likely have an impact on the privacy or personal data of the data subjects involved.

Communication to the data subject

In case the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the incident must also be communicated to the data subject without undue delay.

The notification shall describe in clear and plain language:

- The nature of the personal data breach
- Name and contact details of Code.org responsible person for data protection
- A description of the likely consequences of the personal data breach
- A description of measures taken or proposed by Code.org to address the personal data breach and to mitigate possible adverse effects

However, the communication to the data subject shall not be required if any of the following are true:

- Code.org has implemented appropriate technical and organizational measures with regard to the data affected, rendering the personal data unintelligible to any person who is not authorized to access it, e.g. encryption.
- Code.org has taken subsequent measures ensuring that the high risk to rights and freedoms of data subjects is no longer likely to materialize.
- It would involve a disproportionate effort. In that case, there shall be a public communication or similar measure informing the data subjects in an equally effective manner.

In exceptional cases, when there is a risk that the notification to the data subjects will have an impact on the effectiveness of the investigation of the incident, Code.org can postpone this notification. However, such delay should be mentioned and explained in a notification to the SA.

6.4 Handling Potential Security Risks

Code.org engineering team shall maintain an active security posture against possible information security risks and threats. These threats include but are not limited to vulnerabilities in open-source software and libraries used by Code.org; undiscovered vulnerabilities in Code.org website; and network vulnerabilities. Code.org engineering team shall use commercially feasible techniques to mitigate security risk, including security tools, active discovery of potential vulnerabilities, and sufficient logging, monitoring and auditing to detect attempted or actual breaches.