GoodGames Security Policy

Last updated: November 12, 2021

GoodGames is built to be easily accessible by our clients and participants. Our products offer an easy and accessible way to enhance interactivity, engagement and inclusivity in meetings, presentations, workshops, and other real-time (synchronous) gatherings. Ease of use, openness and inclusivity are valuable and important aspects of the GoodGames value proposition to our users.

Keeping your data secure is of utmost importance to us and we have implemented appropriate technical and organizational measures to ensure that all data sent to GoodGames is handled in a secure manner.

If you wish, you can still share URLs, ID, or other information to make the games and their administration less private and we cannot take responsibility for privacy that is breached by the fundamental openness of the platform or sharing information you should not have.

GoodGames is hereinafter referred to as “we”, “us”, “our” or “GoodGames” and ”you” shall be interpreted as the person or entity who has signed up for an Account to use our Services including, to the extent applicable, you who use our Services as a member of an Audience.

Human Resource Security

We have processes in place to ensure that all personnel with access to systems or information about our Users as well as User Data have agreed to a non-disclosure undertaking as part of their employment contract with GoodGames.

Our staff onboarding process includes verifying the identity of staff and the background and skill they state. Our rigorous staff termination process includes revoking access rights, seizing IT equipment, invalidating all access as well as notification of continuous confidentiality obligations.

Any staff with access to information about users shall be required to take appropriate security training on a regular basis as set out in the Security Revision Schedule below. When employment has ended, we revoke all access that the concerned employee had.

Roles, Accountabilities, and Responsibilities

CHIEF EXECUTIVE OFFICER

- Accountable for all aspects of GoodGames’ information security and data processing.
- Determines the privileges and access rights to the resources within their areas.

SECURITY OFFICER

- Responsible for the security of the IT infrastructure.

- Plans against security threats, vulnerabilities, and risks.
- Implements and maintains Security Policy documents.
- Ensures security training programs.
- Ensures IT infrastructure supports Security Policies.
- Responds to information security incidents.
- Helps in disaster recovery plans.

ALL EMPLOYEES

- Must uphold and meet the requirements of GoodGames' Security Policy.
- Report any actual, attempted, and/or suspected security breaches.

In consideration of being entrusted rights to use GoodGames' systems, repositories, and information all employees must acknowledge the following:

- That all confidential information must be kept confidential and that any disclosure of confidential information would cause harm to GoodGames.
- That employee must only handle confidential information on devices issued by GoodGames.
- That employee will not, directly or indirectly, make use of information other than in the course of work duties;
- That employee will keep passwords, etc. entrusted to the employee, strictly confidential. However, Admin passwords are stored on our system in a hashed format and not in clear text;
- We require password-protected SSH keys to access all of our servers.
- GoodGames implements host-based (i.e. per workstation) security by contractually requiring strong (at least AES128) encryption on all workstations. This is verified at the start of employment and at least twice a year.
- Firewall enabled on all workstations.
- That employee will log off the computer or activate the screensaver configured with a password immediately upon completion of each work session;
- That the employee understands that his/her rights to use GoodGames' systems, repositories and information expire upon the termination of their work duty, or at any time upon the request by GoodGames. If the employee is not otherwise instructed, GoodGames requests that the employee shall immediately return all intellectual properties that the employee holds when his/her rights have expired.
- A clear desk policy to protect customer information.
- GoodGames Password Control Policy defines the requirements for proper and secure handling of passwords within the organization. All employees who handle assets and services related to GoodGames use password management via a certified password management system and strong passwords are required.

Operations Security

Physical access to GoodGames' office premises is restricted to staff individually and on a need to have basis.

GoodGames maintains separation/segregation of duties to prevent error and fraud by ensuring that at least two individuals are responsible for separate parts of any task so that no single role or account can access, modify or use data without authorization or detection.

We log important events, which enable us to monitor and follow up on suspicious or malicious activity.

GoodGames maintains the principle of least privilege (PoLP), meaning that every module (such as a process, a user, or a program, depending on the subject) must only have access to the information and resources that are necessary for its legitimate purpose.

Losses, theft, damages, tampering, or other incidents related to IT-assets that compromise security must be reported as soon as possible to the Security Officer.

Business Continuity

We reserve the right to disconnect the Application for service and upgrades without giving prior notice to you. Our intention is to give you notice before updates or maintenance of the Application. Our intention is to only perform planned maintenance on low traffic hours/weekends. We reserve the right to implement new updates and versions of the Application, to the extent deemed suitable by us.

We take help from Intruder who performs vulnerability scans on a regular basis and reports threats. High vulnerabilities are fixed within two weeks, medium within six weeks, low within eight weeks.

Continuous Improvements

Our engineering practices ensure that we have security in mind in all stages of a development lifecycle. While no system is completely secure, we will do our utmost to minimize any type of risk. Examples of Engineering practices:

- Clear code conventions enforced by static code analysis;
- Use of well-known frameworks to protect against common attack vectors (XSS, CSRF, SQL Injection, though we use MongoDB, a NoSQL database);
- Incident response plans are maintained and followed to quickly act on incidents;
- Continuous check-up to keep libraries up-to-date;
- Continuous integration builds and testing;
- Continuous improvement process with the entire product team where security issues are a standing item;
- Penetration tests are done by our hosting provider Akamai (Linode) on their infrastructure
- All code is peer-reviewed to find bugs and security holes early.
- All releases are tested before merging to production.
- Passwords are always kept in password safes or as configuration.

Independent Security Assessments

An independent third-party service provider performs vulnerability and pen-test scans on our web applications on a regular basis, and reports threats in accordance with CVSS. High priority vulnerabilities are fixed within two weeks, medium within six weeks, low within eight weeks.

Processing

We are working with the best-in-class service providers for data storage. The service provider's physical infrastructure is hosted and managed within Akamai's secure data centers. Akamai continually manages risk and undergoes recurring assessments to ensure compliance with industry standards.

Akamai's data center operations have been accredited under:

- SOC 2 Type 2
- SOC 3

Akamai security is covered here (https://www.linode.com/legal-security/)

Security measures are taken to protect you and your data both for "Data at rest" and "Data in transit".

Data at Rest

Credit card information is stored with a Level 1 PCI compliant third-party vendor. See Payment Details below for more information.

Data in Transit

We use standard TLS >=1.2, ie. Encryption of data "in-transit, and are rated A by 3rd party vendor, SSL Labs. Privacy and protection of user data are of the highest importance to us and we both have technical and operational support in place to ensure this.

Backups and Data Loss Prevention

Data is backed up continuously.

User Passwords

We encrypt (hashed and salted) passwords using the Bcrypt algorithm to protect them from being harmful in the case of a breach. GoodGames can never see your password and you can self-reset it by email.

Employee Passwords

Passwords that are used in the line of work are always kept in a safe. We enforce 2FA where applicable and that employees use screen locks whenever they are not by their workstation.

Payment Details

We use Level 1 PCI compliant payment processor Stripe for encrypting and processing credit card payments. We never see or handle credit card information.

Security Incidents

We have in place and will maintain appropriate technical and organizational measures to protect personal data as well as other data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing (a “Security Incident”).

We have an incident management process to detect and handle Security Incidents which shall be reported to the Security Officer (security@goodfocus.net) as soon as they are detected. This applies to GoodGames employees and all processors that handle personal data. All Security Incidents are documented and evaluated internally and an action plan for each individual incident is made, including mitigatory actions. If you are affected by the Security incident, we will contact you as soon as possible through relevant channels.

Security Revision Schedule

This section shows how often GoodGames conducts security revisions and conducts different types of tests. If significant changes occur GoodGames will initiate an otherwise planned activity to ensure continuing security.

Planned activity	Frequency
Security training for personnel	Yearly and at beginning of employment
Revoke system, hardware and document access	At end of employment
Ensures access levels for all systems and employees are correct	Annually

Firewall settings verification for workstations and Network	Annually
Ensure all critical system libraries are up-to-date	Continuously
Unit and integration tests to ensure system functionality and security	Continuously
External vulnerability scans to ensure system security	Continuously

This Security Policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

Contact

GoodGames, LLC is a United States limited liability company.

You can always reach us at hello@goodfocus.net.

Changes To This Security Policy

This Security Policy is not part of the Terms. Laws, regulations, industry standards and our business is in constant change, which requires us to make changes to the Security policy. . We will post the changes to this page and encourage you to review our Security Policy to stay informed. If we make changes that materially alter your privacy rights, we will provide additional notice through the Services or via email if you have subscribed for notifications. If you disagree with the changes to this Security Policy, you should contact us to deactivate your Account.