CORPORATE GIFT.COM

Security Whitepaper

Our Solution

We've constructed our solution around three pillars: a large product catalog with a diverse selection and advanced technology, automation for seamless process control, and a team of experts ready to provide best practice and support to make sure every customer's need is met.

People Security

All CorporateGift employees are required to understand and follow all internal policies and standards. As part of the onboarding process, we provide security training including private device security, acceptable use, preventing spyware/malware and phishing, email security, physical security, passwords, data privacy, account management, incident reporting and more. We also conduct background checks on employees before hiring.

Application Security

Secure Software Development Lifecycle

Standard best practices are employed throughout our software development cycle from design to implementation, testing, and deployment. All code is checked and stored in a permanent, version-controlled repository. Code changes subject to peer review and continuous integration testing to screen for potential security issues on an ongoing basis.

We utilize a formal change control process for all changes to information resources to ensure any proposed change is reviewed, tested and authorized before release, and rolled out in a controlled manner, with each proposed change monitored.

We employ secure programming techniques for both new code developments and code reuse to ensure standards are applied to development and are consistent with currently recognized best practices.

Secure by Design

Security by design is a core principle at CorporateGift. Proposed features are reviewed by a team of senior engineers experienced in building secure technology systems from ideation to ensure compliance with security controls and protocol.
We leverage modern browser protections such as Content Security Policy (CSP) and security HTTP headers to prevent Cross-Site Scripting (XSS), Clickjacking and other code injection attacks resulting from the execution of malicious content in the trusted web page context.

Security Testing
We adhere to the leading Open Web Application Security Project (OWASP) Testing Guide methodology for security testing. Following feature implementation, internal security QA is conducted to verify correctness and resilience against any attacks. If discovered, vulnerabilities are promptly prioritized and mitigated. We also regularly employ third-party security consultancies to independently audit and verify our applications.

Authentication
Corporategift.com allows users to login with Google accounts using OAuth 2.0. To ensure user access tokens are protected against attacks, we employ the most secure version of the OAuth 2.0 authorization code. Both access tokens and refresh tokens are encrypted at rest using AES-128 encryption by OAuth. Corporategift.com does not receive or store user passwords using OAuth. Users may at any time revoke access from CorporateGift.com and request deletion of account data.

In addition to OAuth, Corporategift.com can integrate with any SSO provider that supports OpenID Connect or SAML 2.0, such as Okta, ADFS, Acure, OneLogin and similar services. We rigorously test SSO authentication flows against attacks via a third party security testing company.

Network Security

Encryption in transit
We employ SSL/TLS encryption during data transfer between our servers and databases within the same data center to protect our applications and services. We continuously monitor and update cryptographic and cipher suite settings as risks change.

To prevent middleman attacks, we employ protocol to ensure our applications only communicate with our own servers. Within our application, we flag all authentication cookies as Secure and apply HSTS (HTTP Strict Transport Security). The Corporategift.com domain is included in HSTS Preload list for all major browsers.

Data Encryption at rest
Using Amazon Web Services RDS MySQL based relational database our customers data and backup are encrypted using the open standard AES-256 encryption algorithm. This encryption option protects against physical exfiltration or access of your data bypassing the DB instances. It is therefore critical to complement encrypted resources with an effective encryption key management and database credential management practice to mitigate any unauthorized access.

Web Application Firewall
Corporategift.com uses Amazon Web Services, web application firewall (WAF), to protect our infrastructure from unauthorized access and prevent malicious attacks. AWS WAF is equipped

to protect against common web exploits and bots that may affect availability and compromise security. AWS WAF we are able to create rules that prevent attacks such as SQL injection, cross-site-scripting or issues like OWASP Top 10 security risks.

Network Isolation
Corporategift.com divides its systems into separate networks using logically isolated instances on Amazon Web Services. This setup protects sensitive data by providing isolation between instances in different trust zones. Systems supporting testing and development activities are hosted in a separate network from systems supporting Corporategift.com's production website.

Customer data is only permitted to exist in Corporategift.com's production network (our most tightly controlled network).

We significantly restrict network access to Corporategift.com's production environment from open, public networks (the Internet). Only network protocols essential for making Corporategift.com's service work are open at Corporategift.com's perimeter. All network access between production hosts is restricted using security groups to only allow authorized services to interact in the production network.

Our infrastructure and applications are monitored using standard health checks and log watchers to detect systems that are malfunctioning as well as identify potential intrusions. Any emerging issues are addressed by our on-call engineering team.

Physical Security

Data Center Security
Corporategift.com leverages Amazon Web Services Networks data centers for all production systems and customer data. AWS Networks offers state-of-the-art physical protection for the servers and complies with a comprehensive array of standards.

For more information on Amazon Web Services *Networks Security, see AWS Security info on Introduction to AWS Security - AWS Whitepaper.*

Office and Digital Equipment Security
We have implemented policies and procedures to address the security posture of our workstations and laptops. All employee computers comply with these standards for device security. We require computers to have strong passwords, full disk encryption and automatic lock when idle. Although no data is stored on employee computers or servers located in our office, Corporategift.com's premises are protected with locked building entrances, deadbolted doors, CCTVs, and intrusion detection alarms.

Data Security
We are committed to the goals of confidentiality, integrity, and privacy of our customer data by employing a multifaceted approach to data security.

Employee Access to Customer Data
No customer data persists on employee laptops. We apply the principle of least privilege in all operations to ensure the confidentiality and integrity of customer data. All access to systems and customer data within the production network is limited to those employees with a specific business need and authorization. The best effort is made to troubleshoot issues without accessing customer data; however, if such access is necessary, all actions taken by the authorized employee are logged. Upon termination of work at Corporategift.com, all access to Corporategift.com systems is immediately revoked.

Audit Trails
We log all changes to infrastructure and activities that access customer data for specific business needs for auditing purposes. Only a small number of senior engineers on the infrastructure team have direct access to production servers and databases to protect end user privacy.

Employee Authentication
We protect production services and data using network isolation and strong authentication. We provide every Corporategift.com employee with a secure password manager account to create, store, and enter strong and complex passwords. We require employees to change passwords frequently, avoid reuse across accounts, and other behaviors that impact secure operations.

Server Hardening
We harden our production servers and bastion hosts by disabling unnecessary and potentially insecure services before use. We also scrub default passwords and apply custom configuration settings and follow CIS (Center for Internet Security) Benchmarks.

Vulnerability Management

We conduct regular, automated vulnerability tests and manual pen-testing on the production environment via independent third parties. We also use on-call engineers to immediately address any discovered threats to our network.

To encourage vulnerability disclosure, we provide the following guidelines:

Compliance

Compliance with applicable regulations, standards and industry best practices protect us and our customers sensitive information in ways that are testable and verifiable. The following security-related audits and certifications are applicable to Corporategift.com services:

• Corporategift.com has undergone an ISO27001 audit, and a copy of the most recent
The report is available upon request.

• Privacy Shield: Corporategift.com has certified with the U.S. Privacy Shield Framework with respect to the personal data we receive and process on behalf of our customers.

• GDPR: Corporategift.com had undergone GDPR, the European Union privacy regulation audit and applied the measures and procedures to comply with it.

• CCPA: Corporategift.com undergonce CCPA, California consumer privacy act audit and applied the measures and procedures to comply with it.

Corporategift.com is hosted on Amazon Web Services, which are highly scalable, secure, and reliable. Amazon Web Services complies with leading security policies and frameworks, including SSAE 16, SOC framework, ISO 27001,PCI DSS, GDPR and CCPA. More information can be found at

Disaster Recovery and Business Continuity

Corporategift.com customer data is regularly backed up each day to guard against data loss. All backups are encrypted both in transit and at rest using strong industry encryption. We geographically distribute all backups to maintain redundancy in the event of a natural disaster or a location-specific failure. We are also set up to operate from geographically distributed locations, and leverage cloud resources.

Conclusion

We take user and customer security seriously at Corporategift.com, and every measure is taken to ensure the integrity of our application and services. We work hard to maintain the highest level of trust and safety across our organization and with all stakeholders.

If after reading this whitepaper you have any further questions, please don't hesitate to contact our security team at siso@corporategift.com