welcome

Information Security Policy

OVERVIEW

This document contains details of the information security practices conducted at Glide Holdings, Inc. (dba Welcome) or “The Company.”

SCOPE

This document discusses several information security implementations at Welcome such as:

- Security Risk Management
- Information Classification
- HR Policy
- Access Management
- Technical Operations
- Incident Response
- Physical security
- Privacy Policy

Security Risk Management

Welcome’s web applications are subject to security assessments based on the following criteria:

a. Major/New Application Releases - will be subject to a full assessment prior to the approval of change control documentation and/or deployment into the live/production environment.

b. Point Releases - will be subject to full assessment after which it will be bound to policy requirements.

c. Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

d. Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Director of Engineering or an appropriate manager who has been delegated this authority.

Welcome leverages Github as the Continuous integration provider. All code is reviewed before being added to the service, including third party tools and integrations. Additionally, all source code is scanned by Github (with read-only access) for any open source packages with known vulnerabilities and available upgrades. At any level of severity, the open source packages are upgraded or patched, and released immediately. We have expansive test coverage across our code base, and deploy and test our application in a staging environment before making it available to our customers.

Welcome also uses Cloudflare as the DNS and firewall management platform. Welcome is committed to constantly monitoring and assessing web traffic based on numerous analytical points provided by the vendor. Additionally, Welcome has implemented real-time error logging, system monitoring, and security alerts.

Information Classification

In this section, we detail the tiers of information customers make available to Welcome for storage and responsible use within the web applications and the organization.

Public: Documents/information that are not sensitive and where there is no issue with release to the general public such as public websites, logos, team profiles, and branding information.

Confidential: Documents/information only to be viewed internally or with third parties that have signed a non-disclosure agreement, and to which the parties agree to disclose or share said information

Employee Confidential: Documents/information only to be viewed by employees at the company.

Management Restricted: Documents/information only to be viewed by the senior management at the company.

Private: Documents/information which contain personally identifying or sensitive information. This includes, but is not limited to:

- Company Profile information
- Company Employee information
- Company Candidate information
- Compensation Information
- Information that is not publicly available on any forums, or websites and/or require special authorization to access

HR Policy

As a general good practice, Welcome will conduct background checks on all new employees. New employees are also subject to other security assessments such as references in order to identify any potential physical or digital security risks. As part of the onboarding process, new employees will go through annual security awareness training regardless of the job function to be carried out by such employees. Upon termination of employment, any company-owned hardware will be immediately returned to the designated person(s). Any access to sensitive information via email clients, passwords, and 3rd party software will be immediately discontinued. As a condition of employment, all Welcome employees are required to execute non-disclosure and invention assignment agreements.

Access Management

Welcome employees have tiered access to information regardless of which party provides such information. Customer data access is audited, and limited to Welcome employees on a "least privilege" principle.

Welcome requires and enforces user access and authorization through secure logins and passwords. Passwords to vendor accounts are securely managed by Welcome in 1Password, and access is granted on a need-basis which is subject to an evaluation by engineering leadership. Multi-Factor Authentication is enforced on any 3rd party platforms that have that authentication process implemented on such platforms. Welcome employees have access to a customer management portal used to service our customers. However, provisions and permissions on actions and access to such information is tiered based on the employee's function at Welcome, and all employee activity is audited and logged. All information is to be kept confidential by employees. That is, no information that discloses the identity of Welcome Inc. customers, it's employees and/or sensitive information is to be shared outside of Welcome Inc.

Web applications may have features which require federated access to 3rd party platforms such as Applicant Tracking Systems and/or other providers. When customers enable such features, credentials such as API keys are NEVER stored in plaintext and all information is encrypted at rest. Welcome will never share such information with any third party. Once a customer disables federated access, any sensitive information is automatically deleted and revoked.

Technical Operations

Welcome leverages the Amazon Web Services cloud platform to host core web applications. Access to this hosting platform is limited to the engineering leadership and the development operations team. Two-Factor authentication via an authenticator application is required in order to access this platform.

Logging is enabled and required for all application load balancers, caches, databases, etc. All data is encrypted at-rest and in-transit. Application servers are hosted behind a VPC. Any party wishing to interact with Welcome Inc. exposed systems must always communicate using TLS/SSL. Any unencrypted/insecure communication is logged via Cloudflare and automatically rejected. Such communication is also investigated to assess potential security threats.

Incident Response

Welcome is committed to the security of our customers' data and sensitive information, and has in place a Security Response and Business Continuity Policies. In summary, Welcome keeps extensive database backups and snapshots of our caches. Upon the detection of application failure, downtime, or breach, a full investigation will be launched by the information security team immediately. Parties will be alerted on a need-to-know basis until services are restored. Once patched and deployed to the live/production environment, Welcome employees and customers will be notified of the occurrence. A "post-mortem" report detailing the date/time of the incident, high-level details of the incident, and the resolution will be generated. The report will also note if the information security team believes customers' sensitive information was exposed.

For other incidents regarding an outage or degraded performance of Welcome's applications, customers will be notified immediately via a status page. This status page is publicly available and updates the current status of an incident or outage. Customers will have the option of signing up for email notifications and are notified of any changes in the status of an outage. Details of the outage will be included in the notification as long as the details do not expose any potential security risks.

Physical Security

Welcome owns and manages any hardware required to carry out the functions of all its employees. As such, all hardware and software owned and managed by Welcome is subject to a security audit at any time whether or not an incident occurred. As part of an ongoing information security effort, all Welcome employees are required to enable password protected access to hardware such as laptops and mobile devices.

Privacy Policy

Welcome's Privacy Policy can be reviewed at https://www.heywelcome.com/privacy

Note: This policy document is subject to change, and does not change, modify, or alter the terms and conditions set forth in master services agreements we have executed with our customers.