Qnect Pte Ltd (“Get”)

Security

Get users trust us with their events, memberships, and merchandise. That trust is based upon us keeping data both private and secure. The information on this page is intended to provide transparency about how we protect that data. We will continue to expand and update this information as we add new security capabilities and make security improvements to our products.

Security Program

We drive a security program that includes the following focus areas: product security, infrastructure controls (physical and logical), policies, employee awareness, intrusion detection, and assessment activities. The security team runs an in-house Incident Response (“IR”) program and provides guidance to Get employees on how to report suspicious activity. Our IR team has procedures and tools in place to respond to security issues and continues to evaluate new technologies to improve our ability to detect attacks against our infrastructure, service, and employees. We periodically assess our infrastructure and applications for vulnerabilities and remediate those that could impact the security of customer data. Our security team continually evaluates new tools to increase the coverage and depth of these assessments.

Network Security

Get defines its network boundaries using a combination of load balancers, firewalls, and VPNs. We use these to control which services we expose to the Internet and to segment our production network from the rest of our computing infrastructure. We limit who has access to our production infrastructure based on business need and strongly authenticate that access.

Account Security

We will encrypt the passwords using using Bcrypt algorithm (this creates a non-reversible secure password hash)
> and phone/email will be encrypted/decrypted using hybrid encryption mode.

Get never stores your password in plaintext. We use Brcrypt algorithm which creates a non-reversible secure password hash to securely store your account authentication information. We select the number of hashing iterations in a way that strikes a balance between user experience and password cracking complexity. We limit failed login attempts on both a per-account and per-IP-address basis to slow down password guessing attacks.
Get currently offers two-step verification (“2SV”), also known as two-factor or multi-factor authentication, for all selected accounts, and aim to roll it out to all users as soon as possible. Our 2SV mechanism is based on a time-based one-time password algorithm (TOTP). All users can generate codes locally using an application on their mobile device or can choose to have the codes delivered as a text message.

Product Security

Securing our Internet-facing web service is critically important to protecting your data. Our security team drives an application security program to improve code security hygiene and periodically assess our service for common application security issues including: CSRF, injection attacks (XSS, SQLi), session management, URL redirection, and clickjacking.
Every client application that talks to our service uses a well-defined thrift API for all actions. By brokering all communications through this API, we’re able to establish authorisation checks as a foundational construct in the application architecture. There is no direct object access within the service and each client’s authentication token is checked upon each access to the service to ensure the client is authenticated and authorised to access a particular organisation, event or merchandise.

Customer Segregation

Get's service is multi-tenant and does not segment your data from other users' data. Your data may live on the same servers as another user's data. We consider your data private and do not permit another user to access it unless you explicitly share it.

Media Disposal and Destruction

We securely erase or destroy all storage media if it has ever been used to store user data. We utilise a variety of storage options in Amazon Web Services("AWS"), including local disks, persistent disks, and Cloud Storage buckets. We take advantage of AWS' cryptographic erasure processes to ensure that repurposing storage does not result in exposing private customer data.

Data Retention and Storage

Customers data are kept for at least 5 years after the termination or closure of their account. All data is encrypted and stored in a data centre operated by Amazon Web Services ("AWS"), which is compliant with:

- PCI DSS Level 1
- SOC 1, 2, 3
- ISO 9001, 27001, 27017, 27018
- For others, see http://aws.amazon.com/compliance/

Activity Logging

Get performs server-side logging of client interactions with our services. This includes web server access logging, as well as activity logging for actions taken through our API. We also collect event data from our client applications.

Transport Encryption

Get uses industry standard encryption to protect your data in transit. This is commonly referred to as transport layer security ("TLS") or secure socket layer ("SSL") technology. In addition, we support HTTP Strict Transport Security ("HSTS").

We support a mix of cipher suites and TLS protocols to provide a balance of strong encryption for browsers and clients that support it and backward compatibility for legacy clients that need it. We plan to continue improving our transport security posture to support our commitment to protecting your data. We support STARTTLS for both inbound and outbound email. If your mail service provider supports TLS, your email will be encrypted in transit, both to and from the Get service.
We protect all customer data flowing using IPSEC with GCM-AES-128 encryption or TLS.

Resiliency / Availability

We operate a fault tolerant architecture to ensure that Get is there when you need it. This includes:

- Diverse and redundant Internet connections
- Redundant application load balancers
- Redundant servers and virtual instances
- Redundant underlying storage