Information Security and Business Continuity/Disaster Recovery Policy

Cat & the Fiddle (C&F) is committed to ensuring appropriate data protection and security procedures are practiced and enforced. Esmond Tan, as the outsourced Chief Information Officer (CIO) is responsible for:

- maintaining policies and procedures to protect personal data;
- assessing the impact of proposed changes to our information system;
- training other employees to observe the correct data protection and security procedures; and
- ensuring the information security policy is updated regularly.

The CIO has implemented the following policies regarding each aspect of information security.

Data: C&F does not collect or store any payment information. All payments are processed through secure connections and as such no credit/debit card information or PayPal login details is collected or stored by C&F. As at October 2017, secure connections with PaymentExpress/PayPal are encrypted using leading industry standards. Online account passwords are stored in salted cryptographic hash form, which cannot be restored to the original clear text form.

C&F also protects personal data from misuse or loss by restricting access to the information in electronic format and by appropriate physical and communications security. C&F takes reasonable measures to ensure that personally identifiable information remains secure. Only authorised employees who abide by our Data Security and Acceptable Use policies are permitted to access personally identifiable information. Any data destroyed is disposed of in a way that protects the privacy of personal data in an appropriate manner.

Application Level Security: At the application level, access rights are segregated into three level with different permissions. Basic Users will have permission to access basic customer details whilst Advanced Users will have permission to access all customer details as well as limited permissions to modify data and Administrators will have permission to access and modify all data.

Infrastructure: C&F utilises Digital Ocean ('DO) for its cloud computing infrastructure. DO is renowned for its scalable, highly available and durable infrastructure. Given its geographic location, physical access to C&F infrastructure is tightly controlled by DO and off limits to the general public, including DO and vendor staff. The C&F web server and database server, hosted on DO are not public network facing, therefore remote access is only available via a secure VPN using asymmetric key cryptography. DO subjects all remote access to C&F web and database servers to fine grained access control.

Business Continuity Plans and Disaster Recovery Procedure: At the application level, data and documents are scheduled for daily backups to an onsite Network Attached Storage (NAS) which is connected to an Uninterruptable Power Supply (UPS) to protect from power outages. File data on the NAS is subsequently mirrored on DO.

C&F databases are backed up in the cloud daily, using DO. The C&F database archives database change logs which enables database recovery to any point in time during the backup retention period up to the last five minutes of database usage. The database server is automatically updated periodically, which may include bug fixes and security patches.

C&F uses an automated backup process to automatically back up its database instance during a specific backup window, and keeps the backups for a limited, user-specified period of time. C&F can later recover its database to any point in time during the retention period. In addition to the daily automated backup, DO archives database change logs. This enables database recovery to any point in time during the backup retention period, up to the last five minutes of database usage.

Digital Ocean Security Policies (Source: https://www.digitalocean.com/security)

Physical Security

Our datacenters are co-located in some of the most respected datacenter facility providers in the world. We leverage all of the capabilities of these providers including physical security and environmental controls to secure our infrastructure from physical threat or impact. Each site is staffed 24/7/365 with on-site physical security to protect against unauthorized entry. Security controls provided by our datacenter facilities includes but is not limited to:

- 24/7 Physical security guard services
- Physical entry restrictions to the property and the facility
- Physical entry restrictions to our co-located datacenter within the facility
- Full CCTV coverage externally and internally for the facility
- Biometric readers with two-factor authentication
- Facilities are unmarked as to not draw attention from the outside
- Battery and generator backup
- Generator fuel carrier redundancy
- Secure loading zones for delivery of equipment

Infrastructure Security

DigitalOcean's infrastructure is secured through a defense-in-depth layered approach. Access to the management network infrastructure is provided through multi-factor authentication points which restrict network-level access to infrastructure based on job function utilizing the principle of least privilege. All access to the ingress points are closely monitored, and are subject to stringent change control mechanisms.

Systems are protected through key-based authentication and access is limited by Role-Based Access Control (RBAC). RBAC ensures that only the users who require access to a system are able to login. We consider any system which houses customer data that we collect, or systems which house the data customers store with us to be of the highest sensitivity. As such, access to these systems is extremely limited and closely monitored.

Additionally, hard drives and infrastructure are securely erased before being decommissioned or reused to ensure that your data remains secure.

Access Logging

Systems controlling the management network at DigitalOcean log to our centralized logging environment to allow for performance and security monitoring. Our logging includes system actions as well as the logins and commands issued by our system administrators.

Security Monitoring

DigitalOcean's Security team utilizes monitoring and analytics capabilities to identify potentially malicious activity within our infrastructure. User and system behaviors are monitored for suspicious activity, and investigations are performed following our incident reporting and response procedures.

Droplet Security & Employee Access

The security and data integrity of customer Droplets is of the utmost importance at DigitalOcean. As a result, our technical support staff do not have access to the backend hypervisors where virtual servers reside nor direct access to the NAS/SAN storage systems where snapshots and backup images reside. Only select engineering teams have direct access to the backend hypervisors based on their role.

Snapshot and Backup Security

Snapshots and Backups are stored on an internal non-publicly visible network on NAS/SAN servers. Customers can directly manage the regions where their snapshots and backups exist which allows the customer to control where their data resides within our datacenters for security and compliance purposes.

ISO/IEC 27001:2013 Certification

DigitalOcean is currently working towards achieving ISO/IEC 27001:2013 certification. Becoming certified will attest to our customers the integrity of DigitalOcean's Information Security Management System (ISMS). The scope of the certification will include all of our datacenters. Please check back here or our blog for an update when we are certified.

EU-U.S. Privacy Shield Framework

We are an active participant in and comply with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce and the European Commission. The framework provides DigitalOcean a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States.

You can find more information about our commitment to the EU-U.S. Privacy Shield Framework in our Privacy Policy. Our active participation in the EU-U.S. Privacy Shield Framework can be viewed on their website located here.

Datacenter Colocation Attestations and Certifications

All of our datacenters are audited and/or certified by various internationally-recognized attestation and certification compliance standards. Many of the SOC reports and certifications listed below are available if a signed NDA is in place between DigitalOcean and our customer.

Below is the list of our datacenter locations and the associated most commonly requested attestations / certifications. To request a NDA, SOC report / certificate listed below, or if you have any other compliance related questions please contact our Customer Support team here.

Datacenter	SOC 1 Type II	SOC 2 Type II	ISO/IEC 27001:2013	PCI-DSS
NYC1	✓	✓	✓	
NYC2		✓		✓
NYC3		✓		✓
LON1	✓	✓	✓	✓
AMS2	✓	✓	✓	✓
AMS3	✓	✓	✓	✓

SFO1		✓		✓
SFO2		✓		
SGP1	✓	✓	✓	
FRA1			✓	✓
TOR1	✓	✓	✓	
BLR1			✓	✓

System Changes: All proposed system changes are rigorously tested on our Development Server prior to going live in a carefully staged process and then subsequently reviewed.