Security Statement & Backup Policy

At TheCastleCloud.com we make it a priority to take our users' security, privacy and data integrity concerns seriously. We strive to ensure that user data is kept securely, backed up safely and that we collect only as much personal data as is required to provide our services to users in an efficient and effective manner.

TheCastleCloud.com uses some of the most advanced technology for Internet security that is commercially available today. This Security Statement and backup policy is aimed at being transparent about our security and integrity infrastructure and practices, to help reassure you that your data is appropriately protected.

Data Backup and Retention

General

- **Daily Backup:** Incremental backups are performed daily within each user's account of all the data in that account. This backup forms part of the data-usage of the account. This type of backup can be switched off in the subscription settings. A daily incremental backup is also taken of the entire CaslteCloud system, which is kept on both the CastleCloud server and are copied to a geographically separate, secure server
- **Periodic Backups:** Full Weekly and Monthly backups are taken of the entire CastleCloud system and these are kept on a separate secure server
- **Independent backup:** We advise that you take regular backups independently and download any data that might be critical to your organization. This is purely as a last line of defense

Accessible Data/Archive

- **Your Data:** For an active account that is within its limits of users, instruments and data-storage, your data will continue to be made available to you without archiving or removal.

File Restoration Methods and Timeframe

- **User Account Backup:** The backup made automatically within your account will be available to you to restore and can be accessed through your account. You will not be able to restore any data lost since the last backup.
- **System Backup:** If you need to recover data and do not have a user account backup, you will need to contact Castle Group Ltd to request your data to be restored. You can contact us at support@castlgroup.co.uk or by phoning us on +44(0)1723 584250. We will make every endeavor to have your data restored within 48 hours.

Backup Technologies

- User accounts with data are backed up within the CastleCloud software system using internal file creation scripts.
- Full system backups are created on the castle cloud server using a server-based database backup system.
- Last-line-of-defense-backups are created using Server to Server (STS) backup via an Authenticated Backup Protocol (ABP). These are located on an independent, secure Server.

Application and User Security

- **SSL/TLS Encryption:** All user interactions with thecastlecloud.com are done over a Secure Socket Layer (SSL) connection which protects communications by using both server authentication and data encryption. This ensures that user data in transit is safe, secure, and available only to intended recipients.
- **User Authentication:** User data on our database is logically segregated by account-based access rules. User accounts have unique usernames and passwords that must be entered each time a user logs on. TheCastleCloud.com issues a session cookie only to record encrypted authentication information for the duration of a specific session. The session cookie does not include the password of the user.
- **User Passwords:** User application passwords have minimum complexity requirements. Passwords are individually salted and hashed.
- **Data Encryption:** Certain sensitive user data, such as account passwords, is stored in encrypted format. Credit card information is held independently by https://stripe.com payment provider
- **Data Portability:** TheCastleCloud.com enables you to export your data from our system in a variety of formats so that you can back it up, or use it with other applications.
- **Privacy:** We have a comprehensive privacy policy that provides a very transparent view of how we handle

your data, including how we use your data, who we share it with, and how long we retain it.

Physical Security

- **Data Centers:** Our primary server is located in a Tier 3, ISO certified data center in Amsterdam, Netherlands and is designed using the latest technology to specifically guarantee powerful performance, reliability and security.
- **Redundancy:** Multiple levels of redundancy have been built in to ensure consistent high performance, including multiple paths for cooling and power distribution with emergency backup generators ready to start in the event of power loss.

Network Security

- **Security Policies:** The server is also fully compliant with the latest security policies and audit guidelines, with a meticulous approach to ensuring private data stays private and protected at all times.
- **Security Monitoring:** All files stored on the server are continuously monitored for potential security breaches with immediate warning to us in the event of a suspicious file being added or altered.

Payment System

- **Online Payments:** We use https://Stripe.com for payment processing on thecastlecloud.com for the purchase and renewal of subscriptions.
- **Direct Payments:** Castle Group Ltd offer direct, manual payments through their own administration system. These payments are covered by Castle's Standard Conditions of Sale, which can be found here http://www.castlegroup.co.uk/about-castle-group-ltd/conditions-of-sale/

Organizational & Administrative Security

- **Training:** We provide security and technology use training for relevant employees.
- **Service Providers:** We screen our service providers and bind them under contract to appropriate confidentiality obligations if they deal with any user data.
- **Access:** Access controls to sensitive data in our databases, systems and environments are set on a need-to-know / least privilege necessary basis.

Software Development Practices

- **Coding Practices:** Our engineers use best practices and industry-standard secure coding guidelines to ensure secure coding.

Handling of Security Breaches

Despite best efforts, no method of transmission over the Internet and no methods of electronic storage are perfectly secure. We cannot guarantee absolute security. However, if TheCastleCloud.com learns of a security breach, we will notify affected users so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under UK law, as well as any industry rules or standards that we adhere to. Notification procedures include providing email notices or posting a notice on our website if a breach occurs.

Your Responsibilities

Keeping your data secure also depends on you ensuring that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your own systems, to keep any data you download to your own computer away from prying eyes. We offer SSL certification to secure the transmission of data, but it is your responsibility to ensure that your systems are configured to use that feature where appropriate.

Custom Requests

Due to the number of customers that use our service, specific security questions or custom security forms can only be addressed for customers purchasing a certain volume of user accounts within a TheCastleCloud.com PRO subscription. If your company has a large number of potential or existing users and is interested in exploring such arrangements, please contact us via www.castlegroup.co.uk or call on +44(0)1723 584250