DATA SECURITY POLICY

CONTENTS

1. PURPOSE 2
2. SCOPE 2
3. POLICY STATEMENT 2
   - Physical security 2
   - Application security 2
   - Application Architecture 2
   - Application Engineering and Development 3
   - Quality Assurance 3
   - Data Security 3
   - Data Deletion 3
   - Operational Security 4
   - Network Security 4
4. RESPONSIBILITIES 4
   - Regulatory Compliance 4
   - Reporting issues and threats 5
   - Records management 5
5. TERMS AND DEFINITIONS 5
6. RELATED LEGISLATION AND DOCUMENTS 6
7. FEEDBACK AND SUGGESTIONS 6
8. APPROVAL AND REVIEW DETAILS 6

1. PURPOSE

This policy establishes an effective, accountable and transparent framework for ensuring high standards of data security at The Canterbury Auction Galleries (CAG).

2. SCOPE

This policy applies across all entities or subsidiaries owned, controlled, or operated by CAG and to all employees, including part-time, temporary, or contract employees.

3. POLICY STATEMENT

Physical security

The CAG office is under 24x7 security protection, at both premises level and floor level to ensure only authorized individuals have access to the building and the CAG office. At the premises level, the building's perimeter is secured by barriers and alarms. At the floor levels, smart tag readers are present to authorize individuals before entry. Employees are granted access to the office only after authorization using smart tags. Critical locations in the office are accessible only to authorized individuals.

Important documents are stored in cabinets that can only be accessed by pre-authorized individuals. The office is equipped with surveillance cameras and their footage is monitored periodically by authorized individuals. Fire alarms are in place to detect and mitigate damage in the unlikely event of a fire. Regular fire drills are also conducted by the premises management team to educate employees about emergency evacuation procedures. A policy has been implemented to approve and regulate visitor access to the building. The office is provided with 24x7 power supply, supported by an alternative IT uninterrupted power supply system to ensure smooth functioning in the event of power failure.

CAG hosts its application and data with industry-leading suppliers, whose data centers have been thoroughly tested for security, availability and business continuity and or by house servers located in a strongroom environment at our premises.

Application security

The infrastructure for databases and application servers is managed and maintained by in house..

At CAG, we take a multifaceted approach to application security, to ensure everything from engineering to deployment, including architecture and quality assurance processes complies with our highest standards of security.

Application Architecture

The application is initially protected by a recognised in house' firewall which is equipped to counter regular DDoS attacks and other network related intrusions. The second layer of protection is our own own application firewall which monitors against offending IPs, users and spam. While the application can be accessed only by users with valid credentials, it should be noted that security in cloud-based products is a shared responsibility between the company and the businesses who own those accounts on the cloud. In addition to making it easy for administrators to enforce industry-standard password policies on users, our applications also incorporate features aimed at securing business data on the cloud:

- Configuring secure socket connections to portals;
- Leveraging SAML and custom single sign-on;
- Whitelisting IPs for exclusive access;
- Identity management via Google and Facebook credentials;
- Custom email servers, etc.;
- It should be noted that all account passwords that are stored in the application are one-way hashed and salted.

CAG uses a multi-tenant data model to host all its applications. Each application is serviced from an in house server and each customer is uniquely identified by a tenant ID. The application is engineered and verified to ensure that it always fetches data only for the logged-in tenant. Per this design, no customer has access to another customer's data. Access to the application by the CAG development team is also controlled, managed and audited. Access to the application and the infrastructure are logged for subsequent audits.

The in-line email attachment URLs for the product are public by design, to enable us to embed links within the email for end-user ease. This can be made private on customer request.

Application Engineering and Development

Our engineers are trained in industry-leading secure coding standards and guidelines to ensure our products are developed with security considerations from the ground-up. A security review is a mandatory part of application engineering process at CAG. The security review leverages static code analysis tools, in addition to manual reviews, to ensure adherence to our highest standards.

Quality Assurance

Besides functional validation and verification, the quality assurance process at CAG also subjects application updates to a thorough security validation. The validation process is performed by a dedicated app security team with whose goal is to discover and demonstrate vulnerabilities in the application. An update to the application does not get the stamp of approval from the team if vulnerabilities (that can compromise either the application or data) are identified.

Data Security

CAG takes the protection and security of its customers' data very seriously. CAG manages the security of its application and customers' data. However, provisioning and access management of individual accounts is at the discretion of individual business owners.

The CAG development team has no access to data on production servers. Changes to the application, infrastructure, web content and deployment processes are documented extensively as part of an internal change control process.

Our products collect limited information about customers - name, email address and phone - which are retained for account creation. Postal address is requested and retained by CAG PCI compliant payment processor for billing, along with the date of expiry of credit card and CVV.

CAG takes the integrity and protection of customers' data very seriously. We maintain history of two kinds of data: application logs from the system, and application and customers' data. All data is stored in Cloud Services' state of the art cloud computing platform. Backups are taken every five minutes at multiple locations.

Application logs are maintained for a duration of 90 days. Customers' data is backed up in two ways:

1. A continuous backup is maintained in different locations to support a system failover if it were to occur in the primary data centre. Should an unlikely catastrophe occur in one of the data centres, businesses would lose only five minutes of data.

2. Data is backed up to persistent storage every day and retained for a minimum of the last seven days.

The data at rest is encrypted using AES 256bit standards (key strength - 1024). All data in transit is encrypted using FIPS-140-2 standard encryption over a secure socket connection for all accounts hosted by Cloud Services. For accounts hosted on independent domains, an option to enable a secure socket connection is available.

Different environments are in use for development and testing purposes, access to systems are strictly managed, based on the principles of need to do/know basis appropriate to the information classification, with Segregation of Duties built in, and reviewed on a quarterly basis.

Data Deletion

When an account is deleted, all associated data is destroyed within 14 business days.

Operational Security

CAG understands that formal procedures, controls and well-defined responsibilities need to be in place to ensure continued data security and integrity. The company has clear change management processes, logging and monitoring procedures, and fall back mechanisms which have been set up as part of its operational security directives.

Operational security starts right from recruiting staff to auditing their work products. All employees are provided with adequate training about the information security policies of the company and are required to sign that they have read and understood the company's security-related policies. Confidential information about the company is available for access only to select authorized CAG employees.

Employees are required to report any observed suspicious activities or threats. CAG takes appropriate disciplinary action against employees who violate organizational security policies. Security incidents (breaches and potential vulnerabilities) can be reported by customers via email: dpo@tcag.co.uk.

CAG utilises only authorized and licensed software products. Experienced Third party contractors manage software or information facilities, and no development activity is outsourced other than to our subsidiary IT company (Scarlet Technology). All employee information systems are authorized by the management before they are installed or put to use.

In order to test the resilience of the hosted application, the company employs an external security consultant who perform security tests. This can be conducted in an architecturally equivalent copy of the system with no actual customer data present. The production system is never subject to such tests. Should an individual attempt such a test in the production environment, it will be detected as an intrusion, and the source IP will be blocked. An alert will then be raised so engineers can attend to the incident.

The company has a *Data Protection Policy*, approved by the Board of Directors.

Network Security

Network security is discussed in detail in this section from the perspective of the development centre, and the network where the application is hosted.

The CAG office network where updates are, deployed, monitored and managed is secured by industry-grade firewalls and antivirus software, to protect internal information systems from intrusion and to provide active alerts in the event of a threat or an incident. Firewall logs are stored and reviewed periodically. Access to the production environment is via SSH and remote access is possible only via the office network and encrypted VPN. Audit logs are generated for each remote user session and reviewed. Also, the access to production systems are always through a multi-factor authentication mechanism.

Somed CAG products are hosted in Cloud Services, with security managed by Cloud Services. Our team monitors the infrastructure 24x7 for stability, intrusions and spam using a dedicated alert system. The CAG applications have an in-built spam protection system for businesses that use it, while our team monitors and blocks individual accounts and IP addresses which attempt to access the CAG applications.

4. RESPONSIBILITIES

Regulatory Compliance

All formal processes and security standards at CAG are designed to meet regulations at the industry, state and European Union levels.

Use of our service by customers in the European Economic Area ("EEA"), will include the processing of information relating to their customers. In providing our service, we do not own, control or direct the use of the information stored or processed on our platform at the direction of our customers, and in fact we are largely unaware of what information is being stored on our platform and only access such information as reasonably necessary to provide the service (including to respond to support requests), as otherwise authorized by our customers or as required by law. We are Data Processors for our end customers, but Data Controllers for the customers from whom we collect data on our platform for purposes of the European Union

("EU") on our platform for purposes of the European Union ("EU") General Data Protection Regulation (GDPR). Our EEA based customers, who control their customer data and send it to CAG for processing, are the "Controllers" of that data and are responsible for compliance with the GDPR. In particular, CAG customers are responsible for complying with the GDPR and relevant data protection legislation in the relevant EEA member state before sending personal information to CAG for processing.

As the processors of personal information on behalf of our customers, we follow their instructions with respect to the information they control to the extent consistent with the functionality of our service. In doing so, we implement industry standard security, technical, physical and administrative measures against unauthorized processing of such information and against loss, destruction of, or damage to, personal information as more fully described in CAG's Data Protection Policy.

We work with our customers to help them provide notice to their customers concerning the purpose for which personal information is collected and sign Standard Data Processor Agreement (for data processors) with them to legitimize transfers of personal data from EU to processors established in third countries as may be required under the GDPR.

Reporting issues and threats

If you have found any issues or flaws impacting the data security or privacy of CAG users, please write to dpo@tcag.co.uk with the relevant information so we can get working on it right away.

Your request will be looked into immediately. We might ask for your guidance in identifying or replicating the issue and understanding any means to resolving the threat right away. Please be clear and specific about any information you give us. We deeply appreciate your help in detecting and fixing flaws in CAG, and will acknowledge your contribution to the world once the threat is resolved.

Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic or paper form in a recognised record keeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 6 years.

5. TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

6. RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Information Commissioners Office (ICO)
- The Canterbury Auction Galleries (CAG) Data Protection Policy

7. FEEDBACK AND SUGGESTIONS

7.1. CAG employees may provide feedback and suggestions about this document by speaking to their line manager.

8. APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	The Directors
Data Protection Officer	David Parker
Next Review Date	26/05/2024

Approval and Amendment History	Details
Original Approval Authority and Date	The Directors 26/05/2018
Amendment Authority and Date	