ANCIENT HOUSE
PRINTING GROUP
Web & Sheet-Fed Printers

DATA SECURITY POLICY

CONTENTS

1 PURPOSE

This policy establishes an effective, accountable and transparent framework for ensuring high standards of data security at Ancient House Press Plc.

2 SCOPE

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

3 POLICY STATEMENT

Physical security

The Ancient House Press Plc 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 Ancient House Press Plc office. Staff are on site from 6pm on Sunday to 6pm Saturday as part of the normal working week. At the premises level, the building's perimeter is secured by gates and fences. At the floor level, alarm systems, locked gates, access control door locks and grilled windows are present to prevent unauthorised entry. Employees are granted access to the premises through controlled access door way and all staff are encouraged to challenge anyone not clearly identified or accompanied in their visit whilst on site. Critical locations in the office are accessible only to authorized individuals. CCTV is in operation at all times inside and outside the building. A monitored burglar alarm system is in place and active when staff are not on site.

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. Trained Fire Wardens are in place to activate evacuation and safe exit from the buildings. 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 uninterrupted power supply system to ensure smooth functioning and shut down of critical systems in the event of power failure. Emergency lighting is regularly maintained and inspected.

Ancient House Press Plc hosts its application and data locally and backs up to a Data Centre, whose premises and operations have been thoroughly tested for security, availability and business continuity.

Application security

All of Ancient House Press Plc's applications are hosted locally on premises. The infrastructure for databases and application servers is managed and maintained by a secure and established Support Service Company well known to Ancient House Press Plc and closely monitored by Ancient House Press Plc senior Staff. Regular reviews of systems and protocols takes place between the parties. Data security is a prominent part of this review.

At Ancient House Press Plc, we take a multifaceted approach to application security, to ensure everything from setup to deployment, including architecture and quality assurance processes, comply with our highest standards of security.

Application Architecture

The application is initially protected by the local Firewall which is equipped to counter regular DDoS (Distributed Denial of Service) attacks and other network related intrusions. A second layer is the mail filtering anti-spam/antivirus interception process that all mail is filtered through before it get to our servers. A third layer of protection is the application protection software which monitors against offending IPs, users and spam on site. The applications can be accessed only by users with valid credentials. 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:

- Configuring secure socket connections to portals;
- Leveraging SAML (Security Assertion Markup Language) and custom single sign-on;
- Whitelisting IPs for exclusive access;
- Custom email servers, etc.;
- It should be noted that all account passwords that are stored in the application are one-way hashed and salted.

Ancient House Press Plc uses established and robust software for its business applications. This software runs on locally based servers. User ID’s and passwords are maintained by software Administrators and Network Administrators. Each application is serviced from an individual log-in and each user 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 according to their access rights. Per this design, no User has access to another User’s data. Access to the application by the Ancient House Press Plc Administration 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

Ancient House Press Plc Staff are not trained in secure coding standards and guidelines as they do not need to be so but the Company relies upon the application Vendor staff who are, to ensure our software is developed with security considerations from the ground-up. Vendor security review is a part of the application development process at Ancient House Press Plc.

Quality Assurance

All application updates are subjected to functional validation and verification by testing in a separate environment before releasing and applying the update to “live” data. Ancient House Press Plc relies upon the integrity and professionalism of third party vendors to ensure they deliver secure software in the application updates provided and regularly seek assurances in confirmation of this. An update to the application does not get the stamp of approval from the quality assurance team if vulnerabilities (that can compromise either the application or data) are identified.

Data Security

Ancient House Press Plc takes the protection and security of its customers’ data very seriously. Ancient House Press Plc manages the security of its applications and contact’s data. However, provisioning and access management at the contact’s site of individual business partners is at the discretion of individual business owners.

Our software collects limited information about customers - name, email address and phone - which are retained for account creation. Postal address and secondary contact information is requested and retained by Ancient House Press Plc. PCI compliant payment processor for billing, along with the date of expiry of credit card and CVV are not stored at the present time as these forms of payment are not accepted by Ancient House Press Plc systems. We store payment details for suppliers, for payment of invoices, and employees, for payment of wages, salaries and expenses, within secure software and in paper form. Supplier invoices and statements commonly contain banking information. These are processed through our approval systems on a daily basis and stored in a secure area after processing. Paper versions of Employee details are retained within secure locked storage with limited access at all times.

Ancient House Press Plc takes the integrity and protection of data very seriously. We maintain history of two kinds of data: application logs from the system, and application and contact data. All data is stored in on-site servers. Backups are taken every 5 minutes locally and at regular intervals offsite to a secure Data Centre. Daily physical media backups are also taken and stored off site.

Application logs are maintained for a duration of 90 days.

Contact data is backed up in two ways:

1. A continuous backup is maintained locally to support a system failover if it were to occur in the primary server function.
2. Data is backed up to persistent storage every day and retained for the last seven days.

The data at rest is encrypted using AES 256bit standards (key strength - 1024).

Access to systems are strictly managed, based on the principles of need to do/know basis appropriate to the information classification.

Data Deletion

When data is deleted, all associated data is destroyed within 14 business days. Ancient House Press Plc products also offer data export options which businesses can use if they want a backup of their data before deletion.

Operational Security

Ancient House Press Plc understands that formal procedures, controls and well-defined responsibilities need to be in place to ensure continued data security and integrity.

Operational security starts right from recruiting a member of staff to training and auditing their work products. The recruitment process includes standard background verification checks (including verification of academic records) on all new recruits. 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 Ancient House Press Plc employees.

Employees are required to report any observed suspicious activities or threats. The human resources team takes appropriate disciplinary action against employees who violate organizational security policies. Security incidents (breaches and potential vulnerabilities) can be reported by contacts by email to security@ancienthouse.co.uk or by phone to the usual number.

Ancient House Press Plc maintains an inventory of all information systems used by employees aided by automated software that assists in tracking changes to these systems and their configurations. Only authorized and licensed software products can be installed by employees and only authorized staff can install them in accordance with their network credentials. Third parties or contractors manage software or information facilities by proxy under authorized activities. 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 and additional ethical hackers who perform penetration tests. This is always 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 network where the application is hosted.

The Ancient House Press Plc office network where updates are developed, deployed, monitored and managed is secured by an industry-grade firewall 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 (Secure Socket Shell) and remote access is possible only via the office network. 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.

All Ancient House Press Plc products are hosted locally, with security managed by the Ancient House senior management team and authorized external Support. We monitor the infrastructure 24x7 for stability, intrusions and spam using a dedicated alert system. Every twelve months, end-to-end vulnerability assessments and penetration tests are performed. The Ancient House Press Plc network has a spam protection system while staff and Support will block individual accounts and IP addresses which attempt to access the Ancient House Press Plc applications or to inflict malicious harm.

4 RESPONSIBILITIES

Regulatory Compliance

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

We are Data Controllers for the Contacts from whom we collect data 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 Ancient House Press Plc for processing, are the “Controllers” of that data and are responsible for compliance with the GDPR. In particular, Ancient House Press Plc customers are responsible for complying with the GDPR and relevant data protection legislation in the relevant EEA member state before sending personal information to Ancient House Press Plc 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 Ancient House Press Plc’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 Ancient House Press Plc users, please write to security@ancienthouse.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 Ancient House Press Plc processes, and will acknowledge your contribution once the threat is resolved.

Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised Ancient House Press Plc recordkeeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 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)

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf

- Ancient House Press Plc Data Protection Policy

7 FEEDBACK AND SUGGESTIONS

7.1 Ancient House Press Plc employees may provide feedback and suggestions about this document by emailing gdpr@ancienthouse.co.uk

8 APPROVAL AND REVIEW DETAILS

Approval and Review	**Details**
Approval Authority	Managing Director
Data Protection Officer	Micheal Underdown
Next Review Date	30/04/2021

Approval and Amendment History	**Details**
Original Approval Authority and Date	Managing Director Micheal Underdown 01/05/2018
Amendment Authority and Date	