TECHNICAL AND ORGANIZATIONAL MEASURES

1. Organization of Information Security

1.1 This document describes HautAI's approach to information security and privacy. HautAI's Head of Product is responsible for the organization of information security and implementation of technical and organizational measures. These technical and organizational measures are subject to an annual review.

1.2 An ISMS (Information Security Management System) is established to evaluate data processing risks and security, to manage the assessment and treatment of these risks and to continually improve information security.

2. Human Resource Security

2.1 HautAI's personnel assigned to the services shall be subject to a standard screening process for new employees, to the extent permissible under applicable law.

2.2 HautAI's personnel that are relevant to the service regularly receive formal information security and data protection training.

3. Employee & Third Party Confidentiality

3.1 Except as otherwise required by law or contract, Haut.AI must ensure that all employees and third parties are bound by a confidentiality obligation in writing.

4. Data Security and Access Control

4.1 HautAI applies security procedures and encryption measures to data in transit and at rest in accordance with best industry practice to guard against the loss, destruction, corruption or alteration of data.

4.2 Business continuity and disaster recovery measures, such as using backup services, monitoring for failures, and maintaining incident response procedures, are established and implemented.

4.3 HautAI ensures that all transfers of data between HautAI, its customers and any other authorized third party are only communicated over secure channels.

4.4 Usernames and passwords supplied by HautAI for the purpose of accessing any HautAI system, product or any part of its network are provided for the sole use of one specific individual and must not be shared or divulged to any other person. HautAI implements measures to restrict the sharing of usernames and passwords.

4.5 Passwords used to protect access to HautAI's systems or customer data must be strong in line with industry best practice, regularly changed (at least every 90 days) and maintained in such a manner that they are kept confidential and not easily predicted. Single Sign-On (SSO) and Two-Factor Authentication (2FA) methods are implemented. Access controls are implemented to ensure that only authorized employees are granted access to pertinent information. Access rights are reviewed annually.

4.6 HautAI must not copy, download or store the customer data onto any desktop, laptop, server or other device at HautAI's premises or in HautAI's possession other than those approved by the customer for the provision of the services.

4.7 Data processing is conducted using cloud infrastructure services provided by third-party service providers. Detailed description of security measures applied by the third-party services provider is available at: https://cloud.google.com/docs/security/overview/whitepaper.

4.8 Equipment and data storage media disposal is conducted securely in accordance with industry best practice.

6. Communications and Operations

6.1 HautAI must, in accordance with best industry practice, maintain appropriate physical and logical security over the network and throughout its infrastructure.

6.2 HautAI is responsible for ensuring that neither it nor its personnel corrupt or erase any customer data stored on the customer's systems or networks used for service provision.

6.3 All of customer's confidential information in HautAI's (including its subcontractors) possession, including back-ups, laptop devices, desktop systems and customer's data transferred over the internet or any other network infrastructure, must be encrypted using industry standard encryption algorithms. The Supplier must keep encryption keys confidential and secure and only available to those personnel requiring them for the purpose of providing the Services.

6.4 Except as may be required for the provision of the services or as otherwise agreed, HautAI may not store customer data on any mobile device, storage or any portable media type. To the extent HautAI stores customer data as permitted hereunder, it shall ensure that such data is encrypted using industry standard encryption algorithms.

6.5 Any wireless network used by HautAI in connection with the services must be secured to industry standard(s) and at least to a WPA2 encryption standard and kept secure from unauthorised access.

6.6 HautAI must promptly create or obtain from the appropriate third party any necessary security patch(es) and promptly apply such patch(es). HautAI must keep records of any patches applied. For the avoidance of doubt, any software patch that is classified as critical must be applied within 72 hours of release with all other patches being applied within 14 calendar days of release.

7. Systems Development

7.1 The development of application or system software must be kept separate (logical separation at the minimum) from the production environment. Production systems shall not depend on a development infrastructure.

7.2 All development work undertaken and code changes made must be application security tested by HautAI using well-known application and vulnerability testing tools before release to ensure it is not susceptible to the following common exploits (but not limited to):

i. Injection
ii. Cross-Site Scripting (XSS)
iii. Broken Authentication and Session Management
iv. Insecure Direct Object References
v. Cross-Site Request Forgery
vi. Security Misconfiguration
vii. Insecure Cryptographic Storage
viii. Failure to restrict URL Access
ix. Insufficient Transport Layer Protection
x. Unvalidated Redirects and Forwards

7.3 Passwords must be stored and transmitted in an encrypted format at all times.

7.4 All authentications between the user and the application must be over HTTPS, SSH or VPN using strong cryptographic measures. Any publication of customer data through web pages of the site must be similarly secured using HTTPS and SSL certificates.

7.5 Any HTTP request must be automatically redirected to the HTTPS version of the content.

7.6 SSL certificates must be from a trusted authority, have the right hostname and must be configured to mitigate denial of service attacks. Anonymous or Weak SSL ciphers or hash and SSL protocols with weaknesses must not be used.

7.7 Usernames and passwords must not be hard-coded in application or stored in cookies or temporary files.

7.8 All backup files and temporary files must not be available over web servers. Files which should remain secure must be placed outside the realm of publicly exposed directories. Only the required system services shall be running on the servers providing the service.

7.9 Any session tokens must be user-unique, non-predictable, resistant to reverse-engineering, or be tied to a specific HTTP client instance to prevent hijacking and replay attacks. Session tokens must also expire at session termination or within a reasonable time of session idle timeout. Session token algorithms must never be based on, or use as variables, any user personal information (account number, name, registration details, etc.).

7.10 Any remote access to the system for administration/support purposes must be via secure means.

7.11 Unused services, ports and development kits/tools must be disabled from all internet-facing servers.

7.12 Admin interfaces must not be available to the entire internet address range. All administrative interfaces for the application must be limited to a range of addresses and changed from the default directory. File names must be renamed to names different to the default values so as to limit the opportunity for opportunistic attempts to gain administrative access.

7.13 All databases, irrespective of whether production, staging or development, that contain any customer data must be encrypted to industry standards. All backups of these databases and any backup containing customer data must also be encrypted.

7.14 All communications between any database, application and web server must be encrypted using strong encryption. Events are logged and monitored for security incidents.

7.15 Permissions must be correctly assigned, and users must not be able to traverse directories or access default directories that they do not need access in order to utilize the application.

7.16 Database servers must not be located in the same network segment as web servers and must never be internet-facing. There must be a separation between web servers and database servers.

7.17 Testing must not take place on production servers.

8. Vulnerability Testing

8.1 HautAI performs vulnerability scanning and penetration testing no less frequently than annually and appropriately addresses the issues raised by the tests.

8.2 HautAI performs regular and periodic security tests against all applications and code in order to ensure that they are secure from any new exploits or vulnerabilities.

9. Information Security Incident Management

9.1 HautAI has established a procedure for reporting security breaches. This includes astandardized approach to managing, responding to, and monitoring detected or suspected security incidents.