Huis Technologies Cyber Security Policy

Date: 15/10/2024

Review date: 31/10/2025

1. Purpose

The purpose of this cybersecurity policy is to establish which guidelines and procedures we are using to safeguard the confidentiality, integrity, and availability of information within software systems designed by Huis Technologies Ltd and operated by Huis Technologies Ltd staff. This policy aims to protect against unauthorised access, data breaches, and other cybersecurity threats. We understand that our clients work with vulnerable children, young people, and families and that the security of that information in these settings is paramount.

This policy is reviewed and updated annually and when changes are made to our systems or devices. Policy updates are reviewed and implemented by the Managing Director and Technical Director. Dates for the next planned review are detailed at the top of this policy.

2. Information Classification

Information is processed by software systems supplied by Huis Technologies Ltd to our clients. Client information is also stored on systems used by Huis Technologies Ltd which are also covered under this policy.

Our cyber security policy applies to the following data classifications:

Information classification	Sensitivity of information & access controls
Public: Information that is intended for public consumption.	No confidentiality concerns, and its disclosure does not harm the organisation or its stakeholders.
Internal Use Only: Information meant for internal use within the organisation.	Access is restricted to employees and authorised personnel.
Confidential: Sensitive information that, if disclosed, could harm the organisation or its stakeholders.	Access is limited to individuals with a specific need-to-know (directors only).

Restricted: Highly sensitive data requiring strict access controls.	Access is restricted to a specific group of individuals, typically on a need-to-know basis. Safeguarding information is classified in this way, for example. Access to safeguarding information has mandatory MFA.
Personal Identifiable Information: Information that can be used to identify an individual. Examples include names, dates of birth, addresses, and contact details.	Subject to access controls due to the potential risk of identity theft as well as the potential harm caused by making personal information public. Password protected in all systems. MFA on request.
Financial information: Information related to financial transactions, account details, and payment card information.	Subject to strict security measures due to the risk of financial fraud. No financial details are held directly by Huis Technologies. We do not process payments. Our own financial information (invoicing etc) is password protected via Xero.
Health information: Sensitive personal health information held by organisations who collect and/or store data on behalf of the NHS or private healthcare. Includes medical records, patient information, and health-related data.	Health records kept for medical reasons by other organisations (such as education and social care). Password protected documentation held securely on a cloud-based platform. Access to health information has mandatory MFA.
Proprietary information / intellectual property: Information critical to the organisation's competitiveness. Includes trade secrets, proprietary algorithms, and intellectual property.	Information highly sensitive to the organisation (ourselves or our client) is kept on a separate internal system and can only be accessed by Huis Technologies employees with sufficient permissions.
Legal/compliance information: Data subject to specific legal or compliance requirements. Includes contracts, legal documents, and compliance-related records.	Often considered highly sensitive due to its strategic importance. Password protected and held securely on a cloud-based platform.
Research and development: Information related to ongoing research, development, or innovation.	Often considered highly sensitive due to its strategic importance. Password protected and held securely on a cloud-based platform.
Customer/ client information: Information about customers, including preferences, purchase history, and communication records.	Requires protection due to privacy and trust considerations. Password protected and held securely on a cloud-based platform.
Unclassified information: Data that doesn't fit into specific classified categories	Still subject to general security practices but may not have stringent controls.

3. Inventory/ registers:

3.1 We keep an asset register. It is kept up to date to ensure that we understand which devices fall under the scope of this policy (usually because they contain information about clients of Huis Technologies Ltd as well as information about those whose data our clients process and hold).

3.2 We operate using virtual servers. Our data is stored and protected via AWS in the UK and Republic of Ireland. We do not operate at VLAN (Virtual Local Area Network) that devices connect to.

3.3 We do not operate using thin clients. Our devices are all designated as “fat client”.

3.4 We keep a register of all software and firmware used within Huis Technologies Ltd; this register details which items are supported. Unsupported or unused software is removed from devices as soon as it becomes redundant and/or unsupported. Access to Huis Technologies systems is available to staff via web browser (Google Chrome) on Windows PCs.

3.5 A firewall is in place on our internet router and the routers used by all staff working from home. A full list of routers is kept as part of our asset register and firewall passwords are regularly changed by staff working from home and a record is kept on the register. A process for password updating/changing is in place.

3.6 Mobile devices used by Huis Technologies Ltd staff are set with a locking mechanism to prevent inappropriate access to software. Huis Technologies staff are required to use a pin number, a password, a face-scan, or a fingerprint to lock devices supplied by Huis Technologies Ltd. Staff are required to lock their personal mobile device using one of these mechanisms if they are using the device for the purposes of MFA or other work-related activities.

3.7 Auto-run and auto-play features are disabled in all devices owned by Huis Technologies Ltd or used by Huis Technologies Ltd staff. This is detailed on the register of devices.

4. Access Controls in our own software products:

4.1 We implement role-based access controls (RBAC) to ensure that users have the minimum necessary permissions for their roles. We regularly review and update user access permissions to reflect changes in job roles. We encourage and remind clients to regularly review and update user access permissions to reflect changes in job roles.

4.2 Users who leave Huis Technologies Ltd are removed immediately from our systems. We encourage our clients to remove users who have left their organisation immediately.

4.3 We provide guidance to clients/users of our systems to help them create strong, unique passwords per each individual user. This is part of the setup process for individual users.

4.4 Only “Administrators” (the most senior staff within organisations who use our software systems) can set and re-set passwords or enable/disable MFA. Default passwords can be

used once and users of our software systems are required to change a default password immediately after the first use to gain access.

4.4 All Huis Technologies Ltd devices are installed with malware which is updated regularly. Update logs are reviewed by the Technical Director.

4.5 All our devices are installed with antivirus software. All devices used by staff working from home are installed with malware which is updated regularly. Update logs are reviewed by the Technical Director.

5. Authentication and Authorisation within Huis Technologies Ltd:

5.1 We use strong, unique passwords to limit access to information within Huis Technologies Ltd. We turn off default passwords for all the devices and software we use. Guidance is provided to staff on how to create strong, unique passwords in line with Huis Technologies Ltd's comprehensive password policy; this includes how to avoid brute force password guessing attempts.

5.2 We use MFA on all external and internal cloud services software products used by Huis Technologies Ltd. We understand the shared responsibility security arrangement for cloud based services used within our organisation.

5.3 We encourage multi-factor authentication (MFA) for all users of software supplied by Huis Technologies Ltd. As a minimum, we require that clients processing data using our software that is classified as Restricted Information or Health Information is protected by MFA.

5.4 We restrict access to only authorised personnel based on job responsibilities.

5.5 Single sign on (SSO) is in use by Huis Technologies staff accessing Google applications including Mail, Calendar and Google Drive. SSO is not used for access to any other software.

6. Data Encryption:

6.1 We utilise encryption mechanisms for data both in transit and at rest.

6.2 We employ Transport Layer Security (TLS) for communication between the application and users. TLS is deployed by the email system used by Huis Technologies Ltd for outgoing mail.

6.3 Data stored on our servers is encrypted; data supplied to clients who migrate from a Huis Technologies Ltd software system is available via an encrypted link for viewing or downloading. This is password protected and made available for a limited period of time following termination. Data is ordinarily provided as an appropriate export file (such as a CSV file).

7. Software Development Security:

We implement a range of secure coding practices to minimise vulnerabilities in the development stages of our products.

7.1 We regularly update and patch software components, libraries, and dependencies. Our virtualisation software is licenced, updated and patched. Automatic updates on software are enabled - we do not use software that is not fully supported.

7.2 Extensive testing of new features and updates to new features takes place before rollout, with special care taken to features that include external email functionality.

7.3 Where internal and external email functionality forms part of an update to our systems, developer work is checked over by a minimum of two members of staff.

7.4 Mechanisms are in place to permit access to our software only to the people who need to access the products we supply for specific purposes. Our router is configured to allow access to an external IP address or range used by software suppliers (AWS, for example, who supply our Multi Factor Authentication) providing services to Huis Technologies Ltd. Open ports are limited and configured to two specific suppliers.

8. Security Awareness Training:

8.1 We conduct regular security awareness training for all employees to educate them about phishing threats, social engineering, and best security practices.

8.2 Staff are trained regularly so that they understand their responsibility to protect information and we are registered with the Information Commissioner's Office (ICO). Staff are kept up to date with current UK GDPR protocols and legislation through annual training and regular briefings.

8.3 Staff are aware of their role in maintaining the security of Huis Technologies Ltd software products. All staff are DBS checked annually to ensure that only appropriate persons have access to sensitive information.

8.4 Staff access to personally identifiable information is kept to a minimum. Huis Technologies staff access records only for the purposes of support, using an identification number (rather than a name) for each record in order to ensure that information about clients' service users is anonymous.

9. Incident Response Plan:

Our Incident Response Plan sets out the steps we will take in the event of a suspected or actual information breach. The plan sets out procedures for detecting, responding to, and recovering from security incidents.

9.1 In the event of a suspected breach, stakeholders will be notified in writing at the earliest possible time.

9.2 An internal investigation will take place in the event of a suspected breach.

9.3 If a breach has occurred, it will be reported to the Information Commissioner's Office (ICO) within 72 hours.

9.4 Copies of all reports and the ICO's response will be shared with those whose information has been subject to breach. Learning from any suspected or actual data breach will be included in upcoming training and development for Huis Technologies Ltd staff and a record of this will be made.

10. Data Backup and Recovery:

We store, process and manage all personal data and backups in the UK and Republic of Ireland. Our registered company is Huis Technologies Ltd, and our data is hosted by Amazon Web Services.

10.1 We regularly backup critical data and verify the integrity of backups.

10.2 We regularly test the restoration process to ensure data can be recovered in case of a loss or ransomware attack.

11. Third Party Security:

Huis Technologies Ltd takes no responsibility for the security of third party suppliers of hardware/ devices and telecoms/network products sourced directly by Huis Technologies clients. However we do make every effort to evaluate and monitor the security of third party suppliers used directly by Huis Technologies Ltd.

11.1 We will evaluate and monitor the security practices of third-party suppliers providing services directly to Huis Technologies Ltd. These include our hardware, hosting, internet and telecoms vendors and other software packages used by Huis Technologies staff.

11.2 We ensure that suppliers adhere to security standards and conduct regular security assessments.

11.3 We will make clients aware of any data breach reported by a third party supplier used by Huis Technologies Ltd, and will provide a copy of any resulting investigation should it be appropriate.

11.4 We do not integrate with third party systems and do not have a public API.

12. Monitoring and Logging:

We implement logging mechanisms to track user activities, system events, and security incidents. We regularly review logs to detect and respond to suspicious activities. Alerts are

set up to inform us of any suspicious activity, so that immediate action can be taken to limit the impact on our users and the data they process.

13. Physical Security:

We implement physical security controls to prevent unauthorised access to hardware or to paper files.

13.1 Paper files are kept to a minimum and those with personally identifiable information are kept in a locked cabinet.

13.2 All devices, including mobile telephones and laptops, are password protected. Laptops belonging to managers have additional security features including multi-factor authentication by fingerprint, retinal scan or code.

13.3 Our office building is locked and access is restricted to employees.

13.4 Our support team is UK based and we operate a hybrid working model with some staff in the office and others working from home. Staff take part in regular Cyber Security and GDPR training, and checks are carried out by the Technical Director to ensure staff compliance with this policy.

14. Compliance:

We ensure compliance with relevant data protection regulations and industry standards. We regularly review and update the cybersecurity policy to adapt to changes in regulations or technologies. We conduct regular cybersecurity audits to assess the effectiveness of security controls. We periodically review and update the cybersecurity policy to address emerging threats and technologies.

14.1 We are registered with the Information Commissioner's Office (ICO).

14.2 We are registered under the UK Government's Cyber Essentials programme our most recent accreditation was 15/10/2024.

15. Enforcement:

We encourage a culture of accountability and responsibility for maintaining cybersecurity. Part of this is about creating an environment where staff are able to be honest about their mistakes to ensure that lessons can be learned to prevent future mistakes. However, where security processes are not correctly followed, we have a clearly defined process for managing non-compliance with this policy which falls under the Huis Technologies Ltd disciplinary policy.

This cybersecurity policy serves as a framework to establish a secure environment for our cloud-based software applications as well as for general practices around data collection

and processing. It should be reviewed and updated regularly to address emerging threats and changes in the technology landscape. All employees are expected to adhere to these guidelines to ensure the ongoing security of Huis Technologies Ltd software applications and the protection of sensitive data.