Information Governance

WebChatBot.ai Information Security Policy

Version No: 1.0
Issue Date: July 2024

VERSION HISTORY

Version	Date Issued	Brief Summary of Change	Owner's Name
V1.0	July 2024	Document Created	Charlie Norton

Associated documentation:	**Legal Framework:** The Data Protection Act (1998), Copyright Designs & Patents Act (1988), Computer Misuse Act (1990), Health & Safety at Work Act (1974), Human Rights Act (1998) etc]
Appendices:	
Approved by:	Charlie Norton
Date:	4th July 2024

Review and consultation process:	Annually from review date above. To be Approved IAO/C-level
Responsibility for Implementation & Training:	Charlie Norton

HISTORY

Revisions:		
Date:	**Author:**	**Description:**

Distribution methods:	Email and induction

1. Introduction

This top-level information security policy is a key component of WebChatBot.ai's overall information security management framework.

2. Objectives, Aim and Scope

2.1. Objectives

The objectives of WebChatBot.ai's Information Security Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

2.2. Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by WebChatBot.ai by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day-to-day business.
- Protecting information assets under the control of the organisation.

2.3. Scope

This policy applies to all information, information systems, networks, applications, locations and users of WebChatBot.ai or supplied under contract to it.

3. Responsibilities for Information Security

3.1. Ultimate responsibility for information security rests with the Chief Executive, but on a day-to-day basis the directors shall be responsible for managing and implementing the policy and related procedures.

3.2. Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

3.3. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

3.4. The Information Security Policy shall be maintained, reviewed and updated by the CEO/IAO. This review shall take annually.

3.5. Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

3.6. Each member of staff shall be responsible for the operational security of the information systems they use.

3.7. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

3.8. Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

4. Legislation

4.1. WebChatBot.ai is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the company, who may be held personally accountable for any breaches of information security for which they may be held responsible. The company shall comply with the following legislation and other legislation as appropriate:

- General Data Protection Regulation (GDPR)
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001

5. Policy Framework

5.1. Management of Security

- At board level, responsibility for Information Security shall reside with the CEO/IAO

- The directors of the company shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

5.2. Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

5.3. Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

5.4. Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

5.5. Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

5.6. User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

5.7. Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

5.8. Passwords

Everyone in the company is required to use strong passwords and update them Monthly

5.9. 2FA/MFA

Two/multi factor authentication is required to be set up for all user logins where possible

5.10. Suppliers

AWS - UK based servers with Https Advanced Encryption Standard (AES) 256-bit encryption
Onedrive - UK based servers with Https Advanced Encryption Standard (AES) 256-bit encryption
Google - EU based servers with Https Advanced Encryption Standard (AES) 256-bit encryption
Slack
Rolustech – No customer identifiable data to be transmitted for processing

5.11. Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

5.12. Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

5.13. Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of the company's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

5.14. Information security events and weaknesses

All information security events and suspected weaknesses are to be reported to the CEO. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

5.15. Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the treat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the CEO. Users breaching this requirement may be subject to disciplinary action.

5.16. User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of a director before they may be used on the company systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary.

5.17. Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the CEO before they commence operation.

5.18. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the CEO.

5.19. Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the directors. Users shall not install software on the organisation's property without permission from the CEO. Users breaching this requirement may be subject to disciplinary action.

5.20. Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

6. Policy approved by:

Charlie Norton
Business Manager
WebChatBot.ai