The Cobwebb Information Security and Data Protection Policy

1. Introduction

The Cobwebb Information Security and Data Protection Policy sets out how Cobwebb and its delivery partners/suppliers manage and provide security to Cobwebb, our customers and their sensitive information.

It explains the responsibilities that various functions, roles and individuals have for ensuring the confidentiality, integrity (accuracy) and availability of information within our organisation.

Cobwebb fully supports and complies with the principles of the General Data Protection Regulation (GDPR) which are summarised below:
Personal data shall be:

A. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
B. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation');
C. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
D. accurate and, where necessary, kept up to date; ('accuracy');
E. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; 'storage limitation');
F. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Having an information security policy is government and industry best practice. It helps to prevent any events, accidental or malicious, which results in the unauthorised access or disclosure of electronic files, paper documents and online services, and to detect and recover from any breaches that do occur with due diligence and transparency.

The policy recognises how essential the reputation of Cobwebb is, and the damage that a breach could cause if not handled correctly.

The security policy and its compliance is mandatory for all members of staff employed by Cobwebb. It will also be a minimum compliance for contractors undertaking work for and on behalf of Cobwebb.

Client data stored is physically stored in a UK-based ISO 27001 and ISO 14001 certified data centre, operated by Google therefore any aspect relating to the physical location (i.e. security and utilities) of this Data Centre will not form part of the scope.

Cobwebb is committed to maintaining and developing an information systems infrastructure, which has an appropriate level of security and data protection.

The Cobwebb Directors have made a commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the information systems management. Our commitment includes activities such as ensuring that the proper resources are available to work on these systems and that all employees affected have the proper training, awareness, and competency.

Because the needs of our business change, we recognise that our management system must be continually changed and improved to meet our needs. To this effect, we aim to continually review and update our objectives and processes.

2. Purpose and Scope

Our approach aims to minimise our exposure to breaches through education and best practice, and to detect and recover from any breaches that do occur with due diligence and transparency.

This policy recognises how essential the reputation of Cobwebb is, and the damage that a breach could cause.

The purpose of this policy is:

- To bring to the attention of all staff the need to improve and maintain security of information systems, and to advise managers of the approach being adopted to achieve the appropriate level of security.
- To bring to the attention of all managers and staff, their responsibilities under the requirements of relevant legislation, including Data Protection and Human Rights legislation and guidance, and the importance of ensuring the confidentiality of personal and sensitive data.
- To minimise the risk of security breach and prosecution.
- To ensure business continuity plans are established, maintained, and tested.
- To ensure all personnel are trained on information security and are informed that compliance with the policy is mandatory.
- To ensure all breaches of information security and suspected weaknesses are reported and investigated.
- To ensure that the company complies with current legislation and EU Directives, meets its statutory obligations and observes standards of good practice.

This policy applies to:

- All aspects of cyber and information security, including the specification, design, development, installation, operation, connection, use and decommissioning of the systems, services and equipment used to store, process, transmit or receive information.

- All Cobwebb data, and any data that Cobwebb is processing for other data controllers.
- All Cobwebb employees - who should understand their responsibilities in using the company's information assets including its systems.
- Cobwebb staff engaged in designing and implementing new technology solutions, who must reflect the policy requirements into their design and build.
- Contracted suppliers that handle/access/process data. Contracted suppliers must provide the security measures and safeguards appropriate to the nature and use of the information. All Contracted suppliers of services to Cobwebb must comply, and be able to demonstrate compliance, with the company's relevant policies and standards.

3. Accountabilities

The Information Security Officer is the accountable owner of the Information Security and Data Protection Policy and is responsible for its maintenance and review in-conjunction with the Data Protection Officer.
Any exception to the Information Security and Data Protection Policy must be risk assessed and agreed by the Information Security Officer.
Delegation of responsibilities is outlined in detail in the Information Security Management Procedures.

4. Policy Statements

4.1. Responsibilities

All Employees must act with confidentiality by:

- familiarising themselves with this Policy, and all applicable supporting policies, procedures, standards and guidelines. Compliance with this Policy is mandatory, and any employee failing to comply may be subject to disciplinary procedures.
- complying with all appropriate legislation and all company policies, standards, procedures and guidelines.
- only accessing systems and information, including reports and paper documents to which they are authorised and for the purposes of carrying out their function in the company.
- using systems and information only for the purposes for which they have been authorised.
- not disclosing confidential information to anyone without the permission of the manager of the team(s) who are the information owners or to comply with a statutory duty.
- keeping their passwords secret, and not allow anyone else to use their account to gain access to any system or information.
- notifying their manager, or the Information Security Officer of any actual or suspected breach of Information Security, or of any perceived weakness in Cobwebb's security policies, procedures and practices or infrastructure.

- ensuring that where they are responsible for the management of third parties, the third parties are contractually obliged to comply with this Policy and that those third parties are aware that their failure to comply may lead to contract termination.
- not using non-Cobwebb email accounts (i.e., Gmail, Hotmail, Yahoo, AOL), or other external resources to conduct Cobwebb business, thereby ensuring that company business is never confused with personal business and data is always traceable within the corporate systems.

Senior Leadership Team (SLT) and Managers must:

- Ensure that their staff are fully conversant with this Policy and all associated policies, standards, procedures, guidelines and relevant legislation, and are aware of the consequences of non-compliance.
- Ensure recruits are trustworthy and appropriate employment checks have been carried out.
- Take appropriate disciplinary action in the event of misconduct, and non-compliance with security or data protection policies.
- Ensure Systems Integrity - data should be intact, accurate and complete, and IT systems must be kept operational
- Ensure Systems Availability - users should be able to access information or systems when needed
- Develop compliant procedures, processes and practices for use in their business areas.
- Notify the Information Security Officer of any suspected or actual breaches or perceived weaknesses of information security.
- Notify the Data Protection Officer of any suspected or actual data protection breaches

4.2. Legislation

All employees will comply with all current legislation. Laws relating to information security and data protection including those outlined below:

Data Protection Act 1998 and GDPR

At the heart of the GDPR is the concept that EU citizens will have a clearly defined set of rights regarding the use of their personal data. Personal information relating to identifiable individuals must be kept accurate and up to date. It must be fairly obtained and securely stored. Personal information may only be disclosed to people who are authorised to use it.

Copyright. Patents and Designs Act 1988

Documentation must be used strictly in accordance with current applicable copyright legislation, and software must be used in accordance with the licence restrictions. Unauthorised copies of documents or software may not be made under any circumstances.
Computer Misuse Act 1990
This Act addresses the following offences:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit or facilitate commission of further offences.

- Unauthorised modification of computer material.

Part 3 of The Employment Practices Code

Provides best practice guidance on monitoring of emails, phone calls and internet access in the context of the Data Protection Act.

EU Directive on Privacy and Electronic Communications (PECR)

Defines legal standards for the processing of personal data, and the protection of privacy in the electronic communications sector.

Human Rights Act 1998

Based on the European Convention on Human Rights.

4.3. Authority and access control policy

Cobwebb Tiered Security - Access to data is restricted so that only those who need to access the data can access the data. This is accomplished via Cobwebb Tiered Security

Users access company networks and servers via unique logins that demand authentication, including passwords, biometrics, ID cards, tokens or other . Access is monitored and recorded.

4.4. Data classification

The data that Cobwebb does need to store is classified so that only those who need to access the data can access the data.

See How to Classify and Handle Data
Cobwebb Tiered Security
How to look after Customer Property

4.5. Escalation

If an exposure to a breach of security or data protection is identified, it must be reported and escalated immediately. All staff must follow How to Respond to a Data Breach(1.0).

4.6. Risk Assessment

A risk assessment will be carried out by the Information Security Officer and/or Data Protection Officer for each reported breach of security. They must assess the risk of unauthorised access to information, software, and hardware and consider the risk in relation to each information technology resource and establish security controls and protection in relation to that risk. Risk must be assessed in relation to the following factors:

- Quality of the control mechanism
- Size of the threat
- Potential loss.

4.7. Business Continuity

Cobwebb are fully committed to our employees and clients and recognise the potential strategic, operational and financial risks associated with a business interruption and the importance of maintaining our services if an emergency occurred.

A Business Continuity Plan is in place which assesses the impact of the cause of the interruption to services and ultimately calls on a Disaster Recovery Plan to re-establish working systems.

For full details, see: How to continue the business after a catastrophe

Appendix

Existing Documents

Please note that some of these documents are internal to Cobwebb and anyone outside of the organisation will not be able to view them.

If you require any further information regarding any of the documents below please contact a member of the Cobwebb team who will be happy to assist.

- Cobwebb Security Policy
- #Notes - Cobwebb Password Security
- #Notes - Cybersecurity
- ICT Security Policy
- IT Equipment and Technology Policy
- Bring your own Device Policy
- Data Protection Policy - compliant with GDPR
- Whistleblowing Policy
- How to Make a GDPR Compliance Notification
- How to respond to a Customer Data Access /Delete Request (1.0)
- How to Respond to a Data Breach(1.0)
- How to look after Customer Property
- How to Classify and Handle Data
- How to continue the business after a catastrophe
- How to create a secure password
- How to minimise cyber risk
- How to Share Passwords with Third Parties (V1.0)
- Original Policy Source: Information Security and Data Protection Policy)
- Cobwebb Tiered Security
- Security Levels - The Cobwebb Circle of Trust