Information Security Policy

NOTE: *Please review and edit, or replace, this content as appropriate to meet the needs of your business. Note any places with content in square brackets [ ], are fill-in-the-blank sections. Please provide appropriate content between the [ ]'s before you save the template. Check to ensure the content of your saved policy is consistent with the* ***in-scope controls*** *you have associated with this policy.*

1. *For ISO 27001, all control topic sections are in-scope.*
2. *For SOC 2, all control topic sections are in-scope.*

Policy reviewer and updates: Ashish Mahendru
Policy owner and approver: Sachin Smotra
Last reviewed and updated: 05-MAR-2024
Last approval date: 06-MAR-2024

Foreword

As a leading provider of RAG as a Service to build GenAI applications using proprietary data, committed to mission of “Building LLM enabled applications” & vision of “Enabling every developer to build AI applications”, Dataworkz (“Company”) has an ethical, legal and professional duty to ensure that the information it holds conforms to the principles of confidentiality, integrity and availability. We must ensure that the information we hold or are responsible for is safeguarded where necessary against inappropriate disclosure, is accurate, timely and attributable, and is available to those who should be able to access it.

The Information Security Policy below provides the framework by which we take account of these principles. Its primary purpose is to enable all company employees and contractors to understand both their legal and ethical responsibilities concerning information, and empower them to collect, use, store and distribute it in appropriate ways.

This policy is the cornerstone of our ongoing commitment to enhance and clarify our information security and privacy procedures. It has senior leadership's full support and we encourage all employees and contractors to read it and abide by it in the course of their work.

Introduction

The confidentiality, integrity and availability of information are critical to the on-going functioning and good governance of the company. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for the company to recover from.

This information security policy outlines the company's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the company's information systems. Supporting policies, procedures and guidelines provide further details.

The company is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by adoption and enforcement in accordance with the requirements of SOC 2 Trust Service Criteria for Security.

Objectives

The objectives of this policy are to:

1. Make certain that users are aware of and comply with all current and relevant federal and (where appropriate) state legislation.
2. Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
3. Protect the company from liability or damage
4. Respond to changes in the context of the organization as appropriate, initiating a cycle of continuous improvement.

Scope

This policy is applicable to, and will be communicated to, all employees, members, other employees of the company and third parties who interact with information held by the company and the information systems used to store and process it.

Policy

Compliance, Policy Awareness and Disciplinary Procedures

1. Any security breach of the company's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data
2. The loss or breach of data may result in the loss of business, financial penalties or criminal or civil action against the company. Therefore it is crucial that all users of the company's information systems adhere to this Information Security Policy and its supporting policies as well as the Information Classification Standards.
3. All current employees, members and other authorized users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines.
4. Any security breach will be handled in accordance with all relevant the company policies

Information Classification and Handling

1. Information is classified according to an appropriate level of confidentiality, integrity and availability (see “Data Classification and Handling Policy”)
2. All users must handle information appropriately and in accordance with its classification level.

Customer Support and Agreements

The organization plans and prepares for managing customer support requests and reporting of security incidents by defining, establishing and communicating a formal process, to ensure quick, effective, consistent and orderly responses. A ticketing system is used to monitor, respond to and track customer support requests and incidents:

1. During onboarding, clients are "trained" and provided a link to submit requests and security incidents. A backup option is provided to submit an email directly to the ticketing system or internal customer care team opens a ticket.
2. Tickets are used to document and track ongoing status updates and communication related to ticket requests

Customer service agreements are established and documented to ensure that there is clear understanding between the organization and the customer regarding both parties’ obligations to fulfill relevant information security requirements. A cloud-based tool to manage, deploy and catalog signed agreements is used. Management ensures the standard customer service agreement template is kept up-to-date and includes:

1. Applicable standards, laws and regs
2. Defined service level agreements
3. Rules of Use (link to Terms of Use on website)
4. Defined confidentiality and security clauses with customer responsibilities

The company makes descriptions of its services, component systems, and their boundaries readily available to customers and other stakeholders via its website, product documentation, emails, and/or blog posts.

Incident Handling

1. If an employee or contractor of the company is aware of an information security incident then they must report it to the Help Desk at: security@dataworkz.io
2. All employees of the company Community must report instances of actual or suspected phishing to: security@dataworkz.io

Supporting Topic-specific Policies, Procedures and Guidelines

1. Supporting topic-specific policies have been developed to strengthen and reinforce this policy statement. These, along with associated procedures and guidelines are published together and are available on the company's internal website at: Security Policies
2. Operating procedures are documented and made available to all users who need them.
3. ***All employees, members and any third parties authorized to access the company's network or computing facilities are required to familiarize themselves with these supporting documents and to adhere to them in the working environment.***

Review and Development

1. This policy, and its topic-specific policies, shall be reviewed annually by the Security Committee and updated regularly to reflect any relevant changes to the applicable laws, organizational policies or contractual obligations.
2. Additional policy may be created to cover specific areas.
3. The Security Committee comprises of representatives from all relevant parts of the organization. It shall oversee this information security policy and topic-specific policies.
4. The Security Committee will determine the appropriate levels of security measures applied to all new information systems.

Document Control

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.

Distribution

This policy is to be distributed to all the company employees who manage, oversee or carry out any of the defined policy requirements within this Management Policy.

Version History

If you are reading a printed version of this document you must check Security Policies to ensure that you have the most up to date version.

Appendix A: Summary of Relevant Standards, Laws & Regulations

1. SOC 2 Type 2 - Trust Service Criteria - Security