Datasphere Solutions

INFORMATION SECURITY POLICY

Document version: 1.1

Date: October 10,2023

The policy for information security

1 Version Control

	Last Modified	Last Modified By	Document Changes
1.0	02.04.2022	Kumar (Information Security Officer)	Add new policies contents.

2 Table of Contents

3 Information Security Policy

3.1 Purpose

The main aim of this policy is to establish a complete framework of information security measures that are pertinent and suitable for our organization. The methods have been specifically devised to prioritize the protection of sensitive data by ensuring its confidentiality, integrity, and availability. The objective of implementing this measure is to establish a secure setting that safeguards our confidential data from unauthorized entry, manipulation, or interference. This ensures the continuity and reliability of our company activities. The dedication to maintaining information security is in accordance with established industry norms and recognized standards, such as ISO 27001. This emphasizes our steadfast commitment to safeguarding the confidentiality, integrity, and accessibility of data throughout all aspects of our organization.

3.2 Scope

The policy exhibits inclusivity by encompassing all individuals affiliated with the organization, such as employees, contractors, and third parties, who possess authorized access to the organization's significant information assets. The implementation of this strategy guarantees a standardized and consistent approach to information security among all stakeholders involved.

3.3 Principal

Successful management of information security relies on a few crucial criteria. These activities encompass doing thorough risk assessments to detect vulnerabilities, ensuring rigorous adherence to legal and regulatory duties, and aligning security measures with the larger objectives of the organization. This technique offers a methodical and proactive strategy for safeguarding sensitive data and upholding a secure environment that aligns with the organization's vision and objectives.

3.4 Chief Executives Statement of Commitment

The effective processing of information is crucial to the success of our organization, and safeguarding the confidentiality and integrity of this information is a top concern at the executive level. We prioritize our responsibilities under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, whether it pertains to employee or customer data. We have furnished the necessary resources to establish, execute, and consistently enhance the information security management system that aligns with our organizational operations.

3.5 Introduction

The domain of information security bears a significant duty, namely safeguarding entrusted information. Inadequate management of this critical element can lead to significant consequences for our employees, customers, public image, and financial position. An efficient information security management system serves as a protective measure against potential dangers, ensuring compliance with our legal, regulatory, and contractual responsibilities.

It is of utmost importance to prioritize the provision of quick access to pertinent data for authorized individuals. This enables our organization to operate with efficiency and fulfil operational requirements while upholding security measures. The delicate equilibrium between accessibility and security is paramount.

In the contemporary era characterized by the prevalence of data-driven practices, it is of utmost importance to prioritize compliance with the General Data Protection Regulation (GDPR). The implementation of this measure guarantees the protection of personal data, while also upholding the principles of privacy and individual rights. Our adherence to GDPR compliance not only ensures conformity to legal obligations, but also serves as a testament to our unwavering commitment to ethical and responsible management of data.

As custodians of data, we assume the ethical obligation to protect information and adhere to standards of data management. Our dedication to upholding integrity, confidentiality, and ethical data usage is essential in maintaining the trust bestowed upon us by our clients,

partners, and stakeholders. By following ethical rules and implementing best practices, organizations may safeguard their reputation and secure the long-term success of their organization in a contemporary landscape where information security holds utmost importance.

3.6 Information Security Objectives

In order to safeguard the confidentiality, integrity, and accessibility of organizational information, including personal data as defined by the General Data Protection Regulation (GDPR), it is imperative to adhere to sound risk management practices, legal and regulatory requirements, contractual duties, and business necessities.

The objective is to ensure the availability of necessary resources for the development, implementation, and ongoing enhancement of the information security management system.

In order to efficiently oversee external suppliers responsible for the processing, storage, or transmission of information, it is imperative to implement strategies aimed at mitigating and controlling information security threats.

The objective is to establish a culture centered around information security and data protection by means of comprehensive training and heightened awareness.

3.7 Information Security Defined

- **Confidentiality** - Confidentiality refers to the practice of limiting access to information only to persons who possess the necessary authorization and permissions, hence preventing any unauthorized disclosure. Using measures to ensure confidentiality, sensitive data is shielded from unauthorized disclosure.
- **Integrity** - refers to the state in which information is consistently upheld in a thorough and accurate manner, hence ensuring its alignment with the appropriate dataset. The implementation of this measure serves to mitigate the risks

associated with data corruption, tampering, and inaccuracies, so ensuring the integrity and credibility of our information assets.

- **Availability** - pertains to the requirement for information to be easily obtainable and promptly available when required. The assurance of data availability is crucial for maintaining uninterrupted business operations and facilitating efficient and effective service to our stakeholders.

3.8 Information Security Policy Framework

The foundation of the information security management system is established through the implementation of an information security policy framework. The policy framework is comprised of the following policies, which are implemented in accordance with this policy.

- DP 01 Data protection Policy
- DP 02 Data Retention Policy
- IS 01 Information Security Policy (this policy)
- IS 02 Access Control Policy
- IS 03 Asset Management Policy
- IS 04 Risk Management Policy
- IS 05 Information Classification and Handling Policy
- IS 06 Information Security Awareness and Training Policy
- IS 07 Acceptable Use Policy
- IS 08 Clear Desk and Clear Screen Policy
- IS 09 Mobile and Teleworking Policy
- IS 10 Business Continuity Policy
- IS 11 Backup Policy
- IS 12 Malware and Antivirus Policy
- IS 13 Change Management Policy
- IS 14 Third Party Supplier Security Policy
- IS 15 Continual Improvement Policy
- IS 16 Logging and Monitoring Policy
- IS 17 Network Security Management Policy

- IS 18 Information Transfer Policy
- IS 19 Secure Development Policy
- IS 20 Physical and Environmental Security Policy
- IS 21 Cryptographic Key Management Policy
- IS 22 Cryptographic Control and Encryption Policy
- IS 23 Document and Record Policy
- IS 24 Significant Incident Policy and Collection of Evidence
- IS 25 Patch Management Policy
- IS 26 Cloud Service Policy
- IS 27 Intellectual Property Rights Policy

3.9 Information Security Roles and Responsibilities

The responsibility for information security lies with all individuals, who are expected to possess a comprehensive awareness of the rules, diligently adhere to established processes, and promptly report any suspected or confirmed breaches. The paper titled "Information Security Roles Assigned and Responsibilities" outlines and documents the specific roles and responsibilities pertaining to the operation of the information security management system.

3.10 Monitroring

The effective implementation of information security policies and procedures is contingent upon vigilant supervision. The responsibility of overseeing this matter lies mostly with the Management Review Team, a specialized entity tasked with monitoring the compliance and efficacy of policies. The ongoing assessment and examination of our information security standards are crucial in sustaining their integrity.

In addition, regular audits are conducted both internally and outside. The audits conducted give thorough evaluations of our information security practices, providing useful insights into our adherence to policies, highlighting areas that require enhancement, and proving

our dedication to complying with industry standards. The collective endeavors ensure the durability and continuous improvement of our information security management system.

3.11 Legal and Regulatory Obligations

The organization demonstrates a strong dedication to fulfilling its legal and regulatory responsibilities by diligently documenting these duties in the Legal and Contractual Needs Register, thereby promoting transparency, compliance, and responsibility.

3.12 Training and awareness

3.12.1 Security Training

The personnel are provided with comprehensive training to ensure they possess the requisite knowledge and skills to effectively protect our valuable information assets. Employees are provided with customized security training that is specifically designed to meet the unique demands of their respective positions. The implementation of this focused strategy guarantees that each member of the team possesses a comprehensive understanding and the ability to properly execute security measures, hence diminishing vulnerabilities and mitigating risks.

3.12.2 Promotion of Security Awareness

Our organization actively fosters a pervasive culture of security awareness across all its domains. This level of awareness surpasses a mere adherence to policies and instead signifies a shared dedication to being vigilant and accountable. By means of continuous communication, training, and engagement, we enable our workers to assume the role of proactive protectors of our information security, so effectively bolstering our defenses against potential threats and vulnerabilities.

3.13 Continual Improvement of the Management System

The continuous improvement of the information security management system is emphasized. The company's continuing improvement policy outlines its approach to ongoing improvement, and a corresponding methodology for continual improvement is now implemented.

4 Policy Compliance

4.1 Compliance Measurement

4.1.1 Regular Audits

The maintenance of our strong information security practices is ensured through the implementation of planned security audits. The periodic assessments play a crucial role in evaluating the degree to which we comply with this policy. These audits are carried out by auditors who possess the necessary qualifications, and they thoroughly assess our security controls, processes, and practices in order to verify compliance. The audit findings offer significant insights on the efficacy of our security procedures, highlighting both areas of strength and opportunities for enhancement. By conducting regular audits, we actively monitor our security posture, promoting ongoing improvement and conformance with established standards and best practices.

4.1.2 Non-Compliance and Corrective Action

In the event of non-adherence to our security policy, we implement a prompt and systematic approach. Instances of non-compliance are swiftly addressed, with a primary focus on effectively resolving the underlying causes. Meticulously planned and executed corrective steps are implemented to address deficiencies, mitigate the risk of recurrence, and enhance our security posture. The adoption of a proactive approach guarantees the swift resolution of any policy deviations, thereby reducing potential vulnerabilities and reinforcing our dedication to achieving excellence in information security. The organization's commitment to maintaining the highest security standards is demonstrated by its prompt and thorough response to non-compliance matters.

4.2 Exceptions

To deviate from the established policy, it is necessary to obtain prior approval from the Information Security Manager and subsequently disclose the exception to the Management Review Team.

4.3 Non-Compliance

Employees found to be in violation of this policy may be subject to disciplinary measures, which could potentially result in termination of employment. This underscores the paramount need to comply with our information security protocols and the grave repercussions of neglect in protecting our organization's data and assets.

4.4 Continual Improvement

The policy is a fluid document that is subject to regular modifications and evaluations. The iterative approach mentioned is a crucial element of our dedication to perpetually enhancing information security. By continuously keeping up to date with emerging threats, advancements in technology, and industry best practices, we guarantee that our security measures retain their efficacy and remain in accordance with the dynamic nature of the information security domain.

5 Conclusion

The creation of an Information Security Policy document that adheres to the ISO 27001 standards represents a significant and forward-thinking step in strengthening our organization's information security stance. This statement represents the fundamental principle underlying our dedication to protecting our invaluable information resources. This policy serves to emphasize our commitment to safeguarding data and also comprehensively delineates our goals, offering a systematic framework for mitigating risks and coordinating responses to potential security events.

The present document exemplifies the capacity of our organization to adapt within the continuously changing domain of information security. Regular evaluations and revisions guarantee that it remains congruent with the ever-changing landscape of cyber risks and technological progress. By adhering to this policy, we engage in proactive measures to strengthen our defenses, cultivate a culture of security awareness, and uphold the trust and confidence of our stakeholders.

In essence, this study provides a comprehensive overview of the systematic procedure involved in formulating an Information Security Policy that conforms to ISO 27001 requirements, alongside the corresponding recommended methodologies. This policy serves as a crucial element in our ongoing efforts to uphold the integrity, confidentiality, and accessibility of our information assets, thereby strengthening the fundamental basis of trust on which our organization is established.