CLOUDLAYER

cl8

.com

Information Security Policy

Cloudlayer8

Friday, September 2, 2022

1. Introduction - Purpose

This document sets out the high-level policy for information security management for Cloudlayer8 (hereafter referred to as "Organization").

The Organization is committed to safeguarding the information systems upon which it depends in order to deliver services, both internally and externally. It has therefore devised and agreed this high-level policy for Information Security Management.

The Organization considers information as a valuable asset of utmost importance that needs to be secured in order to ensure reliable services to its stakeholders.

Furthermore, the Organization realizes that information security is an on-going practice of implementing the necessary processes and controls to protect the Organization's information which is crucial from possible risks that can adversely impact the Organization's operations.

This information security policy outlines the Organization's approach to information security management. The aim of this top-level policy is to provide the framework and describe the purpose and guiding principles and responsibilities to safeguard the security of the Organization's information systems.

This policy applies to the entire Information Security Management System (ISMS).

Users of this document are all employees of the Organization as well as relevant external parties, within the scope of the ISMS.

In this regard the Organization has adopted an Information Security Management System comprising of the Information Security Policies, Procedures and Processes to effectively manage the information security risks. This system is aligned with the ISO/IEC 27001:2013 standard.

2. Scope

This policy applies to the entirety of the Organization, including:

- All business locations and functions,
- All information that is stored or processed by the Organization (including that entrusted to the Organization by its clients, commercial partners and its employees) irrespective of the format in which it is stored or processed,
- All authorized Users, whether directly employed by the Organization, or engaged under contract to provide services to the Organization and / or its clients,

Within the broader scope described above, this Policy also establishes and empowers an ISMS that will be certified to the ISO 27001:2013 Standard. The scope of the certified ISMS is described in detail within the document ISMS Scope and Context.

3. Information Security Policy Statement

Information can exist in many forms, printed or written on paper, stored electronically, transmitted by post or by using electronic means, contained within documents, or spoken in conversation. The Organization also relies heavily on computer systems and applications to store, process and manage business and client information. Whatever form the information takes, or means by which it is shared or stored, it must always be appropriately protected. Information in any form is a valuable company asset and shall be treated as such.

Information security problems include information being inappropriately obtained, accessed or disclosed, altered or erroneously validated whether deliberate or accidental or being unavailable when required.

The Organization considers information as a valuable asset of outmost importance that needs to be secured in order to ensure reliable service delivery to its clients. It is therefore an objective for Organization to protect its information through an ongoing practice of implementing and monitoring appropriate controls to protect important information from possible risks that might adversely impact the Organization's business operations or reputation.

In this regard, the Organization has adopted an Information Security Management System (ISMS) comprising of policies, procedures and processes to effectively manage information security risks. The ISMS is aligned with the ISO/IEC 27001:2013 standard.

4. Managing Information Security

Management Commitment

The management of the Organization is committed to ensure that:

- The confidentiality of information is protected and prevent disclosure of valuable or sensitive information.
- The integrity of information is maintained to ensure its accuracy and completeness.
- The availability of information is maintained to meet organizational needs and stakeholder requirements and expectations.
- Regulatory and legislative requirements related to the Organization are met.
- Appropriate information security awareness is provided to all Users within the scope of the Organization's ISMS.
- An incident management process is established and implemented to ensure that all breaches of information security (actual or suspected) are reported and investigated.
- Risks are mitigated to an acceptable level through a risk management framework.
- The ISMS is continually improved.
- Appropriate resources are allocated in order to implement, operate and review an effective ISMS.

Objectives and Measurement

The Organization has envisioned its information security objectives to ensure its related business operations continue to be carried out securely in line with the ISO 27001:2013 standard. Primary information security objectives are as follows:

1) Achieve and maintain compliance with ISO/IEC 27001:2013,
2) Certify an ISMS to the ISO/IEC 27001:2013 standard, with an initial implementation scope based around the Organization's operations, as defined in the ISMS Context & Scope document,
3) Demonstrate Top Management support for Information Security,
4) Demonstrate Continual Improvement,
5) Maintain staff awareness of Information Security,

6) Ensure adequate ISMS Resources and Competence are assigned,
7) Improve Third Party Security,
8) Ensure effective IS Incident Reporting and Management,
9) Ensure effective IS Risk Management.

Detailed information security objectives and the related measurements are documented as part of ISMS Objectives and Effectiveness Measurement.

Continual Improvement

The Organization's management is committed to continual improvement of the ISMS. It is through continual improvement that the effectiveness of the ISMS and security controls will be maintained and improved. These processes are further described in the Continual Improvement Framework document.

KPIs shall be developed and used to measure the effectiveness of the ISMS and more appropriate security controls.

As part of the Management Review of the ISMS, Top Management shall ensure that feedback and improvement recommendations are provided by the Information Security Steering Committee.

As an outcome of the review, the potential improvements to the ISMS will be communicated to the Top Management.

5. Legal, and Regulatory Requirements and Contractual Obligations

All relevant statutory and regulatory requirements as well as contractual obligations shall be identified and complied with.

6. Security in Business Change and Project Management

The Organization acknowledges that the consideration of appropriate information security controls is most effective at the outset of any change within the business. Therefore, information security shall be considered throughout the project lifecycle, with the following specific measures being adhered to:

1) Project managers shall ensure that information security is addressed at all stages of project management, beginning with the project brief.
2) The Information Security Officer together with the Head of Department shall provide a security sign-off at the end of each stage and prior to the initiation and / or closing the project.
3) Risk assessments and security testing shall be conducted, as appropriate, before the project initiation, during the implementation stage and prior to closing the project.
4) Relevant information security requirements shall be included in Proposals, Requests for Proposal (RFP) or Requests for Information (RFI).
5) All External Parties such as suppliers, vendors, external partners, contractors etc. shall sign Non-Disclosure Agreements prior to project initiation.
6) All External Parties such as suppliers, vendors, external partners, contractors etc. shall sign Data Processing Agreements with the Organization whenever personal data is being processed by them on behalf of the Organization.

7. Periodic Reviews

In order to ensure the continued suitability, adequacy, and effectiveness of its information security framework the Organization shall ensure that reviews of this information security policy and related documents are performed at appropriate intervals and when significant changes occur to the Organization, or its information assets.

Reviews and updates shall be discussed during the Information Security Steering Committee's meetings and communicated to the Organization's Management for approval and sign off.

8. Policy Compliance

Compliance with this policy is mandatory for all internal and external Users. Compliance checks will be performed on a regular basis by the Information Security Officer of the Organization.

Any breaches or alleged breaches of this policy will be investigated by the Information Security Officer according to the Human Resources Department procedures and directly reported to the Head of Department to take the appropriate disciplinary actions.