GENERAL GUIDELINES FOR THE INFORMATION SECURITY MANAGEMENT SYSTEM

Av. Apoquindo 4001, Piso 12, Las Condes, Santiago, Chile.
Tel.: (56 2) 2393 9001
www.dcv.cl

DCV

TABLE OF CONTENTS

1. OBJECTIVE 2
2. SPECIFIC OBJECTIVES 2
3. SCOPE 2
4. INFORMATION SECURITY RESPONSIBILITIES 3
5. RELATED DOCUMENTS 3
6. GENERAL SECURITY POLICY 4
7. INFORMATION SECURITY GENERAL PRINCIPLES 4
7.1 Vision of the Business 4
7.2 Responsibility 4
7.3 Need to Know 4
7.4 Life Cycle 4
7.5 Functional Segregation 4
7.6 Legislation 4
7.7 Separation 4
7.8 Classification 4
7.9 Risks 5
8. REGULATORY REFERENCES CONSIDERED FOR THE ISMS 5
9. ISMS OPERATION 5
10. INCIDENTS MANAGEMENT PROCESS AND INFORMATION SECURITY REQUIREMENTS 5
11. ISMS MONITORING, MEASUREMENT, ANALYSIS, AND EVALUATION 6
12. ISMS MAINTENANCE AND IMPROVEMENT 6

1. OBJECTIVE

To support their vision, mission, objectives, and the products and services they provide, Depósito Central de Valores and its subsidiaries, hereinafter DCV, commit to and assign a high priority to their information assets. It establishes, documents, implements, and maintains an information security management system, known as ISMS, to protect all the information it handles.

A set of policies, procedures, standards, and guidelines are established to manage information security. Together, they contribute to preserving the confidentiality, integrity, and availability of information, providing protection against potential threats, and allowing to respond to and contain information security incidents in a controlled manner.

2. SPECIFIC OBJECTIVES:

- Create a formal framework to preserve information confidentiality, integrity, and availability.
- Establish a plan with clear and measurable objectives to provide visibility to the upper management.
- Establish an evaluation model and a way to address information security-related risks and implement the necessary controls to minimize their impact.
- Meet the government and contractual regulations for the services provided by DCV from the point of view of information security.
- Promote a culture to raise people's levels of understanding, awareness, and responsibilities regarding information security.
- Allocate resources to cover information security risks regarding the cost-benefit and the exposure of the information asset.
- Establish a reference framework to define and evaluate information management and the continuous improvement of the system.
- Establish and maintain plans and procedures to detect and respond to security incidents that affect the confidentiality, availability, or the integrity of information.

3. SCOPE

Applies to information assets developed and controlled under the Information Security Management System, maintained by DCV's collaborators, external staff, and providers.

4. INFORMATION SECURITY RESPONSIBILITIES

The contents of this document include the basic responsibility to implement, maintain, and improve DCV's information security management, which is the direct responsibility of the following departments:

Role	Description
DCV's upper management	Direct participation with the ISMS through the Security Committee, the Management Committee, and the Risk and Cybersecurity Committee, among others, comprised of DCV's managers.
IT Security Group	By-weekly meetings to reach agreements for security issues follow-ups and commitments, exceptions management, requirements, vulnerabilities, and gaps.
Head of Information Security and Technology Risk	Exclusively dedicated to their role with the management system, under the coordination of the risk and compliance management.
Cybersecurity Official	Exclusively dedicated to cybersecurity management on the DCV platform, under the coordination of the IT operations and cybersecurity management.

Please check the following document for more information: Roles and responsibilities of the ISMS.

To ensure the compliance of policies, specific roles and responsibilities are established for each process, which require the commitment of all DCV's staff and those related to the company to create and maintain an environment to ensure information security.

5. RELATED DOCUMENTS

- Document master control catalog. (Internal control work document that identifies the documented evidence that the BCMS and the ISMS must keep as per ISO 22301 and ISO 27001).
- Organization Context.
- Scope of the ISMS.
- Roles and responsibilities of the ISMS.

6. GENERAL SECURITY POLICY

DCV has its information security policy which establishes the guidelines that DCV's collaborators must follow to protect their information under the highest security standards.

7. INFORMATION SECURITY GENERAL PRINCIPLES

The following principles are considered for DCV's Information Security Management:

7.1 Vision of the Business

Information security is recognized as a necessary attribute of the services provided by DCV to its clients, both locally and internationally.

7.2 Responsibility

The organization recognizes that the proper awareness and training of its employees in information security are a priority.

7.3 Need to Know

Access to information must be controlled. Collaborators and processes are assigned only the accesses needed for their roles.

7.4 Life Cycle

The confidentiality, integrity, and availability of information must be protected during its entire life cycle, during its creation, transmission, and storage, until its final disposal.

7.5 Functional Segregation

Critical activities must be divided into roles undertaken by independent processes and staff and/or require previous oversight and approval.

7.6 Legislation

The organization claims to meet the current regulations and legislation in terms of non-disclosure and privacy of the information of its shareholders, clients, collaborators, and other stakeholders.

7.7 Separation

It separates and controls business information from its collaborators' personal information.

7.8 Classification

An information classification system and its access with the corresponding controls and authorizations are required.

7.9 Risks

The ISMS adheres to the company's risk model that includes information security issues within the risk assessment.

8. REGULATORY REFERENCES CONSIDERED FOR THE ISMS

The following standards have been considered to write the documentation for the information security system described in this document:

Reference	Version	Title
ISO/IEC 27001:2013	2013	Information technology – Security techniques – Information security management systems – Requirements.
ISO/IEC 27002:2013	2013	Information technology – Security techniques – Code of practice for information security management.
ISO/IEC 27004:2016	2016	Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis, and evaluation.
ISO/IEC 27005:2011	2011	Information technology – Security techniques – Information security risk management.
ISO/IEC 31000:2009	2009	Information technology – Security techniques - Risk management - Principles and guidelines.

9. ISMS OPERATION

DCV's ISMS must define and implement risk treatment plans and their corresponding controls based on the degree applicable to protecting information assets and minimizing their vulnerability, for which specific and detailed policies must be established to define the way of controlling and measuring the efficiency of the corresponding controls.

10. INCIDENTS MANAGEMENT PROCESS AND INFORMATION SECURITY REQUIREMENTS

The ISMS allows detecting security events and incidents on time. If information security incidents occur, the objective is to resume the regular operation of the services as soon as possible, minimizing the impact on the business operations. The objective with requirements is to satisfy clients' expectations within the scope of the services they have hired.

Please check the incidents management procedure and requirements for more information on this process.

11. ISMS MONITORING, MEASUREMENT, ANALYSIS, AND EVALUATION

The ISMS allows for evaluating the performance of the information security management process and its effectiveness. This is why the information security processes and controls must be monitored through indicators measurements and internal and external audits planned in periodical annual review periods.

12. ISMS MAINTENANCE AND IMPROVEMENT

With the reviews and evaluation of the ISMS, it has been established that whenever a system deviation is identified, a non-compliance will be reported, which incorporates proper management implementing improvement opportunities, corrective actions, and actions to avoid reoccurrence.

The upper management is committed to continuous improvement and ensuring effectiveness over time in their information security management system.