GENERAL GUIDELINES FOR THE INFORMATION SECURITY MANAGEMENT SYSTEM

www.dcv.cl

Av. Apoquindo N° 4001, Piso 12.
Las Condes, Santiago.
Tel.: (56 2) 2393 9000 - Fax: (56 2) 2393 9015

INDEX

1. PURPOSE

In line with its vision, mission, objectives, products, and services provided, DCV and its affiliate (hereinafter referred to as DCV) agree to and gives a high priority to its information assets. Accordingly, an information security management system is maintained (hereinafter referred to ISMS) in order to protect in the best way all of the information it handles.

For the management of information security, a series of policies, procedures, standards, and guidelines are established that, as a whole, contribute to maintaining the confidentiality, integrity and availability of the information; they provide protection against potential threats and permit to respond and contain information security incidents in a controlled manner.

2. SPECIFIC OBJECTIVES

- Structure a formal framework in order to maintain the confidentiality, integrity and availability of the information.
- Establish planning with clear and measurable objectives to provide visibility to senior management.
- Establish a model for the evaluation and treatment of risks related to information security and implement the necessary controls to minimize the impact.
- Comply with governmental and contractual regulations that regulate the services provided by DCV (from an information security point of view).
- Promote a culture that increases people's understanding, awareness, and responsibilities regarding information security.
- Establish a reference framework that permits defining and evaluating information management and continuous improvement of the system.
- Establish and maintain plans and procedures to detect and respond to the occurrence of security incidents that affect the confidentiality, availability, or integrity of the information.

3. SCOPE

It applies to the information assets that are developed and controlled under the information security management system, and that are maintained by DCV collaborators, external personnel, and suppliers.

4. RESPONSIBILITIES REGARDING INFORMATION SECURITY

According to the content of this document, a basic responsibility is set: implement, maintain, and improve the information security management of DCV, for which the areas mentioned below are strictly responsible:

Position	Description
Senior Management of DCV	Direct participation with the SGSI through the Security Committee and Management Committee, both made up of DCV managers.
IT Security Group	Biweekly meetings, generation of agreements related to security issues and monitoring of vulnerabilities and open security gaps.
Information Security and Business Continuity Officer	Full-time work in relation to the tasks of the management systems. This position operates under the coordination of risk management.
Cybersecurity Officer	Full-time work in relation to the security management on the DCV platform. This position operates under the coordination of IT operations and cybersecurity management.

Additionally, to ensure compliance with the policies, specific roles and responsibilities are established for each process, which require the commitment of all DCV personnel, and of those who are related to the company. This, in order to create and maintain an environment that ensures the security of the information.

5. RELATED DOCUMENTS

- Principal Control Catalog of Documents. (Document that points out the documents that must be maintained by the BCMS and ISMS under the ISO 22301 and ISO 27001 standards).
- Context of the organization.
- SGI scope
- SGI roles and responsibilities

6. GENERAL SAFETY POLICY

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

7. GENERAL PRINCIPLES OF INFORMATION SECURITY

For DCV's information security management, the following principles are considered:

7.1 Business vision

Information security is acknowledged as a necessary attribute of the services offered by DCV to its clients, both nationally and internationally.

7.2 Responsibility

The organization acknowledges that adequate awareness, training, and training for its personnel in matters of information security are priority tasks.

7.3 Knowledge

Access to information must be controlled. To both collaborators and processes, only the necessary accesses are granted (to be able to operate).

7.4 Phases

The confidentiality, integrity and availability of information must be safeguarded and protected throughout all its phases, i.e., from its creation, transmission, storage to its final destruction.

7.5 Functional Segregation

Critical activities need to be divided into functions that are performed by independent personnel or processes and/or require prior supervision and approval.

7.6 Legislation

The organization declares to comply with current regulations and legislation in relation to the confidentiality and privacy of its shareholders, clients, collaborators, and other stakeholders.

7.7 Separation

The business information and the personal information of the collaborators is distinguished and controlled.

7.8 Classification

An information classification scheme is required. This ensures that access to it is carried out in a controlled and authorized manner.

7.9 Risks

The ISMS adheres to the company's risk model, which includes within the risk assessment, the information security areas.

8. REGULATORY REFERENCES CONSIDERED FOR THE ISMS

For the preparation of the documentation that comprises the information security management system described in this document, the following standards have been considered as a reference:

Reference	Edition	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, as well as the respective controls, according to the degree applied in order to protect information assets and minimize their vulnerability. Accordingly, it must be established in specific and detailed policies that define how to control and measure the effectiveness of the respective controls.

10. INCIDENT MANAGEMENT PROCESS AND INFORMATION SECURITY REQUIREMENTS

The ISMS permits early detection of security events and incidents. In relation to information security incidents, the objective is to restore the normal operation of the services as soon as possible, minimizing the impact on business operations. Regarding the requirements, the objective is to satisfy the client's expectations within the scope of the services hired by the client.

11. ISMS MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION

The ISMS permits an evaluation of management performance on information security and the effectiveness of the implemented management. That is why it is required to monitor the implemented controls and information security processes, which is done through indicator measurements, and also through the execution of internal and external audits. The latter are planned at periodic intervals (annual reviews).

12. MAINTENANCE AND IMPROVEMENT OF THE ISMS

As a result of the reviews and evaluation of the ISMS, it has been established that when a deviation in the system is identified, a non-conformity will be generated that incorporates an adequate management by implementing elements for improvement, corrective actions, and preventive actions.

Senior management is committed to continuing to improve and ensure the effectiveness of its information security management system over time.