PO.19 Information Security Policy

Area: IT
Management: IT Governance and Architecture

Creation: 04/14/2011
Last Review: 03/27/2024

1. OBJECTIVE

This Policy establishes Information Security guidelines and standards for Dexco to protect the confidentiality, integrity, and availability of information assets.

2. SCOPE

This Policy applies to all areas of the Company, its managers and employees, as well as third parties who may be contracted by Dexco S.A. and represent it in the activities referred to herein.

3. NORMATIVE REFERENCES

- NO.44 Application of Disciplinary Measures;
- NO.56 IT Access Management;
- NO.57 Use of Microinformatics Resources;
- NO.58 Information Classification;
- NO.59 Vulnerability Management;
- NO.63 Backup and Restore Management.

4. DEFINITION

Confidentiality: Ensuring that all means of processing and/or storing information have protective measures against unauthorized access and use, ensuring that all information is protected from accidental disclosures, industrial espionage, privacy violations, and similar actions.

Integrity: Ensuring that all information processed, transacted, or stored in Dexco's systems and databases is free from undue alterations and irregularities.

Availability: Guaranteeing that information and its processing capacity, whether manual or automatic, are safeguarded and recovered whenever necessary, ensuring that the business is not significantly impacted and is always available to the requesting entity.

Information Security Incident: Any action that infringes one or more pillars of Information Security (integrity, confidentiality, and availability).

Asset: Any item that has value to Dexco, such as but not limited to: information, physical structure, technological environments.

Backup: Security copy of data (information) or system (applications, software) from one storage device to another environment so that these same data can be restored in case of an Information Security incident.

Employees: All hired professionals with an employment relationship with Dexco, including interns and apprentices.

Third Parties: Service providers or companies hired to provide services and/or labor to Dexco..

ITSM Software: Application used for opening and managing tickets as well as project management.

Incident Management Plan: Document describing how an Information Security incident should be managed, including a contact tree of key people in the company's critical processes.

NDA (Non-Disclosure Agreement): Confidentiality agreement to protect and safeguard Company data such as new developments, processes, projects, products, cost and price information, negotiations, suppliers, and customers from unauthorized disclosure.

5. ROLES & RESPONSABILITIES

5.1 Information Security

- Approve and periodically review this and other policies and standards related to Information Security.
- Ensure the necessary resources for implementing security controls.
- Define rules for managing the technological environment with the best Information Security practices.
- Ensure compliance with current legislation and regulations regarding Dexco's Information Security.
- Identify and evaluate the main threats to information security and propose and implement corrective measures to reduce risks.
- Manage information security incidents, ensuring proper handling.
- Manage periodic access reviews of the audit scope systems.
- Administer the cybersecurity awareness program.

5.2 Infrastructure

- Follow all the guidelines of this Policy.
- Comply with the technological environment management definitions proposed by the Information Security area.

5.3 Service Desk

- Promptly refer Information Security incident tickets opened in the ITSM software to the Information Security area.

5.4 Employees

- Read, understand, and fully comply with the terms of the Information Security Policy as well as other applicable security standards and procedures.

- Sign the "PO-19 Commitment Term," formalizing awareness and full acceptance of the Information Security Policy provisions as well as other security standards and procedures, taking responsibility for their compliance and respecting the confidentiality, integrity, and availability of Dexco's information.
- Protect information against unauthorized access, disclosure, modification, or destruction by Dexco.
- Properly dispose of documents according to their classification level.
- Use equipment and technological resources exclusively for their intended purposes and in Dexco's interest.
- Respect the confidentiality of IT asset access passwords granted to them.
- Report to the Information Security area any event that violates this Policy or may jeopardize Dexco's information security.
- In case of doubts and/or clarification requests about this Policy, contact the Information Security team: segurancadigital@dex.co.

5.5 Managers

- Enforce and ensure compliance with this Policy within their team.
- Require third parties to sign the confidentiality agreement for the information they will access, according to information classification.
- Approve access requests considering the role performed by the requester, segregation of duties, and the principle of least privilege.
- Periodically review their team's accesses in a timely manner whenever necessary or requested by Information Security.
- Request immediate cancellation of IT asset access for any third party under their management who is dismissed or transferred.
- Apply the penalties contained in the "NO.44 Application of Disciplinary Measures" standard in case of non-compliance with this Policy by their subordinate.
- Guide the proper classification of information by their employees.

5.6 Human Resources

- Assign employees, during the formalization of the individual employment contract, internship, among others, the responsibility to maintain information security through the signing of the "PO-19 Commitment Term."
- Immediately report any termination so that all appropriate measures can be taken as provided in the "NO.56 IT Access Management" standard.

5.7 Compliance

- Make this Policy available and disclose it to the Company's employees, in addition to other Information Security-related standards.

6. PROCEDURES

6.1 Information Classification

Dexco's information can be present in systems and various types of media, such as paper, removable media (CD, DVD, pen drive, HD, among others), as well as verbal communication, and must be protected according to its classification and relevance to the business.

Thus, all corporate information must be classified by the information owner considering the following four levels:

- Confidential**:** Information is available only to previously authorized individuals, and unauthorized access to this information can cause significant damage to the business and/or the organization's reputation. In these cases, it is generally necessary to sign an NDA (Non-Disclosure Agreement).

- Restricted: Information is available only to a specific group of authorized employees and third parties and, if improperly disclosed, can cause considerable damage to the business.
- Internal Use: Information is available to all employees and some third parties with access control rules and should be limited to internal use within Dexco.
- Public: Information is or may be available to the general public, including externally, and is usually of low sensitivity.

Information has a life cycle and must be regularly reclassified according to changes in its value, sensitivity, and criticality by the Information Owner. Further information and guidelines should be consulted in the "NO.58 Information Classification" standard.

6.2 Access Management

Access can only be granted after signing the employment/service contract or NDA to ensure confidentiality and proper use of information as expressed in this document and applicable standards.

Unique and identifiable logins must be created for users, and employees are responsible for using their logins for their work scope and securely safeguarding their passwords, including not sharing corporate email externally for personal use, as all logins are unique and non-transferable, and sharing is prohibited.

Third-party user access is a shared responsibility between the third party and the contracting manager, so once the service provision ceases, it is the manager's responsibility to immediately request access termination.

Access granting must follow the principle of least privilege, with permissions necessary and sufficient for an employee to perform their activities for a limited time and with the minimum rights required for their tasks, following the "NO.56 IT Access Management" standard guidelines.

Managers are responsible for evaluating, reviewing, and approving access requests from their subordinates, and in case of conduct deviations through improper approvals, they may be held accountable.

In cases where managers do not review accesses or if there is evidence of misuse by the user, the Information Security team will revoke the accesses.

The use of network resources, systems, equipment, and other information sources is monitored and can be collected and used at Dexco's discretion for internal investigations or to meet judicial measures without prior notice to the involved parties, respecting employees' privacy whenever necessary.

6.3 Asset Management

IT assets must be categorized, inventoried, and managed throughout their life cycle, including disposal, which must be carried out in a way that preserves information confidentiality and minimizes possible environmental impacts.

Access to removable media is blocked on Dexco's workstations, restricted only to people who need this resource to perform their activities solely for the contracted function, and strictly prohibited for personal purposes.

Dexco's assets must be treated confidentially and ethically according to current laws and internal regulations, promoting proper use and preventing undue exposure of information.

6.4 Encryption

All Dexco notebooks are encrypted to ensure the confidentiality and authenticity of information according to the "NO.57 Use of Microinformatics Resources" standard.

6.5 Information Security Incident Management

Any adverse event related to the security of an asset that can harm any Information Security principles (confidentiality, integrity, and availability) must be reported to the Information Security team, where it will be promptly handled and managed according to the Incident Management Plan.

6.6 Vulnerability Management

The Information Security area must periodically conduct vulnerability assessments to identify and remedy possible security weaknesses in Dexco's technological environment.

Vulnerability management must be conducted according to the "NO.59 Vulnerability Management" standard.

6.7 Backup

Critical information used in Dexco's activities must have backup copies.

Backup copies must meet operational, legal, historical, and audit requirements regarding their generation and safeguarding periodicity.

Backup and its restoration must follow the procedure described in the "NO.63 Backup and Restore Management" standard.

6.8 Physical Security

Entry to Data Centers must be properly controlled and monitored.

Data Center areas must be protected with security barriers or access mechanisms to prevent unauthorized access.

Access to the Data Center without proper identification is allowed only in emergencies when the physical security of the Data Center is compromised, such as by fire, natural disasters, or structural building damage.

6.9 Clean Desk and Screen

To reduce the risk of security breaches, fraud, and information leaks caused by documents left on desks or visible on screens in the company's facilities, it is necessary that documents in physical and/or electronic media do not remain on desks or applications unnecessarily and should be properly handled, stored, and discarded. Additionally, all users must lock their equipment when absent.

6.10 Cybersecurity Awareness

Dexco periodically promotes awareness campaigns in person and/or online, addressing best practices in Information Security, with the aim of strengthening the company's cybersecurity culture. These campaigns can be conducted through informative emails, the company's intranet, e-learning, indoor media, and other means deemed necessary by the Security team.

7. SANCTION

Non-compliance with the guidelines of this Policy will be subject to applicable disciplinary measures. In case of violation of the guidelines present in this Policy, the Compliance area must be notified via the departmental mailbox compliance@dex.co, at which point the pertinent areas will be activated to investigate the facts and, if necessary, disciplinary measures will be applied. If the Information Security team itself identifies violations of the guidelines contained in this standard, it will communicate this to the User's Manager, with the consent of the HR unit, about the violation performed. It is the responsibility of the User's Manager to apply the penalties contained in the "NO.44 Application of Disciplinary Measures" standard.

8. VALIDITY

This Policy will come into effect from its publication date and must be reviewed every three (3) years and may be amended at any time, whenever necessary.

9. APPROVAL

This Policy was approved by Dexco's Board of Directors.

10. ATTACHMENTS

- PO-19 – Commitment Term;
- Cybersecurity Incident Management Plan.


DEXCO
Deca Portinari Hydra Duratex Castelatto Ceusa Durafloor