Public Information Security Policy

1 Purpose

So that Information Security is completely efficient, DASA has implemented a series of controls comprised by policies, practices, procedures, organizational structures and technologies.

This document lists the main controls used by DASA to comply with information and cyber security requirements, mitigating incident vulnerabilities.

2 Introduction

DASA, through its Information Security department and aligned with business purposes and requirements, sets forth rules and guidance based on NBR ISO 27001, 27002 and NIST (National Institute of Standards and Technology) standards to be followed and applied to people, processes and technology, in order to protect organization, customer, supplier and business information.

3 General Guidelines

With the purpose is assisting its employees and stakeholders to understanding their responsibilities, to assure they are in compliance with previously set guidelines and laws and regulations, some documents were developed to disseminate information security process and procedure knowledge.

These documents are in an environment protected against modifications, available in accessible location to employees and forwarded to stakeholders, whenever requested.

4 Business Information Security

Next, the main controls used buy DASA to protection information, comply with cyber security requirements and reduce incident vulnerability are listed.

4.1 Logical and Physical Access

- Restricted Room Physical Access

Sets the physical access perimeter and control required to environments that host critical servers, biological samples and classified documents.

- Data Network and Information System Logical Access

  It sets forth guidelines and requirements for application access controls and technology environment systems.

- Corporate Wireless Network Access

  It sets forth general guidelines for wireless network installation, setup, access release and security.

- Manging Information System Passwords

  It sets forth password usage guidelines to enable access security to network and computer systems.

- Computer System Access Credentials

  It sets forth user account credentials, privileges and nomenclature to computer system access.

- Granting internet access

  It sets forth internet access guidelines by user profile type.

4.2 Data protection

- Information Classification, Labeling and Handling

  It sets forth information classification, labeling and handling guidelines according to its sensitivity and criticality to the organization, aiming at proper protection level establishment.

- Information sharing and storage

  It sets forth guidelines to keep safety in information and knowledge exchange or sharing in the company, and with any external agencies. As well as data encryption at rest and in motion.

- Submitting, accessing and receiving encrypted e-mails

It sets forth guidelines to submit and received encrypted e-mails.

- Handling, managing and disposing media safely

  It sets forth guidelines to handle, managed and dispose safely printed or digital media.

- Pen-drive access

  It sets forth pen-drive access guidelines in company equipment by user profile type.

- Data leak prevention - DLP

  It sets forth guidelines so that company data is managed in standardized way in all conglomerate, assuring it is classified as confidential and with restricted use, is not shared by mistake, willingly and/or maliciously t unauthorized users.

4.3 Network security

- Internet use and access

  It sets forth internet access and usage criteria and standards by network users, sustaining compliance with information security policy and laws and regulations in force.

- Electronic messaging service

It sets forth user e-mail service access and usage guidelines.

- Applying perimeter security

  It sets forth equipment security policy application, in order to protect and mitigate possible vulnerabilities that can be developed and that enable an external (originated through the internet) or side attack.

4.4 Application security

- Information system application, maintenance and development

It sets forth minimum requirements to application safe acquisition, development and maintenance, aiming at risk reduction associated to data security used by applications or with the infrastructure used.

- Developing software and system safe code

  It sets forth application safe development criteria and practices, in order to reduce risks and impacts in business areas, and it also provides security and reliability to development process / change deployment and/or new system versions in production environment.

- System acquisition foundations and guidance

It guides and sets forth system acquisition safe strategy and methods.

- Assessing, testing and validating developed application security

  It sets forth criteria to application security assessment, test and validations developed in Dasa ratification environment.

- Information system encryption

  It sets forth safe procedure, setting the encryption application scope, with the purpose of assuring a safe channel to information communication.

4.5 Endpoint security

- Malicious code prevention

  IT sets forth control guidelines against malicious codes to be applied in Dasa managed devices.

- Information Technology feature acceptable use

  It guides employees in practices for correct Information Technology asset and feature usage.

- Backup

  It sets forth guidelines to information backup execution. Corporate files, production systems, programs, applications, operating systems, databases, scripts, setup parameters and regular recovery tests for files stored in servers.

4.6 Supply chain management

- Supplier assessment

  It sets forth external provider selection, assessment and reassessment principles and rules.

4.7 Prevention

- Change management

  It sets forth IT change management process general rules, designed to assure method and control application that result in minimum negative impacts, originated from poorly planned and/or executed changes in assets.

- Technical vulnerability management

  It sets forth technical vulnerability management principles and rules in the environment, identifying and mapping attack risk and asset exposure.

- Information technology audit management

  It sets forth rules to perform information security audits, in order to minimize system or information compromising risks. Such audit purpose is assessing users, system, their mechanisms and controls.

- Business continuity management

  It sets forth guidelines in order to minimize negative impacts caused by any events that might jeopardize Dasa business continuity. Also responsible for setting roles and responsibilities required to management process execution.

- Intrusion test

  It sets forth guidelines to execute intrusion test to search and identify network, system or tool security vulnerabilities.

- Awareness

It sets forth awareness program and security training to employees and service providers.

4.8 Defense Center and Cyber Operations

- Information security incident management

  It sets forth the process to identify, notify and manage information security incidents and defines rules to assess, hold accountable and apply corrective and disciplinary measures due to information security policy violations.

- Information technology crisis management

  It sets forth crisis management plan, that covers procedures and instructions to be adopted whenever crisis situation or threat takes place.

- Risk Management

  This process sets forth guidelines to identify, analyze, measure and handle information security risks identified in the environment.

- Information security consequence management

  This process sets consequence management criteria and procedures in information security incident result occurred in the environment, in order to standardize administrative actions and assurance relevant information, system, application and asset confidentiality, availability and integrity.

- Log and event management

  This process manages activities or events through log management and analysis, detecting unauthorized or inadequate information processing activities and complying with applicable relevant legal requirements to record and monitoring activities.

5 Responsibilities

5.1 Employees and third parties

- Every DASA employee and third party is responsible for complying with information security and security principles provided in organization policies, processes and procedures.

5.2 Information Security Area

- Setting, keeping and raising awareness on information security corporate policies, procedures and patterns;
- Performing regular qualification planning and conducting with the purpose of disseminating security culture within the company, as well as notifying occasionally performed updates in information security corporate policies, procedures and patterns;
- Assuring access grant, access right end or change to network and critical applications, according to the user profile;
- Assuring organization information and cyber security improvement through projects and initiatives;
- Leading information security incident management, including investigations to define causes and responsible parties and perform internal communications of the facts occurred.

5.3 Top Management

Top Management is the last instance responsible for supervising information and cyber security policy, procedure, control development and implementation, and they are responsible for:

- Approving information security policies and procedures and subsequent changes;
- Providing clear guidance and support to information security initiatives;
- Fostering organization information and cyber security culture;
- Providing features required to information security management system.

6 Information security communication channel

If you want to notify any incident, forward to:

- security@dasa.com.br

7 Terms and Definitions

Term	Definition
Top Management	Person or group of people that manages and controls an organization in its highest level
Backup	Storage device data security copy to another one, so that it can be recovered in case of original data loss
Malicious Code	Harmful computer code which purpose is creating vulnerabilities in company assets
Compliance	Requirement compliance
Encryption	Practice to code and decode data
Crisis	Any event that threatens people integrity, that causes high impact to business and/or company reputation
Event	Occurrence or change in a specific circumstance set that can have several causes
Incident	Situation that can represent or lead to business stoppage, losses, emergencies or crises
Infrastructure	Installation, equipment and service system required to organization operation
Firewall	Computer network device with the purpose of applying security policies
Log	Expression used to describe relevant event record process in a computer system
Ongoing Improvement	Recurring activity to improve performance
NBR ISO 27001	Brazilian organization that sets forth requirements to an organization information security management system.
NIST	United States Trade Department technology administration non-regulatory government agency
Stakeholders	Person or organization that can impact, be impacted or that understand they are impacted by an organization decision
Pen-drive	Data storage device
Risk	Probability that an event happens, whether it is a threat, whenever negative, or opportunity, whenever positive
Wireless Network	It is a wireless communication infrastructure that enables data transmission and information with no cable use required
Intrusion test	It is a method that assesses a computer or network system security, simulating a malicious source attack
Vulnerability	It is an asset weakness that could be potentially explored by one or more threats