Deloitte.

Information Security Policies for compliance by third parties– Annex: Information Systems

Deloitte Portugal

Version: 2
Date of 1st version: 14-09-2017
Data of current version: 12-08-2021
Classification: Restrict
Reference: SGSI_Políticas de Segurança de Informação a cumprir por terceiros _Anexo_Sist. Inform_EN.docx

Target Audience - Notice

This document is a complement to documents “SGSI_Políticas de Segurança de Informação a cumprir por terceiros_Geral” (SGSI – Information Security Policies for compliance by third parties – General) and “SGSI_Políticas de Segurança de Informação a cumprir por terceiros_Específico” (SGSI – Information Security Policies for compliance by third parties – Specific) and is directed to all third parties (companies or individuals) who provide Information Systems related services to Deloitte Portugal and must be aware of and enforce compliance with their content.

Control of Versions - Notice

This document is a controlled document, which supersedes all other versions. Any copies from previous versions or dated prior to the abovementioned publication shall not be deemed valid.

Copyright - Notice

This document contains information owned by Deloitte Central Services, S.A. (a member firm of Deloitte in Portugal). Non-authorised reproduction, distribution or disclosure of any information contained herein is a violation to the organisation’s policies and copyrights.

Miscellaneous - Notice

Any product names used herein are for identification purposes only and may be trademarks of the respective organisations.

Once services are rendered, any third party undertakes to return and/or destroy any copies hereof (printed and/or electronic format), and shall be held liable for noncompliance with this procedure.

Index

1 Security Requirements for New Information Systems

1.1 Foreword on specification and analysis of information security requirements

Whenever a new information system is devised and developed, information security requirements must be identified, documented and reviewed on a regular basis, by using different methods, namely: deriving compliance requirements vs policies and regulations, modelling of threats or information security incident reviews.

The identification and management of information security requirements and associated processes must be integrated into the early stages of this projects.

Information security requirements for new information systems should consider the following:

- *Hosting* and environments segregation:

  Deloitte Portugal systems or applications must be located in approved *hosts*: *data center on premises*, *cloud hosting*, *SaaS (software-as-a-service)* or any other contractual mode; production environment shall be segregated from other environments, with specific security requirements, such as authentication and authorization.

- Authentication:

  Prevention of access to systems, applications and their data by unknown or unauthorized users; there must be a maximum level of confidence regarding the identity of the users (eg userid and password, two-factor authentication, SSO, etc.), complying with the norms and standards in force at the firm, such as the mandatory use of the MFA (Multi Factor Authentication) for applications accessible via the internet.

- Authorization:

  The principle of least privilege must be applied: each duly authenticated user should only have access to the data they need to carry out their functions; there must be differentiated authorization and provisioning processes for common users, privileged users and service users.

- Roles, responsibilities and functions segregation:

  The potential risk of abuse of information access privileges must be addressed; the accesses and roles of each system or application must be assigned to users based on the real need for information to carry out the respective activities and taking into account the segregation of functions: it must be ensured that the execution of critical activities for the business and the respective control are not performed by the same user.

- Privacy and e confidentiality:

  Appropriate levels of protection and controls must be defined in order to safeguard the undue disclosure and disclosure of confidential or sensitive information.

- Integrity:

  Appropriate levels of protection and controls must be defined in order to safeguard the undue modification of data or transactions; cloud and mobile applications must provide specific protection mechanisms, due to their greater exposure to the risk of cyber-attacks that lead to non-integrity of data.

- Availability:

  The business requirements regarding availability (eg load, downtime, redundancy, continuous availability, etc.) must be included in the system or application architecture.

- *Monitor and audit Logs*:

  The tracking of user activities carried out in systems and applications must be defined, with special attention to critical actions for the business; for each type of action in the system or application, the level of detail of information to be generated and its safeguard location must be defined, including the actions performed by users with privileged access. Logs must be monitored systematically and frequently, so that it is possible to obtain alerts of anomalous or suspicious activities and carry out forensic analysis of these activities.

- Data breach:

  Establishment of security controls that prevent the leakage of sensitive and confidential information; systems and applications must be frequently monitored, in order to detect unusual access to information (eg excess of queries, reports or downloads compared to the normal pattern of use). Special attention should be paid to the design and architecture of mobile applications, in order to incorporate protection mechanisms against cyber-attacks, namely reverse engineering.

- Business Continuity Plan and Disaster Recovery:

  The functional owners of the processes covered by the system or application in question must review Deloitte Portugal's Business Continuity Plan and ensure that the requirements for recovery in the event of a disaster have been included, namely the RTO (Recovery Time Objective) and the RPO (Recovery Point Objective); the architecture of the system or application must include these requirements, namely at the hosting level.

- Other considerations:

  Before starting the system or application design phase, it must be ensured that the various security processes have been validated and approved in accordance with the standards in force in the firm (e.g. system risk analysis, supplier risk analysis , PIA - Privacy Impact Assessment, etc.).

2. Operation Model

It must be used the firm current methodology, following all the stages, validations and approvals provided for the compliance with the securety safety details in which one of the checklists published.

3. Glossary

- ACL – Access Control List
- SSO – Single Sign On

2 Safe Development Policy

2.1 Safe development policy

Security controls for accessing Deloitte Portugal's development environments and testing environments must be in compliance with the access control policy of the company.

Data repositories that store information related to the development or modification of applications or systems that process confidential customer information must have the necessary security controls to preserve confidentiality, integrity and availability of such information.

According the current firm standards, principles for safe coding and better programming language practices must be followed as well as any used development framework.

Information security requirements must be established and formalised during the analysis phase and included in the design phase of any application or system that processes confidential customer information or when they need to be altered.

The project associated with the development or improvement of applications or systems that process confidential customer information must consist of specific phases, in appropriate moments, in order to check compliance with information security control requirements.

A process that includes phases related to the entire development life cycle of any applications or systems must be formalised, which identifies procedures to be conducted during review and solution testing phases.

Information deemed necessary to control application or system versions must be properly stored and protected, regarding the processing of confidential customer information of the company.

In-house or outsourced personnel who contribute to the development or modification of applications or systems which process confidential customer information must have the necessary skills that contribute for a safe development of these environments.

2.2 Principles for the development of safe systems

The internal development of safe information systems must take into account the need for:

- Analysing and incorporating, whenever possible, security components in all architecture levels (business, applications, data and technology);
- Analysing the possibility of incorporation of open security standards for the protection of any systems' portability and interoperability;
- Designing and implementing audit mechanisms to detect any unauthorised use and support to security incident investigations;
- Limiting, wherever possible, the level of assigned privileges regarding the information system domain;
- Balancing information confidentiality protection controls with information accessibility requirements;
- Analysing security threats of new technologies used;
- Developing the project with security controls that respond to known attack patterns;
- Designing the system by considering its use in network environments, formulating security controls that address multiple domains, authenticating users and processes internally and externally to the system domain;
- Assuming that external systems are unsafe;
- Assessing the incorporation of these principles into third-party information systems service contracts or agreements;
- Apply these principles in the development of applications that have input and output interfaces with confidential customer information.

3 Change Management Policy

3.1 Change Management Policy

Any changes to Deloitte Portugal's information systems and support infrastructure must follow the defined Change Management process (including usual and urgent changes), and must be duly approved before their implementation.

The process is applicable to:

- Routers;
- Switches;
- Firewalls;
- Servers;
- Appliances; and
- Business support applications.

Any changes that may impact the confidentiality, availability and integrity of the systems and confidential customer information, require the filing of a change order that must be recorded in the process supporting application.

Change orders shall be analysed and their impact must be assessed, together with several areas/involved teams. Based on this analysis, the change order may be approved or denied.

These changes include, but are not limited to:

- Firmware upgrades;
- Software upgrades;
- Hardware upgrades;
- Changes to the settings of servers, firewalls, switches;
- Installation of patches and updates;
- New application functionalities or fixes to existing functionalities.

Whenever possible and applicable:

- Changes must be previously made and tested in a testing environment and subject to acceptance before being applied to production systems;
- Fall-back procedures and mechanisms must be ensured prior to implementation of the change;
- Documentation supporting the information and infrastructure systems that have been altered should be updated.

The implementation of changes should be timed in order to avoid or minimise business disruptions.

Deloitte.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.