Deloitte.

Information Security Policies for compliance by third parties - General

Deloitte Portugal

Version: 3
Date of 1st version: 14-09-2017
Data of current version: 12-08-2017
Classification: Restrict
Reference: SGSI_Políticas de Segurança de Informação a cumprir por terceiros_Geral_EN.docx

Target Audience - Notice

This document is directed to all third parties (companies or individuals) who provide 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

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 Information Security Policy

1.1 Information Security Policy

The protection regarding the processing, safeguarding and transmission of confidential customer information in a consistent manner with professional, ethical, legal, regulatory and contractual requirements is one of Deloitte Portugal's top priorities and something that is deemed critical to the company's success. Loss or theft of confidential information can have serious legal, financial and/or reputational consequences, and Deloitte Portugal is committed to protecting the confidentiality, integrity and availability of confidential customer information and of Deloitte itself whether it is on print, digital media or intellectual property.

Thus, information security policy principles ensure that:

- Information is protected against unauthorised access;
- Confidentiality of information is guaranteed;
- Information integrity is maintained;
- All applicable laws and regulations are respected;
- Appropriate business continuity plans are maintained and tested regularly; and
- All and any information security breaches that are detected or suspected are investigated by the competent areas.

Hence, Deloitte Portugal maintains an Information Security Management System (ISMS) consisting of policies, processes and procedures and was designed to maintain, review and continuously improve information security at Deloitte Portugal, based on the assessment of existing risks. The ISMS aims to:

- Ensure that all employees are aware of and comply with this Policy, and other existing security policies and/or procedures;
- Define and communicate information security responsibilities at the company;
- Promote ongoing information security awareness and conduct training programs to ensure that all employees understand how information security is part of their functions and the responsibilities they have in protecting the confidentiality, integrity and availability of information;
- Include information security as a crucial component of all business planning and operation aspects;
- Continuously assess information security threats by ensuring that these are identified and managed based on risk assessment and the application of appropriate controls;
- Provide suitable infrastructure protection of the company's information and communications systems against loss, misuse or improper access;
- Promote the detection, recording, reporting and investigation of security incidents in an effective and efficient manner to ensure the minimisation of impacts regarding these types of incidents at the company;
- Ensure the implementation and testing of business continuity plans that assure the continuity of operations, minimising the impact of a security incident or an emergency situation;
- Guarantee the availability of the necessary resources to ensure effective ISMS maintenance and continuous improvement; and
- Carry out the ongoing review of security mechanisms and processes to ensure that they are effective, relevant and appropriate to corporate needs.

1.2 Responsibilities

All employees, as well as third parties who, in any way, can have access to Deloitte Portugal's confidential customer information, must comply with and enforce all information security policies of the company, and shall promptly report to the Chief Information Security Officer (CISO) any security incidents, that is, any event that may cause, or that has caused, an information security breach.

2 Physical and Environmental Security Policy

Special identification badges [1] may be issued to third parties who may require temporary access Deloitte Portugal's premises. These will be considered as pre-authorised third parties. This access must be set up in order to only allow access to the areas which pre-authorised third parties need access to, for the exercise of their functions for which they have been authorized or contracted. The availability of these badges should be subject to pre-authorisation, issued by the staff member of the company responsible for the presence of such third party, specifying the areas that require access. The identification badge shall always be worn in a clearly visible manner during their stay at the company's premises.

For each Deloitte Portugal's building, the following physical security perimeters must be identified:

- External perimeter - public areas; all areas that precede the semi-public perimeter;
- Semi-public perimeter - controlled access areas [2] in which third parties to Deloitte Portugal can transit and remain;
- Reserved perimeter - working areas of Deloitte Portugal's personnel;
- Secure perimeter or safe area - areas where confidential customer information is stored or processed, or where there are production assets that support the company's information and communication infrastructure.

The semi-public perimeters shall respect the following rules:

• All third parties without access credentials willing to access Deloitte Portugal's premises may do so only after obtaining a visitor's authorisation. The reception staff must register the name of any third party before they enter Deloitte Portugal's offices;

• Third parties without credentials must be accompanied by a reception staff member when accessing these perimeters. It is not necessary to accompany these third parties on a permanent basis whilst they are in these perimeters;

• Access to these perimeters by Deloitte Portugal's employees and pre-authorised visitors must be made by using the company's identification badge in electronic access control systems.

The reserved perimeters must respect the following rules:

• Access to this perimeter by Deloitte Portugal's employees or pre-authorised third parties must be made by using the company's card in electronic access control systems;

• Access outside normal office hours must always be protected by access control mechanisms with two authentication factors: card and PIN;

• Non-authorised third parties may only enter and remain in this perimeter when accompanied by company's employees;

• Access to this perimeter must be subject to image recording.

Safe perimeters or safe areas must comply with the following rules:

- They must always be protected by access control mechanisms with two authentication factors: card and PIN;
- Deloitte Portugal's employees with access to safe areas must be subject to specific authorisation issued by the person responsible for the area in question, whenever it is an exception to the approved physical access matrix. These should be included in an internal access authorisation list to safe areas that will be kept updated by the same responsible staff member. A review of the persons included in this list should be carried out at least once a year;

• Any third party who needs access to secure areas (DataCenters and Central and Intermediate Archives) must be subject to specific authorisation issued by the person responsible for the area, registering the need for access, the time and allocation of pre-authorised time as well as any other information deemed relevant to the access;

---

[1] External Entity or Regular Visitor.

[2] Zones after the reception area of Clients, suppliers or visitors including customer meeting rooms on floor 1 of Deloitte Hub.

• Access and permanence of third parties in secure areas (DataCenters and Central and Intermediate Archives) should be permanently monitored by authorised company personnel;

• External access to DataCenters, Central Archives, and Intermediate Archives should be recorded. In the case of DataCenters, whenever possible, a surveillance camera must be placed inside the perimeter to allow remote surveillance of the presence of persons within the perimeter;

• When performing activities in safe areas, the following actions are forbidden:

- Smoking, eating or drinking;
- Photographing or filming, except when previously authorised by the person responsible for the area.

• Equipment residing in safe areas should not be removed from the premises without the prior authorisation of the person responsible for the area and the person responsible for the applicable asset;

• Any equipment or information in physical format (for Central and Intermediate Archives) taken from a safe area must be properly registered, where the following items will be identified: Date/Time of operation, name of the employee responsible for the operation, reason. The corresponding inventory of supporting ISMS assets should be updated in the case of IT or communication equipment;

• All assets supporting information and communication infrastructures to be removed from these perimeters must be previously verified as to the need to delete any confidential customer information and licenced software;

• Whenever possible, the performance of activities in the safe areas should be performed by more than one staff member in order to deliver adequate response in case of an incident to one of the items and to prevent malicious activities;

• The existence of material not directly related to management and maintenance activities of IT and communication infrastructures is forbidden, except when previously authorised by the person responsible the area. This stay must be authorised for the shortest time deemed necessary;

• Safe areas must bear appropriate signs in their interior to inform existing prohibitions and recommendations;

• Safe areas should not be identified as such on the outside, except when required by the competent Authorities.

3 Acceptable Asset Use Policy

3.1 Deloitte's Information Disclosure and Internet Exposure

Employees cannot:

- Publish Deloitte's confidential or public information on third party websites, without prior and express approval of the company;
- Make comments or statements about Deloitte Portugal in newsgroups, instant messaging, chat rooms, social media or other public forums;
- Make comments or statements about clients and engagements in newsgroups, instant messaging, chat rooms, social media or other public forums;
- Use Deloitte's e-mail address in public communications, newsgroups, instant messaging, chat rooms, social media or other public forums, unless participation in such communications is a mandatory requirement of their function at Deloitte and only upon prior approval;
- Publish or make available Deloitte's email address on websites, such as contact email to receive communications;
- Engage in any communication that is unlawful or in violation of any company policy, including (but not limited to) defamatory, obscene, racist, sexist communications, or that contain religious bias;
- Create websites or web pages that represent or submit offers of Deloitte's products and services without approval from the marketing department;
- Promote products, manage business or business transactions that are not directly related to their function in the company;

Promote or advocate causes, charities or institutions of any kind (including political activism) unless expressly authorised by the company.

3.2 Social Networks

Deloitte Portugal's employees may not use Deloitte's image or brand, disclose confidential customer or corporate information, contacts or other information from employees, engagements or clients on social networks.

3.3 Physical access control

1. Building security

Regarding the Physical and Environmental Security Policy:

- entry into Deloitte's buildings is controlled by access cards that are assigned to all Deloitte's professionals, external entities and regular visitors (including suppliers of goods or services requiring access to Deloitte's premises on a regular basis);
- Pontual visitors (clients or third parties who have meetings at the office) should go to the reception for registration and accompaniment by a Deloitte professional;
- all Deloitte's building entrances and exits are monitored by CCTV, and images are stored for a period of 30 days;
- The management of CCTV cameras is conducted by Deloitte's Office Administration - Facilities.

2. Global rules for employees

Badges, in addition to allowing access to the buildings and their security zones, according to the duties of each employee, identify the person as being a Deloitte's staff member, and they should wear the identification badges in a visible manner, preferably using the official neck strap.

Employees are responsible for their badges and the latter should be used exclusively by employees. Lending identification badges to other employees or third parties is forbidden.

Any Deloitte's employee should be aware of and approach any person who does not wear the identification badge in a clearly visible manner, reporting possible security breaches according to the security incident management process.

If any Professional, External Entity or Regular Visitor loses, damages or forgets their identification badge, they should go to and inform the reception staff.

3. Global rules for visitors

Visitors, including personnel from external entities who provide regular equipment maintenance services, should follow the procedures in force regarding the access to Deloitte Portugal's facilities.

Deloitte.