www.pwc.com.br

Corporate Security Statement

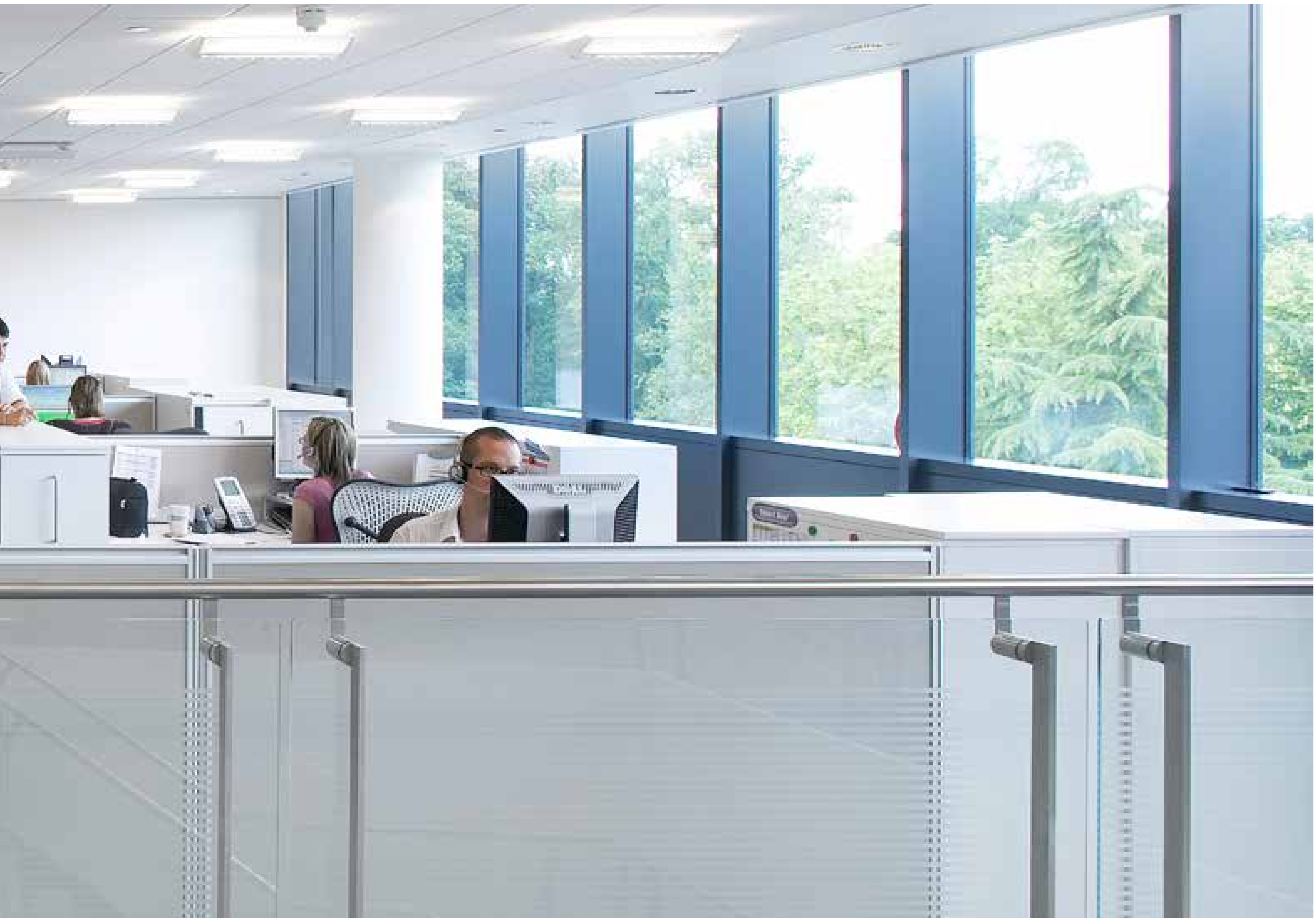
February 2013

pwc

Table of Contents

Overview

The leadership of PwC Brazil takes the security of its information, infrastructure and applications very seriously. Its commitment to corporate security is shown through the implementation of policies, controls and procedures, as well as the allocation of dedicated resources required for a formal Corporate Security organization. This document provides an overview of the security controls employed by PwC Brazil and is intended to be shared with its current and potential clients.



Disclaimer

In this document, “PwC Brazil” (“PwC” or “Firm”) refers to PricewaterhouseCoopers Brasil Ltda., which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity. The intent of this statement is to provide a brief overview of the security measures implemented to help protect the PwC information, infrastructure and applications. It does not represent all efforts made by the Firm to mitigate the risks related to Information Technology. These security measures do not guarantee complete protection.

The information contained in this statement is for current or potential clients and should not be distributed to others without permission from PwC.

Security Policy

PwC provides its employees with security policies and guidelines to communicate individual responsibilities with respect to safeguarding the Firm's resources. These policies are readily available to employees through the intranet portal and specific handbooks.

PwC utilizes an Information Security Policy based on ISO 27002. This Information Security Policy has been independently reviewed to ensure compatibility with and conformity to ISO/IEC 27002:2005.

All PwC new hires are required to undertake a series of training sessions, which among other issues address partner and staff responsibilities as they relate to our Code of Conduct, local policies and procedures, Information Security, and privacy. The Firm's Code of Conduct is available at www.pwc.com.br.

PwC partners and staff are required to complete an individual confirmation of their responsibility for the security of PwC's information to which they are granted access and to take due care to protect the technology equipment assigned to them.

Security Organization

Internal Security Organization

PwC has a formal Corporate Security organization led by the Chief Security Officer (CSO), who is responsible for all the security matters in the Firm and is assisted by a team of technology and security professionals.

The CSO reports to a Corporate Security Committee, which is formed by PwC partners and has the ultimate responsibility for the Firm's security-related decisions and strategies.

These security professionals hold a variety of certifications, including Certified Information Systems Security Professional (CISSP), ISO 27001 Lead Auditor, and other credentials that attest their proficiency in the field.

They participate in training programs and activities sponsored by industry-specific security groups to stay abreast of current security trends and issues.

Confidentiality Agreements

All PwC partners and employees, upon joining the Firm and/or during their employment period, as well as certain service providers, are required to sign non-disclosure and confidentiality agreements, demonstrating their commitment to the Firm and its information security.

Asset Management

Asset Inventory and Classification

PwC has established and maintains asset inventory processes for its main physical and information assets.

PwC's information security policy defines a four-tier scheme for classifying its main information assets, which are:

- Determination of the data classification level of information assets;
- Identification of the information owner;
- Identification of security risk factors; and,
- Identification of disaster recovery risk factors.

Information Handling

Information subject to legislative or regulatory requirements is identified through the asset inventory process. Security controls are established to address the relevant requirements. PwC professionals are regularly provided with instructions on identifying and handling the Firm's information.

Human Resources Security

People connecting to the PwC network are required to conduct themselves in a manner consistent with the Firm's security policies regarding, among other matters, confidentiality, business ethics and professional standards. PwC requires that communications via these connections comply with applicable laws and regulations, including those governing:

- Restrictions on the use of telecommunications technology and encryption;
- Copyrights and license agreement terms and conditions.

Confirmation of Security Responsibilities

All PwC professionals must participate in the Firm's annual regulatory process for Compliance Confirmation. This process requires that the professionals provide an individual confirmation of their responsibility for the security of PwC's information to which they have access, and to take due care to protect the technology equipment assigned to them.

All partners, staff and service providers sign a personal liability agreement acknowledging their responsibility for the professional equipment and tools received to develop their work, being also responsible for the physical security of these assets.

Appropriate Use

The PwC Code of Conduct and the Guide for Information Security and Protection address the appropriate use of electronic tools and technologies. Those who violate the Code or PwC policies and procedures will be subject to the sanctions established by the labor legislation in force, up to and including dismissal, depending on the seriousness of the violation.

Security Awareness Training

Security awareness training is a component of the PwC hiring process. An awareness program reinforces periodically the concepts and responsibilities defined in the Information Security Policy.

Termination Processes

PwC has established documented termination processes that define responsibilities for collection of information assets and removal of access rights for professionals who leave the Firm.

Physical and Environmental Security

Data Center Security

The following physical and environmental controls are incorporated into the design of the PwC Data Center:

- Separate protected facilities;
- Biometric entrance control;
- Internal and external cameras;
- Temperature and humidity control and monitoring;
- Smoke detection alarm;
- Lightning suppression;
- Transient voltage surge suppression and grounding;
- Redundant power feeds and UPS Systems; and,
- Physically secured network equipment areas and locked cabinets.

Data center access is limited to authorized personnel. Visitor access procedures and loading dock security protocols are established.

PwC Office Security

Physical access controls are implemented at all PwC offices in Brazil. Controls vary by location, but typically include card-reader access to facilities, on-premises security staff and defined procedures for visitor access control.

Communications and Operations Management

Operational Procedures and Responsibilities

PwC's IT organization has established and maintains controls over standard operating procedures, including a repository of procedures, formal review and approval processes, and revision management.

Change Control

PwC's IT organization has established and maintains a Change Management/Change Control process which includes risk assessment, test and retrieval procedures and review and approval components.

Development Environments

PwC maintains separate development and production environments. Development environments are required to be physically separated from production environments. The transfer of an application from development to production follows the procedures established in the Change Management/Change Control process.

Security Software Suite

PwC uses a combination of technology tools to provide a secure computing environment equipped with:

- Antivirus - the virus protection software package is loaded during the operating system start up process and performs on-access scans of all data. The software is configured to clean or delete infected files and provides other safeguards. Virus signatures are automatically and constantly updated through a process managed on a central basis.

- Antispyware - PwC installs spyware detection and removal of malicious software on all the Firm's computers.

- Desktop Firewall - PwC's desktop firewall software is automatically enabled and uses the Firm's standard configuration to protect against malicious network traffic, including internet-based network threats, untrusted networks or malicious software. Database configuration settings are secured against change, tampering or disablement by end users or malicious programs.

- Secure Remote Access - PwC utilizes virtual private network (VPN) software, configured to require dual factor authentication to enable secure remote access to its networks.

- Lotus Notes - The Firm uses Lotus Notes for a number of applications, including e-mail. Lotus Notes' security features are widely recognized in the market.

Spam Blocking and URL Filtering

PwC has deployed and regularly updates URL filtering software that blocks access to inappropriate web sites from its network. The Firm has also established and maintains e-mail gateway with spam-blocking and anti-virus software.

System Backup

Data center systems are routinely backed up for disaster recovery purposes. Restoration success metrics are maintained. PwC utilizes an information protection and storage provider for secure transport and offsite storage of backup media.

Wireless Networks

Only IT-managed wireless networks are permitted on PwC's network. Wireless access security controls include standards for encryption and authentication that are managed by PwC's IT department.

Network Security

All data center internet access points feature firewall segregation. Intrusion Prevention Systems (IPS) are positioned or installed at strategic locations in all internet connections. Firewall logging is enabled to track communications (failed and successful access attempts) between the internet and PwC's internal network. Console access to the firewalls is limited to administrative personnel using the Secure Shell protocol.

Secure Storage Media Disposition

PwC has established procedures for secure erasure or destruction of data center storage media prior to disposal, aimed at protecting the secrecy and confidentiality of information.

Application Security Reviews

Procedures for conducting application security reviews have been established and include the following:

- Asset classification;
- Infrastructure vulnerability scanning;
- Application security review; and,
- Database security review.

Access Control

Authorization and Authentication Controls

PwC follows a formal process to grant or revoke access to its resources. System access is based on the concepts of "least-possible-privilege" and "need-to-know" to ensure that authorized access is consistent with defined responsibilities. The Firm uses a combination of user-based, role-based and rule-based access control approaches.

PwC has established documented procedures for secure creation and deletion of user accounts, including processes to disable and/or delete accounts of employees temporarily away from the Firm. All PwC's partners and staff are required to agree to take reasonable precautions to protect the integrity and confidentiality of security credentials.

Privileged Access

Access to authentication servers at administrative, root or system levels is limited to those professionals designated by PwC.

Password Requirements

The Firm's security policy establishes requirements for password changes, reuse and complexity.

PwC requires the use of screensavers that reactivate after a period of inactivity through the use of a password.

Remote Access

PwC uses virtual private network (VPN) software to enable secure, internet-based remote access for its professionals. VPN users are required to authenticate using two-factor authentication; both a valid user name/password and a corresponding password-protected VPN token are required to create a VPN tunnel.

VPN tunnels are secured using 3DES or higher encryption.

The client software uses smart tunneling technology to ensure that communications between the host PC and the PwC network are transmitted via an encrypted VPN tunnel.

Communications to internet-routed addresses will be conducted outside of the established VPN tunnel.

Also, session timeout settings are configured to automatically disconnect the user from a session after a period of mouse or keyboard inactivity.

Processes are established to limit third-party remote access to PwC systems. Such access requires approval from the security organization and access is limited to those systems required for the third-party to complete the task and is monitored on a regular basis.

Computer Security

All PwC desktops and laptops are protected by hard drive encryption software through the 256-bit AES encryption algorithm. The software enforces password controls and uses a dynamic password time-out to prevent brute force password attacks.

Additionally, the software is bound to the hard drive, protecting not only the operating system, but also the data.

Laptop computers are provided with a locking steel cable to secure the equipment and deter theft. The internal policy that regulates the use of laptop is widely disclosed to PwC professionals. Training is delivered to new employees to educate them about theft and to encourage behavior that will help protect laptops against it.

Mobile Devices

Mobile device access is only permitted from Blackberry devices configured in accordance with the Firm's security policy.

This security policy requires a password to be entered to access the device, that the information in the device be erased after ten incorrect access attempts and allows remote erasure if the Blackberry device is reported lost or stolen.

Information Systems Development Cycle

PwC has established a methodology to manage the acquisition, development and maintenance of systems. Key security components related to this methodology include:

- Business criticality assessment;
- Risk assessment;
- Security organization involvement in project reviews and key contracts; and,
- Utilization of established change control processes to transfer changes from the development to the production environment.

Internal and External Network Scanning

PwC utilizes multiple vulnerability scanning tools to assess its internal and externally facing network environments. These tools are selected and configured to match the requirements of PwC's IT infrastructure, and are updated on an ongoing basis. Processes are established to assess and correct the vulnerabilities discovered.

Patch Management

PwC has patch management processes and tools to assess and deploy operating system and application-specific patches and updates.

This process includes steps to evaluate vendor supplied patches to determine servers that require patches and updates, to document procedures for patching and updating servers, and to deploy patches and updates in a timely manner to protect the PwC infrastructure.

PwC continually reviews patches and updates, as they are released, to determine their criticalities. Patches released on a regularly scheduled basis are applied following the release; patches released on a regular basis and others determined to be critical are applied as needed to ensure protection from vulnerabilities.

Information Security Incident Management

PwC professionals are made aware that security incidents must be reported immediately. PwC has documented procedures for the receipt of security incident reports. PwC's Corporate Security organization has a documented incident response process which includes:

- Escalation process;
- Pre-defined roles and responsibilities; and,
- Virus response plan.

Business Continuity Management

PwC maintains a Recovery Plan for its critical operations.

The purpose of this plan is to provide a set of guidelines and corresponding processes for supporting business processes in the event of a disaster.

Examples of disaster situations that could lead to the plan activation are destructive events such as fire, power or communication blackouts, storms, floods, hurricanes, earthquakes, civil unrest, sabotage, etc.

While PwC has taken many steps to mitigate the risk of a disaster, the Firm recognizes that there are variables beyond its control.

Compliance

Vulnerability Scanning

PwC has established processes for performing periodic vulnerability scans of its IT systems. These procedures specify the use of multiple vulnerability scanning software packages, the creation of vulnerability assessment reports, and the presentation of vulnerability scanning results to the IT Operations organization and IT leadership.

Access to vulnerability scanning tools is restricted to authorized members of the security team.

Internal Audit

PwC has an Internal Audit organization responsible for assessing internal operations, including the Security and IT organizations.

Ethics & Compliance

PwC has implemented communication channels (telephone hotline and email) which can be used to report, either anonymously or not, any misconduct of its professionals or third-parties with respect to the Code of Ethics and laws and regulations referring to property, secrecy, confidentiality, ethics, business conduct, as well as to internal policies and procedures.

Privacy Organization

PwC has established Data Protection rules that define, among other issues, the standards of behavior regarding the protection of PwC information.

PwC Brazil Offices

São Paulo - SP
Av. Francisco Matarazzo, 1400
05001-903 - São Paulo/SP
Torre Torino - Água Branca
Telefone: (11) 3674-2000

Barueri - SP
Alameda Caiapós 243, Térreo
Centro Empresarial Tamboré
06460-110 - Barueri/SP
Telefone: (11) 3509-8200
Fax: (11) 3509-8500

Belo Horizonte - MG
Rua dos Inconfidentes, 1190 - 9º
30140-120 - Belo Horizonte/MG
Telefone: (31) 3269-1500
Fax: (31) 3261-6950

Brasília - DF
SHS - Quadra 6
Conjunto A - Bloco C
Edifício Business Center Tower
Salas 801 a 811 - Brasília/DF
70322-915 - Caixa Postal 08850
Telefone: (61) 2196-1800
Fax: (61) 2196-1820

Campinas - SP
Rua José Pires Neto, 314 - 10º
13025-170 - Campinas/SP
Telefone: (19) 3794-5400
Fax: (19) 3794-5454

Caxias do Sul - RS
Rua Os 18 do Forte, 1256 - Sala 11
95020-471 - Caxias do Sul/RS
Telefone: (54) 3202-1466
Fax: (54) 3225-6789

Curitiba - PR
Al. Dr. Carlos de Carvalho, 417 - 10º
Curitiba Trade Center
80410-180 - Curitiba/PR
Telefone: (41) 3883-1600
Fax: (41) 3222-6514

Florianópolis - SC
Avenida Rio Branco, 847
Salas 401/ 402/ 403 e 409
88015-205 Florianópolis/SC
Telefone: (48) 3212-0200
Fax: (48) 3212-0210

Porto Alegre - RS
Rua Mostardeiro, 800 8º e 9º
Edifício Madison Center
90430-000 - Porto Alegre/RS
Telefone: (51) 3378-1700
Fax: (51) 3328-1609

Recife - PE
Rua Padre Carapuceiro, 733 - 8º
Edifício Empresarial Center
51020-280 - Recife/PE
Telefone: (81) 3465-8688
Fax: (81) 3465-1063

Ribeirão Preto - SP
Av. Antônio Diederichsen, 400
21º e 22º - Edifício Metropolitan
Business Center
14020-250 - Ribeirão Preto/SP
Telefone: (16) 2133-6600
Fax: (16) 2133-6685

Ribeirão Preto - SP | Outsourcing
Rua Rui Barbosa, 1145 - 12º
14015-120 - Ribeirão Preto/SP
Telefone: (16) 3635-4303
Fax: (16) 3632-4424

Rio de Janeiro - RJ
Av. José Silva de Azevedo Neto 200,
1º e 2º - Torre Evolution IV
Barra da Tijuca
22775-056 - Rio de Janeiro/RJ
Telefone: (21) 3232-6112
Fax: (21) 3232-6113

Rio de Janeiro - RJ
Rua da Candelária 65, 20º - Centro
20091-020 - Rio de Janeiro/RJ
Telefone: (21) 3232-6112
Fax: (21) 2516-6319

Salvador - BA
Av. Tancredo Neves, 620 - 30º e 34º
Ed. Empresarial Mundo Plaza
41820-020 - Salvador/BA
Telefone: (71) 3319-1900
Fax: (71) 3319-1937

São José dos Campos - SP
Rua Euclides Miragaia, 433
Cjs. 301 e 304
12245-550 - São José dos Campos/SP
Telefone: (12) 3913-4505
Fax: (12) 3942-3329

Sorocaba - SP
Rua Riachuelo, 460 - 5º
Edifício Trade Tower
Salas 501, 502, 503 e 504
18035-330 - Sorocaba/SP
Telefone: (15) 3332-8080
Fax: (15) 3332-8076