

## **INFORMATION SECURITY POLICY**

Pearce & Pearce, Inc. maintains electronic and hardcopy information assets which are essential to performing services for our clients. Similar to any other capital resources owned by the company, these resources are to be viewed as valuable assets over which the company has both rights and obligations to manage, protect, secure, and control. Pearce & Pearce, Inc. employees, contractors, and other affiliates are expected to utilize these information assets for only legitimate business purposes while assuring the Confidentiality, Integrity and Availability of the assets.

The Board and management of Pearce & Pearce, Inc., located at 1945 W. Palmetto St., Suite 105, Florence, SC 29501, which operates in special risk insurance and student insurance, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the organization in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with Pearce & Pearce, Inc. goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, for e-commerce and for reducing information-related risks to acceptable levels.

The Pearce & Pearce, Inc. current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The risk assessment, Statement of Applicability and risk treatment plan identify how information-related risks are controlled. The Chief Operating Officer is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

The purpose of the Policy is to protect the Company's information assets from all threats, whether internal or external, deliberate or accidental.

In particular, business continuity and contingency plans, data back up procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Manual and are supported by specific, documented policies and procedures.

All employees of Pearce & Pearce, Inc. and certain external parties identified in the ISMS scope document are expected to comply with this policy and with the ISMS that implement this policy. All staff, and certain external parties, will receive and be required to provide appropriate training to individuals supporting Pearce & Pearce, Inc. Violations of the security policy will be investigated in accordance with the company's disciplinary procedures and will incur disciplinary measures the same as violations of other company policies.

The ISMS is subject to continuous, systematic review and improvement.

Pearce & Pearce, Inc. has established an Information Steering Committee, chaired by the CEO/COO and including the Chief Security Officer, Information Security Manager and other executives/specialists/risk specialists to support the ISMS framework and to periodically review the security policy.

Pearce & Pearce, Inc. has completed the certification of its ISMS to ISO27001:2005 as of January 03, 2008.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, “information security” is defined as:

**preserving**

This means that management, all full time or part time staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policy and procedures identified in section 13 of the Manual) and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in the Pearce & Pearce, Inc. disciplinary policy. All staff will receive information security awareness training and more specialized staff will receive appropriately specialized information security training.

**the confidentiality**

This involves ensuring that information is only accessible to those authorized to access it and therefore preventing both deliberate and accidental unauthorized access to Pearce & Pearce, Inc.’s information and proprietary knowledge and its systems [including its network(s), website(s), extranet(s), and e-commerce systems].

**the integrity**

This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorized modification, of either physical assets or electronic data. There must be appropriate contingency [including for network(s), e-commerce system(s), web site(s), extranet(s)] and data back-up plans, and security incident reporting. Pearce & Pearce, Inc. must comply with all relevant data-related legislation in those jurisdictions within which it operates.

**and the availability.**

This means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The computer network [identified as part of the scope in section 1 of the Manual] must be resilient and Pearce & Pearce, Inc. must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

*of the physical assets - Non IT*

The physical non IT related assets of Pearce & Pearce, Inc. including but not limited to headquarters office, telephone systems, filing systems, Fax machines, APS and copiers.

*of the physical assets - IT*

The physical IT related assets of Pearce & Pearce, Inc. including but not limited to computer hardware, data cabling, fax server, firewall appliance, laptops, printer, and T-1 line.

*the information assets*

The information assets of Pearce & Pearce, Inc. include information printed or written on paper, transmitted by mail or shown in films, or spoken in conversation, as well as information stored electronically on servers, web site(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs as well as on CD ROMs, floppy disks, USB sticks, back up tapes and any other digital or magnetic media, and information transmitted electronically by any means.

*the software assets*

The software assets of Pearce & Pearce, Inc. include the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, custom programs, etc).

*the supporting documents*

The supporting document assets of Pearce & Pearce, Inc. include policies, information security procedures and work instructions, SLAs, disaster recovery plans, HR Procedures and business plans.

*the services*

The service assets of Pearce & Pearce, Inc. include HVAC, ISP, electric power, firewall monitoring, and telecommunication services.

*and the intangible assets*

The intangible assets of Pearce & Pearce, Inc. include company reputation, public image, client relationship, and company intellectual property.

Pearce & Pearce, Inc. and partners are part of our integrated network and have signed up to our security policy and have accepted our ISMS.

---

All managers are directly responsible for implementing the Policy within their business areas, and for adherence by their staff.

It is the responsibility of each employee to do everything reasonable and within their power to ensure that the Policy is adhered to.

Changes to this Policy in response to changing operational, legislative, regulatory and contractual requirements will be made as necessary by the Information Security Manager.

The ISMS is the Information Security Management System, of which this policy, the information security manual (“the Manual”) and other supporting and related documentation is a part, and which has been designed in accordance with the requirements contained in ISO27001:2005.

A SECURITY BREACH is any incident or activity that causes or may cause a break down in the availability, confidentiality or integrity of the physical or electronic information assets of the Organization. All information security incidents, actual or suspected, will be reported to and investigated by the Information Security Manager.