Information Security Policy

Companies in the PDS Group have controls to protect the confidentiality, integrity, and availability of information that is owned by or entrusted to the company. The intent of the document is to provide assurances to customers, potential customers, and any other interested parties that the information in the company's custody is properly protected –and that the protections in place are consistent with any appropriate compliance requirements.

Overview

The group of affiliated PDS companies ("PDS Group Companies") provide software, consulting, and online services. The Boards of Directors and management of PDS Group Companies are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to compete in the market place and maintain its legal, regulatory and contractual compliance and commercial image.

To achieve this, PDS Group Companies have implemented a Group-wide Information Security Management System (ISMS) in accordance with the international standard ISO/IEC 27001:2013 requirements to ensure that all information within the company's custody is properly and adequately protected. The ISMS is subject to continuous systematic review and improvement.

The PDS Group demonstrates its commitment to information security by:

- Dedicating resources to security in terms of staff, budget, and technology.
- Investing in security technology and in highly available and recoverable systems and facilities.
- Continually evaluating and improving procedures related to security.
- Adopting policies, communication and training related to promote employee awareness.
- Striving to maintain compliance with all applicable legal and industry requirements.

Security Policies and Standards

The PDS Group uses security policies and standards to support business objectives within its information systems and processes. These policies and standards are implemented, communicated, and reviewed on a regular basis and are a reflection of the executive management team's commitment to information security.

Policies and standards are in place to govern the protection of the company's information assets and any information assets of our customers (and others) that have been entrusted to a PDS Group company.

Human Resources

The PDS Group of companies employ staff whose responsibility is the protection of information. In addition, it is the responsibility of all of employees to be aware of information security issues within their daily work. In order to promote awareness, PDS Group employees are provided with training on topics such as the company's security policies, their responsibilities to protect the confidentiality of information entrusted to them, the appropriate use of resources, the extra care required for the protection of mobile devices, and other related topics.

Confidentiality Agreements

PDS Group companies enter into confidentiality or non-disclosure agreements with its vendors, contractors, employees and clients to contractually safeguard personal and other confidential information belonging to a PDS Group company or in the custody of a PDS Group company.

Audits and Assessments

Regular risk assessments are performed to help the company identify any potential risks to its information assets and to help prioritize efforts to mitigate those risks.

Periodically, the company also engages external firms to perform more in-depth evaluations of its security controls by conducting penetration testing and other similar exercises.

In addition to external reviews, internal tests are conducted on a regular basis to ensure compliance and verify control effectiveness. Vulnerability scans are conducted, and the results of these scans are used to identify vulnerabilities to be addressed and to prioritize the efforts of those staff that are responsible for keeping PDS Group systems up to date and protected.

Physical Security

All sites hosting PDS Group company information (or information that is managed by a PDS Group company on the behalf of others) are secured structures protected by defined security perimeters. These facilities are protected by physical security barriers and entry controls designed to prevent unauthorized access, damage, and interference. Fire suppression, environmental controls, and uninterrupted power supplies are all in place, as are security cameras to monitor the facilities and all entrances to them.

Operational Security

Responsibilities and procedures for the management and operation of information processing facilities are established and separation of duties by function across the organization has been implemented.

Operational change to systems is controlled through various defined change management processes.

Access Control

Access to information, information processing facilities, and business processes are controlled on the basis of business and security requirements. Access control rules take into account the basic principle of “need-to-know” and the sensitivity of corporate and personal information.

Layers of security controls limit access to information. These include controls at the network, application, operating system, and database levels. Passwords are used in conjunction with each of these layers; they are subject to defined password construction rules and must be changed at regular intervals. Password administration and management are controlled processes that generate automated audit records.

Data Communications Security

Technologies such as SSL (TLS), and IPsec are used to encrypt data when in transit over public networks. The use of such technologies is dependent upon the level of sensitivity of the information, both corporate and personal.

Computer Security Measures

Various security technologies are deployed within the infrastructures and include firewalls, anti-virus, antispyware, encryption, and intrusion detection systems and processes.

Security data is logged and regularly reviewed to identify policy violations and security incidents. Incidents are documented and investigated to determine severity, root cause, and follow-up actions required. Measures to be taken to prevent re-occurrence are also identified, documented, and implemented as needed.

Disaster Prevention and Recovery

Adequate back-up capabilities exist to ensure that all essential information and software can be recovered following a disaster or media failure. Backup information is stored at a remote secure location, at a sufficient distance to escape any damage from a disaster at the primary site. Backup media is protected against unauthorized access, misuse or corruption during transportation beyond the data center boundaries.

Combinations of preventive and recovery controls are implemented to help protect from harm due to loss of data or processing capabilities. These controls are designed based on an assessment of risk and are meant to keep the harmful effects of any outages to a minimum. The processes making up these control measures are tested on a regular basis.

Contact information:

Security@PDS.Group