

PCI DSS has been in our sights for a while as it is being raised more and more often by our clients and of course is getting a lot of press. Staff and contractor supply to the Payment Card Industry has to be managed within the requirements of PCI DSS. We consider it mandatory to build PCI DSS into the recruitment process. The requirements of the Data Protection Act have a close parallel to the PCI standards.

Our PCI DSS Policy follows.

1. THE PCI DSS SCHEME IN OUTLINE

Aqua Resources Group is a major supplier to the card industry in the provision of recruitment services; contract, permanent and interim personnel as well as salary surveys, HCM solutions and consultancy provision.

Aqua is not a vendor or merchant as prescribed by the standard however such is our involvement in the sector that we have taken the decision to mirror PCI DSS compliance and validation requirements for three reasons:

- 1.1. To map onto our clients' security strategies
- 1.2. To enhance our existing Data Security standards
- 1.3. To align ourselves with the industry standard for marketing and competitive entry purposes.

2. REQUIREMENTS OF THE PCI SCHEME

Similar to other Security Protocols the scheme demands:

2.1. Secure Network

- (a) Firewall
- (b) Internal Password Issuance and Control

2.2. Data Protection

- (a) Encryption
- (b) Data Security Systems
- (c) Data Transmission Security, e.g. Masking

2.3. Vulnerability Protection

- (a) Anti Virus
- (b) Secure Applications, Networks and Domain

2.4. Access Control

- (a) Unique User Passwords
- (b) Restricted Access
- (c) Remote Access Controls
- (d) Physical Protection of Data and Data Systems

Middle East Operations

Tel: +441273 573 865
Email: recruit@argme.com
Web: www.argme.com



Service Portfolio
Executive Search and Selection
Interim Management
HR Consultancy



2.5. Monitoring and Testing

- (a) Tracking and User Access Monitoring
- (b) Regular Testing [Penetration and Access]

2.6. Policy

- (a) DP Policy and Controls
- (b) DSS Policy

3. DELIVERY TO PCI REQUIREMENTS

3.1. Build and Maintain Secure Network

- (a) Aqua Resources Group has a secure network with no external access possible other than through the firewall both in the UK and Bahrain. Additionally each user station has its own sub-firewall. As a Microsoft Partner we maintain the latest installation of all anti intrusion software.
- (b) The Group is installing a new network in 2006. The network will be protected by VPN Capable Firewalls, Sophos or Razorgate anti Spy/Spam Ware and PIX Technology.
- (c) Company policy is that no vendor-supplied passwords, defaults or other standard 'access' measures are allowed. This is monitored by our system administrator, database access passwords are changed every 3 months.

3.2. Protect Customer Data

- (a) Stored Data [CV and Applicant Information] is held on two systems; our core database and our office system. Protection on our core system is provided by our system provider, Piersoft, who deploy a multi layered security system that protects and segments our data. Piersoft have three layers of redundancy [mirrored and off site servers] as part of the BCM mandate. Access to the system's data is strictly by unique user access as in 3.1.c and is regularly monitored for integrity.
- (b) Office system data is protected by network security and by individual user access. CVs and other applicant data is stored centrally on a protected drive.
- (c) We ensure that all candidate data is fully validated; this includes eligibility to work in the host country, qualifications, work references, identity and credit/security checks were required. A mandatory process of screening candidates is in place and has been audited and approved to the REC Gold Audit Standard in April 2006.
- (d) Hard copy candidate and job data is held only as part of WIP files and is cross-shredded after use.
- (e) All aspects of data protection are audited monthly as an integral part of our DP Policy encompassing the eight principals of Data Protection.

3.3. Vulnerability Management

- (a) The Group deploys the network version of AVG which has proved highly dependable since its introduction in 2004. When the Group installs the new system in 2006 we will be scaling up to a MS Small Business Server/PIX/Sophos or Razorgate environment [specification available].
- (b) Vulnerability assessment has been a key driver in our move to a higher end solution. We do not intend to develop any software. Vendor supplied software deployed by the Group has to meet our security standard and be warranted by the vendor.



3.4. Access Control Measures

- (a) Certain system privileges are restricted, e.g. only the system administrator can change passwords on the company's core systems.
- (b) The use of auto complete password functionality is forbidden and disabled on all machines.
- (c) Unique logons control access to both office and database systems. Database logons are changed every 3 months by the system administrator.
- (d) Staff are encouraged to change their access passwords on their workstation on a frequent but irregular basis.
- (e) Email user passwords are changed every 6 months by the system administrator.
- (f) When a client exceeds their factor limit no commission is available until the client is back within their limit or their limit is increased to give adequate cover.
- (g) Our operating environment is secure to normal office standards. The significant enhancements to physical security are; security bars installed at all windows, double locking main access door, manned reception, machine unique ids and off site backup storage. All off site backups are fully encrypted using File2File by Cryptomathic.

3.5. Monitoring and Test

- (a) We monitor our office and database systems weekly for integrity and user access.
- (b) We intrusion test our systems once a month.
- (c) Our DP Policy demands that we audit for compliance monthly with each member of staff and quarterly for corporate compliance.

3.6. Security Policy

- (a) The Group has in place both a Data Protection and Data Security Policy of which this document forms an integral part.
- (b) Our security policy forms part of our induction and ongoing training programme. All staff sign off on the Group's DP policy and guidelines.

4. REC ACCREDITATION

- 4.1. As part of our continuous improvement policy we have recently been audited by our industry body, REC, against their highest standard – the REC Gold Audit. The assessment was conducted by SGS the world leader in assessment and accreditation.
- 4.2. The accreditation demands compliance with every Act of Parliament associated with our industry; concerning Data Protection, Immigration, Discrimination, Agencies, Employment, etc.
- 4.3. It also requires that we comply with the industry Code of Conduct, a stringent requirement for all agencies and employment businesses.