Information Security Policy

	Process Owner		QA Approval
Position	IT Systems Manager	Position	Director of Operations
Date	23/07/2013	Date	23/07/2013

Great Minds Think viglen

Document History

Date	Issue Number	Issued by	Changes
25/10/10	7	HM	
16/06/10	8	AW	Addition of Objectives, Document Ownership and change history
18/08/11	8.1	AW	Ownership correction
02/09/11	9	HM	Clause 9.11 inserted with reference to Blackberry devices & typographical error corrected
14/02/2012	9.1	AW	Clause 6.2 amended to include 'a director' 6.7 and 6.8 references to user names removed, 9.11 – or IT Manager approved devices inserted, document alignment reformatted and up issued.
13/07/2012	9.2	AW	Addition of text on objectives review
23/07/2013	10	HM/EAJ	Document reviewed and minor changes applied to 3.7, 4.7, 5.3.4 and the removal of 6.15. Document reformatted, with minor grammar updates, document up-issued

TABLE OF CONTENTS

I.T. Security Policy

1. POLICY STATEMENT

The purpose of this document is to provide an Information Security Policy that will provide a framework for managing information security within the organisation.
It is the intention that this document shall provide adequate policy for protection of all corporate data and proprietary software systems, to ensure the continued confidentiality and availability of data and programs to all authorised members of staff and to ensure the integrity of all data and configuration controls.

2. Objectives

- To ensure Information is only accessible to authorized persons from within or outside our company
- To ensure Confidentiality of information is maintained
- To ensure integrity of information is maintained
- To ensure business continuity plans are established maintained and tested
- To ensure all personnel are trained on information security and are informed that compliance is mandatory
- To ensure all breaches of security and suspected weaknesses are reported and investigated
- To ensure procedures exist to support the policy, including virus control measures, passwords and continuity plans
- To ensure business requirements for availability of information and systems are met
- To ensure the director responsible for security maintains the policy
- To ensure all managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments

These objectives will be monitored and measured in terms of compliance within the quality management review quarterly meetings.

3. Summary of Main Security Policies

3.1. Confidentiality of all data shall be maintained through discretionary and mandatory access controls.

3.2. Information will be handled appropriately and in accordance with the Information Classification Policy (MSD-IS-PL003).

3.3. Sensitive information will be removed from desks when not required.

3.4. Only authorised and licensed software shall be installed, and installation shall only be performed by I.T. Department staff and, where appropriate, the installation shall be carried out by the user under the guidance and instruction of the IT Department staff.

3.5. The use of unauthorised software is prohibited. In the event of unauthorised software being discovered it shall be removed from the workstation immediately, invoking disciplinary proceedings in accordance with the company handbook.

3.6. Data shall only be transferred for the purposes determined in the Organisation's data-protection policy (MSD-IS-PL001).

3.7. All removable media from external sources shall be virus checked before they are used within the Organisation. The internal use of removable devices such as USB Pen Drives, Portable Hard Drives is prohibited, unless authorised at the relevant level.

3.8. Passwords shall be kept private and shall not be divulged to any person.

3.9. Workstation configurations shall only be changed or modified by I.T. Department staff.

3.10. It is the responsibility of the End User to ensure that any data that is stored locally on Workstations/Laptops is regularly copied to the file servers.

3.11. Encryption is limited to the credit card processes within the ERP system.

4. VIRUS PROTECTION

4.1. The I.T. Department shall have available at all times up to date virus scanning software for the scanning and removal of suspected viruses and malicious code.

4.2. Corporate file-servers shall be protected with virus scanning software where deemed necessary.

4.3. Workstations shall be protected by virus scanning software which shall not be disabled or tampered with by the user.

4.4. All workstation and server anti-virus software shall be regularly updated with the latest anti-virus patches by the I.T. Department.

4.5. No disk that is brought in from outside the Organisation shall be used until it has been scanned.

4.6. All removable media containing executable software (software with .EXE and .COM extensions) shall be 'write' protected wherever possible.

4.7. No customer/supplier shall be authorised to connect their own hardware be it PC or Laptop onto the Viglen internal infrastructure, and limited to the Viglen Visitor Network only.

4.8. All demonstrations by vendors shall be run on their machines and not on the Organisation's.

4.9. New commercial software shall be scanned before it is installed as it occasionally contains viruses.

4.10. All removable media brought in to the Organisation by field engineers or support personnel shall have to be scanned before they are used on site.

4.11. To enable data to be recovered in the event malicious attack, regular server backups shall be taken by the I.T. Department.

4.12. Users shall be kept informed of current procedures and policies.

4.13. Employees shall be accountable for any breaches of the Organisation's anti-virus policies.

4.14. Anti-virus policies and procedures shall be reviewed regularly.

4.15. In the event of a possible virus infection the user must inform the I.T. Department immediately. The I.T. Department shall then scan the infected machine and any removable media or other workstations to which the virus may have spread and eradicate it.

5. PHYSICAL SECURITY OF COMPUTER EQUIPMENT

Physical Security of computer equipment shall comply with the guidelines as detailed below.

5.1. DEFINITIONS

5.1.1. COMPUTER SUITE

Fileservers plus all inter-connected wiring, fixed disks, telecommunication equipment, ancillary, peripheral and terminal equipment linked into the fileservers, contained within a purpose built computer suite.

5.1.2. *COMPUTER EQUIPMENT*

All computer equipment not contained within the **COMPUTER SUITE** which shall include **PCs**, monitors, printers, disk drives, modems and associated and peripheral equipment.

5.2. REQUIRED PHYSICAL SECURITY

5.2.1. The computer suite shall be a secure and temperature controlled environment.

5.2.2. Access to the computer suite shall restrict to I.T Department staff. All other access shall be upon explicit permission of IT Manager or Company Directors and shall be supervised by a Member of I.T. Department.

5.2.3. No water, rain water or drainage pipes shall run within or above the computer suite to reduce the risk of flooding

5.2.4. Power to the File Servers and critical equipment shall be on UPS to safeguard against power surges and power failure.

5.2.5. No Computer Equipment shall be taken off site without the prior express permission of Directors, the temporary removal for must be completed and signed a copy of which shall be kept by the security officers at the point of exit.

5.2.6. All computer equipment i.e. Laptops, printers and external storage device that are issued to external employees shall need to be issued based on a SOR (Sales or Return) order and invoice.

5.2.7. Copies of SOR Invoice shall be held by I.T Department, HR Department, Security Officers and the Employee.

5.2.8. The Security officer shall check the serial number of equipment against their records.

5.3. REQUIRED PHYSICAL DATA SECURITY

5.3.1. Data kept within the Organisation is subject to Data Protection Act 1998.

5.3.2. No Information or data shall be divulged to third parties unless consent has been obtained.

5.3.3. All Data stored on the File Severs shall be backed up according to backup procedure and shall be kept in secure environment.

5.3.4. Data Backups shall be periodically checked, to ensure quality and accuracy of the backup, by restoring from disk in temporary location. The restored data may be deleted after verification of quality and accuracy of the backup.

6. ACCESS CONTROL

6.1. Users shall only be given sufficient rights to all systems to enable them to perform their job function. User rights shall be kept to a minimum at all times and shall be based on the details in the "Systems user requirements form" (MSD-HR-016) completed by the employee's manager at the start of employment.

6.2. Issue of laptops to new employees shall be subject of explicit permission of a Director.

6.3. Users requiring additional access to systems or changes to their current access shall make a written application via the "Systems user requirements form" (MSD-HR-F016).

6.4. Where possible no one person shall have full rights to any system. The I.T. Department shall control network/server passwords and system passwords shall be assigned by the system administrator in the end-user department.

6.5. The system administrator shall be responsible for the maintaining the data integrity of the end-user department's data and for determining end-user access rights.

6.6. Access to the network/servers and systems shall be by individual username and password.

6.7. Passwords shall not be shared by users.

6.8. Passwords shall not be written down.

6.9. Usernames shall consist of employee first name and initial of surname wherever possible.

6.10. Intruder detection shall be implemented where possible. The user account shall be locked after 3 incorrect attempts.

6.11. The I.T. Department shall be notified of all employees leaving the Organisation's employment by HR Department. The I.T. Department shall then remove the employee's rights to all systems upon departure or before as appropriate.

6.12. Network/server supervisor passwords and system supervisor passwords shall be stored in a secure location in case of an emergency or disaster, for example a fire safe in the I.T. Department.

6.13. Access to the network/servers shall be restricted to normal working hours. Users requiring access outside normal working hours must request such access in writing on the forms provided by the I.T. Department.

6.14. File systems shall have the maximum security implemented that is possible. Where possible, users shall only be given Read and Filescan rights to directories, files shall be flagged as read only to prevent accidental deletion.

6.15. Sub-Contractor and third party access to the internal systems, internally or externally, shall not be available. Unless explicit permission has been obtained from Directors and appropriate non-disclosure agreement has been signed.

7. LAN Security

7.1. LAN equipment, hubs, bridges, repeaters, routers, switches shall be kept in computer suite.

7.2. All unused workstations must be switched off outside working hours.

7.3. All network wiring shall be fully documented.

7.4. All unused network points shall be de-activated when not in use.

7.5. Users must not place or store any item on top of network cabling.

7.6. Redundant cabling schemes shall be used where possible.

7.7. The use of LAN analyser and packet sniffing software is restricted to the I.T. Department.

7.8. LAN analysers and packet sniffers shall be securely locked up when not in use.

7.9. All servers shall be kept securely under lock and key.

7.10. Access to the system console and server disk/tape drives shall be restricted to authorised I.T. Department staff only.

7.11. All servers shall be fitted with UPSs that also condition the power supply.

7.12. All hubs, bridges, repeaters, routers, switches and other critical network equipment shall also be fitted with UPSs.

7.13. In the event of a mains power failure, the UPSs shall have sufficient power to keep the network and servers running until the power can be restored or the orderly shutdown process is initiated.

7.14. Software shall be installed on all servers to implement an orderly shutdown in the event of a total power failure.

7.15. All UPSs shall be tested periodically.

7.16. The I.T. Department shall keep a full inventory of all computer equipment and software in use throughout the Company using auditing software.

8. SERVER SPECIFIC SECURITY

This section applies to Windows and Novell servers.

8.1. The operating system shall be kept up to date and patched on a regular basis.

8.2. Servers shall be checked periodically for viruses.

8.3. Servers shall be locked in a secure room.

8.4. Where appropriate the server console feature shall be activated.

8.5. Users possessing Admin/Administrator rights shall be limited to trained members of the I.T. Department staff only.

8.6. Use of the Admin/Administrator accounts shall be kept to a minimum.

8.7. Assigning security equivalences that give one user the same access rights as another user shall be avoided where possible.

8.8. Users access to data and applications shall be limited by the access control features.

8.9. Intruder detection and lockout shall be enabled.

8.10. All unused workstations shall be switched off outside working hours.

8.11. All accounts shall be assigned a password of a minimum of six characters.

8.12. Unique passwords shall be used.

8.13. The number of grace loginsshall be limited to three.

8.14. The number of concurrent connectionsshall be limited to one. The only exceptions to this shall be based on the justification approved by the IT Department.

8.15. Network login time restrictionsshall be enforced preventing users from logging in to the network outside normal working hours.

9. WIDE AREA NETWORK SECURITY

9.1. Wireless LANs shall make use of the most secure encryption and authentication facilities available.

9.2. Users shall not install their own wireless equipment under any circumstances.

9.3. Dial-in modems shall not be used if at all possible. If a modem must be used, dial-back modemsshall be used. The Dial back number shall be fixed prior to the service initiation and shall only be controlled by the I.T. Department staff

9.4. Modems shall not be used by users without first notifying the I.T. Department and obtaining their approval.

9.5. Where dial-in modems are used, the modem shall be unplugged from the telephone network and the access software disabled when not in use.

9.6. Modems shall only be used where necessary, in normal circumstances all communications shall pass through the Organisation's router and firewall.

9.7. All bridges, routers and gateways shall be kept locked up in Computer Suite

9.8. Unnecessary protocols shall be removed from routers.

9.9. The preferred method of connection to outside Organisations is by a secure VPN connection, using IPSEC or SSL. This connection method is severely restricted to I.T. Department.

9.10. All connections made to the Organisation's network by outside organisations shall be logged.

9.11. Blackberry Devices

Only IT Manager approved devices or company issued Blackberrys are permitted to be configured to collect business email. All Blackerrys are deployed with a mandatory screen lock which activates when holstered. The device also automatically locks after a period of non-activity when un-holstered.

It is good practice to lock the device when not in use rather than waiting for the auto-lock feature to operate. If a Blackberry is stolen it is your responsibility to inform a member of systems of the theft so that the

device can be remotely wiped and locked down, to prevent unauthorised access to your Blackberry.

10.TCP/IP & INTERNET SECURITY

10.1. Permanent connections to the Internet shall be via the means of a firewall to regulate network traffic.

10.2. Permanent connections to other external networks, for offsite processing etc., shall be via the means of a firewall to regulate network traffic.

10.3. Network equipment shall be configured to close inactive sessions.

10.4. Workstation access to the Internet shall be via the Organisation's proxy server and website content scanner.

10.5. All incoming e-mail shall be scanned by the Organisation's e-mail content scanner, for virus and unwanted content.

10.6. Organisations shall keep a log and a copy of all incoming and outgoing emails.

10.7. Access to the internet shall be based on users Job requirement and shall be controlled by membership of security groups.

10.8. Access to the non work related websites shall be severely restricted.

10.9. Downloading and accessing of non work related sites shall result in disciplinary proceedings being initiated.

11. RISK ANALYSIS AND INCIDENT REPORTING

11.1. Risk Analysis

11.1.1. All Server hardware and software upgrades shall be carried out on a duplicated test system(s), where possible, to assess the impact of the upgrade.

11.1.2. All new implementation of systems e.g. Software, Servers and network hardware and topology shall be trialled prior to going live.

11.1.3. A recent copy of live data where appropriate shall be used for the trail process.

11.1.4. The trialled system shall be decommissioned and data used destroyed upon the completion of the trial.

11.1.5. Access to the trail system shall be subject to the Access control policies outlined in section 4 of this document.

11.1.6. An ongoing risk assessment is carried out to ensure maximum availability and protection of the information systems.

11.1.7. Incident Capture and Reporting

11.1.8. Security breaches and weaknesses will be reported to the appropriate department (Systems for virtual security events and Security for physical security events) and logged accordingly.

11.1.9. The logged information is subject to analysis to determine the cause and operational impact on the organisation.

11.1.10. Any major security failings will be reported to the Board of Directors immediately.

11.1.11. As a result of the analysis a corrective action, where appropriate, shall be implemented to eliminate/reduce the possibility of re-occurrence.

11.1.12. Logs will be reviewed periodically by the Security Management Team and any patterns or areas of concern will be highlighted to the board of directors with appropriate corrective action proposals for approval.