Information Technology Security Policy
2024

valwade
RECRUITMENT

Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

Information Security Policy

The Company handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

The Company commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process information so that we can meet these promises.

Employees handling Sensitive data should ensure:
Handle Company and Client information in a manner that fits with their sensitivity;

Limit personal use of the Company information and telecommunication systems and ensure it doesn't interfere with your job performance;

The Company reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;

Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;

Do not disclose personnel information unless authorised;
Protect sensitive customer information;
Keep passwords and accounts secure;
Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;

Always leave desks clear of sensitive data and lock computer screens when unattended;

Information security incidents must be reported, without delay, to the individual responsible for incident response locally –

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the Company's established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies

Employees should take all necessary steps to prevent unauthorised access to confidential data.

Employees should ensure that technologies should be used and setup in acceptable network locations.

Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts.

All PCs, laptops and workstations should be secured with a password protected screensaver with the automatic activation feature.

Because information contained on portable computers is especially vulnerable, special care should be exercised.

Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Company, unless posting is in the course of business duties.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

Protect Stored Data

All sensitive data stored and handled by the Company and its employees must be securely protected against unauthorised use at all times. Any sensitive data that is no longer required by the Company for business reasons must be discarded in a secure and irrecoverable manner.

Information Classification

Data and media containing data must always be labelled to indicate sensitivity level

Confidential data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to the Company if disclosed or modified.

Internal Use data might include information that the data owner feels should be protected to prevent unauthorised disclosure;

Public data is information that may be freely disseminated.

Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies

Employees should take all necessary steps to prevent unauthorised access to confidential data.

Employees should ensure that technologies should be used and setup in acceptable network locations

A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.

Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts.

Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.

Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.

Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.

Procedures must be in place to help all personnel easily distinguish between employees and visitors. “Employee” refers to full-time and part time employees, temporary employees and personnel, and consultants who are “resident” on the Company sites.
A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.

Network Jacks located in public and areas accessible to visitors must be Disabled and enabled when network access is explicitly authorised.

All PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered. Strict control is maintained over the external or internal distribution of any media data and has to be approved by management.Strict control is maintained over the storage and accessibility of media.

Protect Data in Transit

All sensitive data must be protected securely if it is to be transported physically or electronically.

If there is a business justification to send bank details data via email or via the internet or any other modes then it should be done after authorisation and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, GSM, GPRS, Wireless technologies etc.,).

The transportation of media containing sensitive data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

Disposal of Sensitive Data

All data must be securely disposed of when no longer required by the Company, regardless of the media or application type on which it is stored.

An automatic process must exist to permanently delete on-line data, when no longer required.

The Company will have procedures for the destruction of hardcopy (Paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.

The Company will have documented procedures for the destruction of electronic media. If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.

Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.

Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form.

Company security policies must be reviewed annually and updated as needed.

Network Security

Firewalls must be implemented at each internet connection and any demilitarised zone and the internal company network.

A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.

A firewall and router configuration document must be maintained which includes a documented list of services, protocols and ports including a business justification.

Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.

All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions have to be documented.

All outbound traffic has to be authorised by management (i.e. what are the whitelisted category of sites that can be visited by the employees) and the restrictions have to be documented

Disclosure of private IP addresses to external entities must be authorised.

A topology of the firewall environment has to be documented and has to be updated in accordance to the changes in the network.

The firewall rules will be reviewed on a six months basis to ensure validity and the firewall has to have clean up rule at the bottom of the rule base.

All traffic has to traverse through a firewall.

System and Password Policy

All users, including contractors and vendors with access to the Company systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

A system configuration standard must be developed along industry acceptable hardening standards (SANS, NIST, ISO)

System configurations should be updated as new issues are identified (as defined in PCI DSS requirement 6.1)

System configurations must include common security parameter settings

The systems configuration standard should be applied to any new systems configured.

All vendor default accounts and passwords for the systems have to be changed at the time of provisioning the system/device into the Company network and all unnecessary services and user/system accounts have to be disabled.

Security parameter settings must me set appropriately on System components

All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed.

All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system.

Any insecure protocols, daemons, services in use must be documented and justified.

All users with access to card holder data must have a unique ID.

All user must use a password to access the company network or any other electronic resources

All user ID's for terminated users must be deactivated or removed immediately.

The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account.

All system and user level passwords must be changed on at least a quarterly basis.

A minimum password history of four must be implemented.
A unique password must be setup for new users and the users prompted to change the password on first login.

Group, shared or generic user account or password or other authentication methods must not be used to administer any system components.

Where SNMP is used, the community strings must be defined as something other than the Standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.

All non-console administrative access will use appropriate technologies like ssh,vpn etc. or strong encryption is invoked before the administrator password is requested

System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands

Administrator access to web based management interfaces is encrypted using strong cryptography.

The responsibility of selecting a password that is hard to guess generally falls to users. A strong password must:

Be as long as possible (never shorter than 8 characters).
Include mixed-case letters, if possible.
Include digits and punctuation marks, if possible.
Not be based on any personal information.
Not be based on any dictionary word, in any language.

If an operating system without security features is used (such as DOS, Windows or MacOS), then an intruder only needs temporary physical access to the console to insert a keyboard monitor program. If the workstation is not physically secured, then an intruder can reboot even a secure operating system, restart the workstation from his own media, and insert the offending program.

To protect against network analysis attacks, both the workstation and server should be cryptographically secured. Examples of strong protocols are the encrypted Netware login and Kerberos.

Anti Virus Policy

All machines must be configured to run the latest anti-virus software as approved by the Company. The antivirus should have periodic scanning enabled for all the systems.

The antivirus software in use should be capable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits)

All removable media (for example floppy and others) should be scanned for viruses before being used.

All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS requirement 10.7 of 3 months online and 1 year offline.

Master Installations of the Antivirus software should be setup for automatic updates and periodic scans

End users must not be able to modify and any settings or alter the antivirus software

E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

Patch Management Policy

All Workstations, servers, software, system components etc. owned by the Company must have up-to-date system security patches installed to protect the asset from known vulnerabilities.

Where ever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors. Security patches have to be installed within one month of release from the respective vendor and have to follow the process in accordance with change control process.

Any exceptions to this process have to be documented.

Remote Access policy

It is the responsibility of the Company employees, contractors, vendors and agents with remote access privileges to the Company's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Company.

Secure remote access must be strictly controlled. Control will be enforced by two factor authentication via one-time password authentication or public/private keys with strong pass-phrases.

Vendor accounts with access to the company network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.

Remote access connection will be setup to be disconnected automatically after 30 minutes of inactivity

All hosts that are connected to the Company internal networks via remote access technologies will be monitored on a regular basis.

All remote access accounts used by vendors or 3rd parties will be reconciled at regular interviews and the accounts will be revoked if there is no further business justification.

Vendor accounts with access to the Company network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.

Vulnerability Management Policy

All the vulnerabilities would be assigned a risk ranking such as High, Medium and Low based on industry best practices such as CVSS base score.

As part of the PCI-DSS Compliance requirements, the Company will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

Quarterly internal vulnerability scans must be performed by the Company by internal staff or a 3rd party vendor and the scan process has to include that rescans will be done until passing results are obtained, or all High vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.

Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by the Company's internal staff. The scan process should include re-scans until passing results are obtained.

Configuration Standards:

Information systems that process transmit, or store sensitive data must be configured in accordance with the applicable standard for that class of system. Standards must be written and maintained by the team responsible for the management of the system.

All network device configurations must adhere to the Company required standards before being placed on the network as specified in the Company configuration guide. Using this guide, a boilerplate configuration has been created that will be applied to all network devices before being placed on the network.

Before being deployed into production, a system must be certified to meet the applicable configuration standard. Updates to network device operating system and/or configuration settings that fall under the Company standards are announced by the Management .
Updates must be applied within the timeframe identified by the Management .

Administrators of network devices that do not adhere to the Company standards (as identified via a previous exception) must document and follow a review process of announced vendor updates to operating system and/or configuration settings.

This process must include a review schedule, risk analysis method and update method.

All network device configurations must be checked annually against the configuration boilerplate to ensure the configuration continues to meet required standards.Where possible, network configuration management software will be used to automate the process of confirming adherence to the boilerplate configuration.

For other devices an audit will be performed quarterly to compare the boilerplate configuration to the configuration currently in place.

All discrepancies will be evaluated and remediated by Network Administration.

Change control Process

Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.

The change control process shall be formally defined and documented.

A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.

All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented.

A documented audit trail, maintained at a Business Unit Level, containing relevant information shall be maintained at all times. This should include change request documentation, change authorisation and the outcome of the change.

No single person should be able to effect changes to production information systems without the approval of other authorised personnel.

A risk assessment shall be performed for all changes and dependent on the outcome, an impact assessment should be performed.
The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.

All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.

All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.

Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project.

Major changes will be classified according to effort required to develop and implement said changes.

Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies. Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.

All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

Audit and Log review
This procedure covers all logs generated for systems within the cardholder data environment, based on the flow of cardholder data over the Company network, including the following components:

- Operating System Logs (Event Logs and su logs).
- Database Audit Logs.
- Firewalls & Network Switch Logs.
- IDS Logs.
- Antivirus Logs.
- Cctv Video recordings.
- File integrity monitoring system logs.

Audit Logs must be maintained for a minimum of 3 months online (available for immediate analysis) and 12 months offline.
Review of logs is to be carried out by means of the Company's network monitoring system (the Company to define hostname), which is controlled from the Company console (the Company to define hostname). The console is installed on the server (the Company to define hostname / IP address), located within the Company data centre environment.

The following personnel are the only people permitted to access log files (the Company to define which individuals have a job-related need to view audit trails and access log files).

The network monitoring system software (the Company to define) is configured to alert the Company to any conditions deemed to be potentially suspicious, for further investigation. Alerts are configured to: A dashboard browser-based interface, monitored by the Company.
Email / SMS alerts to the Company mailbox with a summary of the incident. The Company will also receive details of email alerts for informational purposes.

The following Operating System Events are configured for logging, and are monitored by the console the Company to define hostname:

Any additions, modifications or deletions of user accounts.
Any failed or unauthorised attempt at user logon.
Any modification to system files.
Any access to the server, or application running on the server, including files that hold cardholder data.
Actions taken by any individual with root or administrative privileges.
Any user access to audit trails.
Any creation / deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)

The following Database System Events are configured for logging, and are monitored by the network monitoring system (the Company\ CRM Adapt):

Any failed user access attempts to log in to the CRM's database.
Any login that has been added or removed as a database user to a database.
Any login that has been added or removed from a role.
Any database role that has been added or removed from a database.
Any password that has been changed for an application role.
Any database that has been created, altered, or dropped.
Any database object, such as a schema, that has been connected to.

Actions taken by any individual with DBA privileges.

The following Firewall Events are configured for logging, and are monitored by the network monitoring system (the Company to define software and hostname):
ACL violations.
Invalid user authentication attempts.
Logon and actions taken by any individual using privileged accounts.
Configuration changes made to the firewall (e.g. policies disabled, added, deleted, or modified).

The following Switch Events are to be configured for logging and monitored by the network monitoring system (the Company to define software and hostname):
Invalid user authentication attempts.
Logon and actions taken by any individual using privileged accounts.
Configuration changes made to the switch (e.g. configuration disabled, added, deleted, or modified).

The following Intrusion Detection Events are to be configured for logging, and are monitored by the network monitoring system (the Company to define software and hostname): Any vulnerability listed in the Common Vulnerability Entry (CVE) database.

Any generic attack(s) not listed in CVE.
Any known denial of service attack(s).
Any traffic patterns that indicated pre-attack reconnaissance occurred.
Any attempts to exploit security-related configuration errors.
Any authentication failure(s) that might indicate an attack.
Any traffic to or from a back-door program.
Any traffic typical of known stealth attacks.

The following File Integrity Events are to be configured for logging and monitored by (the Company to define software and hostname):
Any modification to system files.
Actions taken by any individual with Administrative privileges.
Any user access to audit trails.
Any Creation / Deletion of system-level objects installed by Windows.
(Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)

For any suspicious event confirmed, the following must be recorded on F17 - Log Review Form, and the Company management informed:
User Identification.
Event Type.
Date & Time.
Success or Failure indication.
Event Origination (e.g. IP address).
Reference to the data, system component or resource affected.

Incident Response Plan

'Security incident' means any incident (accidental, intentional or deliberate) relating to your communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage your company.

The Incident response plan has to be tested once annually. Copies of this incident response plan is to be made available to all relevant staff members, and take steps to ensure that they understand it and what is expected of them.

Employees of the company will be expected to report to management for any security related issues.

The Company PCI security incident response plan is as follows:

Each person must report an incident to Management (preferably) or to IT managed services (PCI response team)

That member of the team receiving the report will advise the PCI Response Team of the incident.

The PCI Response Team will investigate the incident

The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties as necessary.

The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.

If an unauthorised wireless access point or devices is identified or detected as part of the quarterly test this is should be immediately escalated to Management or someone with similar privileges who has the authority to stop, cease, shut down, and remove the offending device immediately.

A member of staff that reasonably believes it may have an account breach of systems related to the PCI environment in general, must inform the Company PCI Incident Response Team.
After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment departments' response plans.

The Company PCI Security Incident Response Team:

Managing Director
Operations Director

Incident Response Notification

Escalation – First Level
Director of the company

Escalation – Second Level
Managing Director

External Contacts
Internet Service Provider
External Response Team as applicable (CERT Coordination Centre 1,etc.) Law Enforcement Agencies as applicable in local jurisdiction

In response to a systems compromise, the PCI Response Team and designees will:
Ensure compromised system/s is isolated on/from the network.
Gather, review and analyse the logs and related information from various central and local safeguards and security controls
Conduct appropriate forensic analysis of compromised system.
Contact internal and external departments and entities as appropriate.

Roles and Responsibilities

The directors are responsible for overseeing all aspects of information security, including but not limited to:
Creating and distributing security policies and procedures.
Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel. creating and distributing security incident response and escalation procedures that include:

Maintaining a formal security awareness program for all employees that provide multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings).
The Information Technology Office (or equivalent) shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).
System and Application Administrators shall: monitor and analyse security alerts and information and distribute to appropriate personnel administer user accounts and manage authentication
Monitor and control all access to data.
Maintain a list of service providers.
Ensure there is a process for engaging service providers including proper due diligence prior to engagement.
Maintain a program to verify service providers' PCI-DSS compliant status, with supporting documentation.
The Human Resources Office (or equivalent) is responsible for tracking employee participation in the security awareness program, including: Facilitating participation upon hire and at least annually.
Ensuring that employees acknowledge in writing at least annually that they have read and understand the Company's information security policy.
Written contracts require adherence to PCI-DSS by the service provider.
Written contracts include acknowledgement or responsibility for the security of customer data by the service provider.

Third party access to data

All third-party companies providing critical services to the Company must provide an agreed Service Level Agreement.
All third-party companies providing hosting facilities must comply with the Company's Physical Security and Access Control Policy.
Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.

User Access Management
Access to company is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.

Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out. There is a standard level of access; other services can be accessed when specifically authorised by HR/line management.
A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

Name of person making request:
Job title of the newcomers and workgroup:
Start date:
Services required (default services are: MS Outlook, MS Office and Internet access):

Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
Access to all company systems is provided by IT and can only be started after proper procedures are completed.
As soon as an individual leaves the Company employment, all his her system logons must be immediately revoked.
As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

Access Control Policy

Access Control systems are in place to protect the interests of all users of The Company computer systems by providing a safe, secure and readily accessible environment in which to work.
The Company will provide all employees and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.
The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorisation provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
Access rights will be accorded following the principles of least privilege and need to know.
Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent. Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification
Users are obligated to report instances of non-compliance to the Company CISO.
Access to The Company IT resources and services will be given through the provision of a unique Active Directory account and complex password.
No access to any of The Company IT resources and services will be provided without prior authentication and authorisation of a users Windows Active Directory account.
Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory, Group Policy Objects.
Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative.
Requests for access permission to be granted, changed or revoked must be made in writing.
Users are expected to become familiar with and abide by The Company policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
Access for remote users shall be subject to authorisation by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy.
No uncontrolled external access shall be permitted to any network device or networked
system.

Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.
Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.

A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights

Wireless Policy

Installation or use of any wireless device or wireless network intended to be used to connect to any of the company networks or environments is prohibited.

A quarterly test should be run to discover any wireless access points connected to the company network
Usage of appropriate testing using tools like net stumbler, kismet etc. must be performed on a quarterly basis to ensure that:
Any devices which support wireless communication remain disabled or decommissioned. If any violation of the Wireless Policy is discovered as a result of the normal audit processes, the security officer or any one with similar job description has the authorisation to stop, cease, shut down, and remove the offending device immediately.

If the need arises to use wireless technology it should be approved by the company and the following wireless standards have to be adhered to:

Default SNMP community strings and passwords, pass-phrases, Encryption keys/security related vendor defaults (if applicable) should be changed immediately after the installation of the device and if anyone with knowledge of these leaves the company.

The firmware on the wireless devices has to be updated accordingly as per vendors release schedule the firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.

Any other security related wireless vendor defaults should be changed if applicable.
Wireless networks must implement industry best practices (IEEE 802.11i)
An Inventory of authorised access points along with a business justification must be maintained. (Update Appendix B)

Appendix A – Agreement to Comply Form – Agreement to Comply With Information Security Policies

____
Employee Name (printed)

____

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to the Company by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the Company, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.

I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the Company security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.
I also agree to promptly report all violations or suspected violations of information security policies to the designated member of the team.

____
Employee Signature

Appendix B

List of Service Providers

Name of Service Provider
Contact Details
Services Provided
PCI DSS Compliant
PCI DSS Validation Date

Definitions
Use of the Facilities
Work use of the Facilities
Personal use of the Facilities
Prohibited use of the Facilities

Use of Networking Sites

Professional Networking SitesRules for using Professional Networking SitesContacts made via Professional Networking SitesMaintenance of the Company profile on Professional Networking Sites Social Networking Sites
Post termination of employment or engagement restrictions

How to use the Facilities, and Networking Sites

Information recipients
Content and tone of communications
Out of Office messages
Deleting or archiving material
Suspect material, documents or viruses
Passwords

Monitoring use of the Facilities and Networking Sites
Unsolicited communications
Termination of employment with the Company
Status of this policy
Acknowledgement of receipt of this policy

Definitions

“Confidential Information” means: information relating to the Company’s business plans, finances, new or maturing business opportunities, and research and development projects; marketing information relating to the Company’s marketing or sales of any past, present or future service including without limitation sales targets and statistics, market share and pricing statistics, marketing surveys and plans, market research reports, sales techniques and price lists; details of Professional Contacts including names, addresses, contact details, terms of business or proposed terms of business with them, their business requirements, pricing structures, lists of employees and their terms of employment; and any other information of a confidential nature belonging to employees, candidates, clients, and employees of clients of the Company or in respect of which the Company owes any other obligation of confidence.”

“Facilities” means telephone and computer facilities, including email and the internet, and hardware including mobile media such as laptops, mobile phones, BlackBerries™, smartphones, personal digital assistants, iPads™, tablets or notebooks, or similar equipment.

“Networking Sites” includes (but is not limited to) professional networking sites such as LinkedIn, Xing, Viadeo ((Professional Networking Sites) and social networking sites such as Facebook, Twitter, SecondLife, Google+, Wikipedia, (Social Networking Sites). Your access to and use of Networking Sites, whilst employed by the Company is set out in this policy. [see Note 2]

"Personal Contacts" means any of Your friends (not including Professional Contacts).[see Note 3]

"Professional Contacts" means any Candidate, Client, Introducer, Key Employee, Prospective Candidate or Prospective Client (all as defined in Annex 1), together with any contacts made through a professional body trade or association of which You or the Company is a member. [see Note 3]

Use of the Facilities:

Work use of the Facilities

The Facilities are made available to You during the course of your employment with the Company to assist You in carrying out and promoting the Company's business and interests.

Personal use of the Facilities

The Facilities [may OR may not] be used[, within reason,] for personal communications or to send and retrieve personal messages and to browse external web-sites for personal use [although this should be done outside office hours and be kept to a reasonable limit. It must not interfere with business commitments. If there is any evidence that this privilege is being abused then the privilege [may/ will] be withdrawn]. The content of personal e-mails must also comply with the restrictions set out in section 3.3 of this policy. If using the Facilities for personal communications You should be aware that the Company may monitor your use of the Facilities in accordance with section 6 of this policy and any breaches of this policy may result in disciplinary action up to and including dismissal. [see Notes 4 and 12]

Prohibited use of the Facilities

The following uses of the Facilities are expressly prohibited:

Viewing internet sites which contain pornographic, obscene, abusive, slanderous or otherwise offensive material or downloading or forwarding such material within or outside the Company;

Sending, receiving or forwarding communications that are in violation of company policy including, but not limited to, the transmission of obscene, offensive or harassing messages;

Sending receiving or forwarding communications which make unsubstantiated and potentially defamatory comments about colleagues, clients, candidates or any other person via the Facilities or any Networking Site. You are reminded that communications via social media constitutes publication just as printing in hard copy or via email is publication. You personally, and/ or the Company could face a defamation action should you publish unsubstantiated and potentially defamatory material;

Sending, receiving or forwarding communications that disclose Confidential Information without the prior authorisation of [the Company's IT Manager/ your line manager/ or other];

Bullying or harassing colleagues, clients, candidates or any other person via the Facilities or any Networking Sites

Discriminating or making offensive or derogatory comments about any colleagues, clients, candidates or any other person via the Facilities or any Networking Site;

Breaching any other Company's policies including in particular, but not limited to, the Information Security and Data Protection Policy, the Equal Opportunities and Diversity Policy and [any other];

Engaging in any behaviour which might cause either the Company to be in breach of the REC Code of Professional Conduct or You to be in breach of the Institute of Recruitment Professionals' Code of Ethics (if You are a member of that Institute);

Duplicating copyrighted or licensed software or other information without the appropriate authorisation;

Installing or downloading any software or hardware without the specific approval of the [Company's IT Manager/ Managing Director/ other] or other person delegated by him/ her to give such approval;

Forwarding or otherwise perpetuating junk mail or "chain-letter " type e-mail within or outside the Company;

Removing any hardware or software from the Facilities or the Company's premises without prior approval of the [Company's IT Manager/ Managing Director/ other]; and

Selling or advertising anything via the Facilities or broadcast messages about lost property, sponsorship or charity appeals, without the written agreement of your line manager.

If you engage in any prohibited activities this may result in the Company taking action against You under the Company's Disciplinary, Dismissal and Grievance Procedures and which ultimately could lead to the termination of Your employment.

Use of Networking Sites:

Networking Sites are a valuable business tool which the Company wishes to use to build its brand, reputation and business [see Note 5], and which it recognises You may wish to use to build Your own professional reputation. However, in addition to the benefits there are also certain risks attached to using Networking Sites including but not limited to the Company's Confidential Information, reputation and compliance with their legal obligations. In order to reduce those risks, for both Yourself and the Company, where and when You are representing the Company You must comply with conditions set out in this policy. Failure to comply with this policy may result in the Company taking action against you under the Company's Disciplinary and Grievance Procedure.

Professional Networking Sites

The Company may provide You with access to Professional Networking Sites. Such access is granted for work-related purposes only and should be done for the benefit of the Company alone, though professional networking activity may be done inside or outside of working hours.

Rules for using Professional Networking Sites

The following rules apply when You access or use a Professional Networking Site: [set out here how your organisation authorises account opening e.g.]

You must have written permission from [the Company's IT Manager/ Your line manager/ or other] before setting up an account for any Professional Networking Site.

You should create the account on the Professional Networking Site using your work email address only.

You must notify [the Company's IT Manager/ Your line manager/ or other] of the details of your account including the password.

Your password is confidential and should not be disclosed to any unauthorised person.

You should only use the account for the purpose for which it was authorised. If you are commenting on a Professional Networking Site on behalf of the Company you must seek approval from your line manager before submitting that comment.

You shall inform the Company of activities that you carry out in relation to Professional Networking Sites including details of your membership of sites that you have set up and new contacts that you have made during the course of your employment.

You must regularly backup your Professional Contacts.

You must regularly upload Professional Contacts to the Company's database(s).

You should not disclose Confidential Information unless You have been authorised to disclose by [Your line manager/ the Managing Director/ the Finance Director/ other].

You must comply with the terms and conditions of use of all Networking Sites that You use. You should pay particular attention to any codes of behaviour or professional conduct contained within those terms and conditions. [see Note 6]

REC Corporate members are also required to comply with the Code of Professional Practice and individual recruiters with the Code of Ethics of the Institute of Professional Recruiters. [see Note 7]

You must advise the Company if you become aware of any breach of this policy by a colleague. Failure to do so may be a disciplinary offence. [see Note 8]

The Company reserves the right to restrict your access to Professional Networking Sites and accounts that the Company has created for you.

Contacts made via Professional Networking Sites

If You already have an account with any Professional Networking Site which contains Confidential Information belonging to the Company You must transfer that Confidential Information to a new account set up in accordance with section 4.1.1 of this policy. [see Note 9] Such account shall be subject to the rules set out in section 4.1.1 of this policy and the following additional rules:

You must keep Personal Contacts separate from Professional Contacts.

The Company reserves the right to require You to provide evidence and details as to when You made your contacts and in which capacity they were made. You will be required to give access to your account(s) to [the Company's IT Manager/ Your line manager/ or other] for this purpose. The Company's decision on whether a contact constitutes a Personal or Professional Contact shall be final.

Maintenance of company profile on Professional Networking Sites

Certain Professional Networking Sites contain company profile pages relating to the Company. For the avoidance of doubt, these profile pages may only be edited by authorised users. Amendment of the Company's profile pages by unauthorised users shall be a disciplinary offence (and for this purpose You are referred to the Company's Disciplinary, Dismissal and Grievance Procedures).

If you are authorised to make a comment on a Professional Networking Site you must state clearly that these are personal views and not the views of the Company. [see Note 10]

Use of Social Networking Sites

The Company respects Your right to a private life [A: and therefore You may access social networking sites using the Facilities. However this should be done outside office hours and be kept to a reasonable limit.

If there is any evidence that this privilege is being abused then the privilege may be withdrawn OR B: but access to social networking websites via the Facilities and during working hours is strictly forbidden [unless prior authorisation is obtained from [the Company's IT Manager/ Your line manager/ or other].

Your use of Social Networking Sites may impact on the Company and its business. Such impact includes potentially causing damage to its reputation, loss of Confidential Information, or exposure to other liabilities such as claims of discrimination, harassment or workplace bullying. The content of any communications or comments posted on a Social Networking Site must not damage or bring into disrepute the Company, its staff, clients or candidates. Therefore if You use Social Networking Sites, even where this is not via the Facilities or is outside of working hours You are prohibited from:

[identifying Yourself as working for the Company;] [see Notes 11 and 12]

Engaging in any conduct or posting any comments which are detrimental to the Company;

Engaging in any conduct or posting any comments which could damage working relationships between members of staff, Introducers, suppliers, affiliates, Clients and Candidates of the Company. Where you express personal views You must state that these are personal views and do not represent the views of the Company;

Engaging in any conduct or posting any comments which could be derogatory to another person or third party or which could constitute unlawful discrimination or harassment;

Recording any Confidential Information regarding the Company on any social networking site or posting comments about any Company related topics such as the Company's performance; and/ or

Making information available which could provide any person with unauthorised access to the Company, the Facilities and or any Confidential Information.

You may be required to remove postings deemed to constitute a breach of this policy. This may include any 'likes' or 'dislikes' of other people's posts or the re-posting/tweeting of other people's comments (or links thereto) which of themselves may constitute a breach of this policy.

Post termination of employment or engagement restrictions

For the avoidance of doubt, the restrictions on the use of Networking Sites continue to apply throughout Your employment with the Company including any period of garden leave you may serve.

How to use the Facilities and Networking Sites

Information recipients

You must exercise caution when using the Facilities and any Networking Sites. In addition to the restrictions set out in sections 3 and 4 of this policy, care must be used in addressing emails, postings on Networking Sites or other electronic communications to make sure that they are not sent to the wrong individual or company. In particular, exercise care in using e-mail distribution lists or Networking Sites to make sure that all addressees or site group members are appropriate recipients of the information sent or posted.

Content and tone of communications

All e-mails, postings on Networking Sites and electronic communications should be courteous, professional and business-like and, as set out in sections 2 and 3, should not contain any material, which would reflect badly on the Company's reputation. If You receive an e-mail, posting or other communication containing material that is offensive or inappropriate to the office environment then You must inform [the Company's IT Manager/ your line manager/ or other] and delete on their instruction. Under no circumstances should such e-mails, postings or communications be forwarded internally or externally. [see Note 12]

Out of Office messages

If You are out of the office [for more than8 hours] you should put an "Out of Office" message on your emails and on your voicemail(s). This message should indicate when you will be back in the office and should identify another person whom the sender or caller can contact in your absence should they need to.

[Your emails and phone calls [may/ will] be monitored in your absence.] [see Note 13]

Deleting or archiving material

You should not store large quantities of e-mail or downloaded files or attachments. The retention of data utilises large amounts of storage space on network servers, PCs and mobile media, and can adversely affect system performance.

You should delete any e-mails or other communications sent or received that no longer require action or are no longer relevant to Your work or to the Company.

You should retain any information that you need for record-keeping purposes in line with the Company's Information Security and Data Protection policy.

Suspect documents, messages or viruses

Any files or software downloaded from the Internet, personal mobile media or other software or hardware brought from home (and for which you have previously obtained authorisation to download as per section 2 of this policy) must be virus-checked before installation on the Facilities and use.

If you receive any suspect e-mails, communications, documents or computer virus alerts you should:

Contact [the Company's IT manager/ your line manager/ or other] immediately;
Not open attachments to any email message whose address You do not recognise; and
Not forward them to any other internal or external user without the approval of [the Company's IT Manager/ your line manager/ or other].

Passwords

Your password(s) is/ are confidential and should not be disclosed to any unauthorised person.

The Company reserves the right to access any accounts (whether email or networking sites) in which case You will be required to give Your password to [the Company's IT Manager/ your line manager/ or other].

Passwords should be changed regularly. To protect passwords, You should not access the Facilities in the presence of others and Confidential Information should never be left open on the screen when equipment is unattended.

Monitoring use of the Facilities, Professional and Social Networking Sites: [see Note 13]

The Company has the right to monitor any and all aspects of the use of the Facilities and any Networking Sites and to monitor, intercept and/or record any communications made by using the Facilities and any Networking Sites. This is to ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

By using the Facilities and any Networking Sites You consent voluntarily and knowingly to Your use being monitored. You also acknowledge the right of the Company to conduct such monitoring.

Unsolicited Communications

It is unlawful to send unsolicited emails or mobile telephone text messages to individuals with whom there is no existing customer relationship unless those individuals have given their consent.

Before any direct marketing approach is used to contact individuals by means of email or mobile telephone text message You must first obtain the authorisation of [the Company's IT Manager/ your line manager/ or other]. In any event any unsolicited communications sent in this way must include wording in the title or in the text enabling the receiver to opt-out of further contact in the future [see Note 14].

If you are using telephone or fax to contact companies and individuals with unsolicited direct marketing you must first check whether such companies or individuals are registered with the Telephone Preference Service (TPS) or Fax Preference Service (FPS) operated by the Direct Marketing Association. You may not send unsolicited direct marketing to a company that is registered with the TPS or FPS, unless you have their consent to do so.

If you are informed that an individual with whom the Company has an existing customer relationship or who has previously consented to receiving information wishes to opt-out of receiving such communications in the future you must [update the data relating to that individual immediately OR inform [Insert name of person to contact] immediately] and on no account must you continue to communicate with that individual by such means

Termination of employment or engagement with the Company

All email address lists or other contact information stored on the Facilities are Confidential Information and remain the property of the Company even after the termination of Your employment or engagement with the Company.

You may not copy or remove any email address lists or other contact information stored on the Facilities without prior written permission from the Company.

You should ensure that any genuinely Personal Contacts are, where possible, stored separately from any Professional Contacts. Upon termination of Your employment or engagement for whatever reason you may seek the Company's permission to remove or copy Your Personal Contacts from the Facilities.

On or prior to the termination of your employment or engagement with the Company for whatever reason you must speak to Your line manager to determine what steps to take in relation to any Professional Networking Sites you use.

The Company reserves the right to require you to:

> Advise your Professional Contacts on any Professional Networking Site of the date on which you will be leaving the Company and who Your Professional Contacts can contact at the Company when You leave the Company;
>
> Delete Your account on any Professional Networking Site;
>
> Delete all of Your Professional Contacts and not retain a copy of Your Professional Contacts' details without prior written permission from the Company;
>
> Hand over control of your account on all or any Professional Networking Site(s) to [the Company's IT Manager/ Your line manager/ or other] together with all passwords. [The Company's IT Manager/ Your line manager/ or other] will be entitled to notify your contacts on all or any Professional Networking Site(s) of the fact that he/she has taken over your account.
>
> Employees must be aware that failure to comply with the above rules regarding Networking Sites could result in disciplinary action or dismissal even if the failure to comply occurs outside the workplace. [see Notes 8 and 11]

Status of this policy

This policy does not constitute a contract and the Company reserves the right to change its terms at any time. Failure to comply with this policy may lead to disciplinary action up to and including termination of Your employment or engagement with the Company.

Acknowledgement of receipt of policy

You are required to read a copy of this policy and return it, signed, to [your line manager/Human Resources/other] to acknowledge that you have read and understood its terms [see Note 15].

……………………………………………….
Employee signature

Employee name in block capitals: