Management System Manual

Table of Contents

1 Introduction

CentralNic Ltd was established in 1995 as an independent global domain name registry committed to making it easier for Internet users to establish new and distinctive domain names with regional and country-specific identities.

Headquartered in London, CentralNic currently has a portfolio of 27 domain extensions available for registration worldwide. Top Level Domain names such as .COM, .NET, and .ORG are used by companies and non-profit organizations to identify themselves on the Internet, and each country in the world has its own Country Code TLD, such as .UK for the United Kingdom and .DE for Germany.

CentralNic uses the .COM, .NET and .ORG standard domain name structure to offer additional regional and country-specific domain names, ensuring a secure, inexpensive solution for creating easily identifiable Internet addresses worldwide. CentralNic's registry service is particularly useful for Internet users in countries where domain names are difficult to obtain due to restrictive domain regulations.

The CentralNic portfolio also has wide appeal to individuals and companies seeking to define an Internet identity in a region or country where they intend to establish or expand their business or for any other reason establish a geographically distinct identity. Users often turn to CentralNic when a conventional Top Level Domain (TLD) such as .COM, or a country TLD such as .UK address has already been claimed by another party.

CentralNic has a worldwide network of **more than 1,500 registrars** that provides customers with efficient local access for registration. The company also provides extensive customer support, including legal expertise on such issues such as country specific regulations and individual vs. corporate ownership of domain names.

CentralNic is a profitable organization that has experienced rapid growth, fuelled by the growing use of the Internet for commercial purposes, and the scarcity of suitable domain names.

To serve its customers without interruption, CentralNic operates a network of domain name servers to ensure maximum reliability and performance. We operate DNS servers on over a dozen locations, and new nodes are installed regularly.

1.1 Introduction to Quality and Information Security Information Security Management

To demonstrate commitment to Quality and Information Security, CentralNic has created a Management System compliant with the international standards ISO 9001 (Quality) and ISO 27001 (Information Security).

To serve its customers without interruption, CentralNic operates a network of domain name servers to ensure maximum quality, reliability, security and performance. The quality of CentralNic's services is of paramount importance. CentralNic is committed to continually improve quality through driving innovation, and is involved in the introduction and development of new technologies, including EPP and IRIS.

Due to the nature of the environment that CentralNic operates in, Information Security is critical to the success and reputation of the CentralNic brand and services it offers. Information Security is described within the organisation as the preservation of confidentiality, integrity and availability of information.

- **Confidentiality**

  Ensuring that information is accessible only to those authorised to have access.

- **Integrity**

  Safeguarding the accuracy and completeness of information and processing methods.

- **Availability**

  Ensuring that authorised users have access to information and associated assets when required.

The Board of CentralNic has created Quality and Information Security Policies to set a clear direction for Quality and information security to demonstrate support for, and commitment to, quality and information security throughout the company.

The Policies will be reviewed annually to assess the policy's effectiveness, demonstrated by the number and impact of recorded security incidents, and the impacts on business efficiency and technology, combined with the response to any significant changes affecting the company.

2 Scope

The scope of the CentralNic Management System compliant to ISO 9001 and ISO 27001, as described in this manual, encompasses all business activities: ***The provision of innovative, reliable and flexible registry services for ccTLD, gTLD and private domain name registries.***

The scope of the management system will cover the CentralNic offices located at:-

CentralNic Ltd, 35-39 Moorgate, London, EC2R 6AR.

The domain name registry system currently hosted at:

Qube Managed Services Ltd, 260-266 Goswell Road, London EC1V 7EB

The Disaster Recovery Site currently hosted at:

Domicilium (IOM) Ltd, The Isle of Man Datacentre, Ronaldsway Industrial Estate, Ballasalla, Isle of Man IM9 2RS

CentralNic's satellite offices and external stakeholders' premises are out of scope of this management system.

The information assets should be shareable (available for use) within the CentralNic premises. Outside of the CentralNic premises the information assets must not be available for use (i.e. scarce) and therefore not shareable.

2.1 Network Boundary

The network boundary is the section of the network which is physically in the Moorgate office, and which is hosted in our dedicated racks in Qube's data centre. This corresponds to the elements below the two red firewalls as illustrated in the Network diagram in Section 5.5.1.

3 Exclusions, References and Definitions

3.1 Exclusions

The exclusions from ISO27001 are referenced in the Statement of Applicability.

The following clauses are excluded from the scope of ISO90001:

7.5.2 Validation of processes for production and service provision **-** There are no instances where validation of product cannot be carried out after the product has been delivered to the client, therefore this clause has been excluded from scope.

7.6 Calibration of equipment – the company uses no equipment that requires calibration; therefore this clause has been excluded from the scope of certification.

3.2 References & Definitions

All references in this management system are taken from ISO900, ISO27001 and ISO27002.

4 Management System Policies

CentralNic employees and management are committed to assuring that company policies are implemented, understood, maintained at all levels of the organization and are available to the public on request.

CentralNic policies have been established by the Chief Executive Officer to provide clear direction, support and commitment to employees.

The policies are supported by procedures and objectives for each function and personnel role included within the organisation. This together with our core values will enable us to exceed our clients' expectations.

The policies may also be made available to clients and other interested parties where necessary.

The policies included within the Management System are:

- Quality Policy
- Information Security

Other CentralNic policies are located on the Wiki under 'Policies'.

4.1 Quality Policy

It is the policy of the CentralNic to provide domain name services, which meet the requirements of its clients and quality criteria accordance with the highest professional standards aiming for continual improvement and customer satisfaction through the involvement and participation of all levels of management, staff and other interested parties.

This policy for quality has been established to ensure that it:-

- is appropriate to the purpose of the organisation, the expected level of client satisfaction and the needs of other interested parties
- commits to meeting requirements and to continual improvement
- ensures that the resource requirements are established and available
- provides a framework for establishing and reviewing quality objectives
- demonstrates top management commitment and ensures the quality objectives are communicated, understood and implemented at appropriate levels of the organisation
- is regularly reviewed at the management review meeting for suitability and effectiveness addressing continual improvement and client satisfaction.

Management is ultimately responsible for making balanced judgements, assessing the significance of variations and taking decisions. In arriving at such decisions, the quality and personal integrity of staff are of fundamental importance. In this context, all effort is made to ensure that each person in the organisation understands that quality assurance is important to their future, know how they can assist in the achievement of adequate quality and are stimulated and encouraged to do so.

This policy is approved and endorsed by the Board of Directors and is supported by all levels of Management within the organisation. All personnel shall be guided by the contents of the quality management system and no deviation from the methods and procedures set down shall be permitted.

Our Objective is to continue to promote our inter-disciplinary culture to ensure that clients receive a depth and breadth of service unrivalled within our sector.

4.2 Information Security Management Policy

The Board of CentralNic recognises the significance of integrity and security of information. CentralNic's Information Security Management (ISM) policy is to maintain the highest standard of confidentiality, integrity and availability of data and information that is collected (customer, supplier) or generated (internally) by the organization, that it stays safe and does not conflict with relevant legislation.

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

Corporate information is a critical business asset. The success of CentralNic's business is dependent upon the company's ability to store information securely, and retrieve and process it as and when required. Such information and the way it may be processed is subject to UK legislation.

Our Information Security Policy is achieved by a stringent set of controls, including policies, processes, procedures, software and hardware functions. These controls are continuously monitored, reviewed and improved, where necessary, to ensure that specific security and business objectives are met. This is operated in conjunction with other business management processes, and incorporates the applicable statutory, regulatory and contractual requirements.

Our ISM Policy Awareness Program is incorporated in our induction process, training and Quality Management System. The ISM policy is readily accessible internally and presented to existing and prospective clients.

In addition to employees; suppliers, contractors and sub-contractors of CentralNic are expected to adhere to our ISM policy.

All employees are empowered to take responsibility for Information Security and a robust process for identifying and reporting security risks and incidents is in place and is regularly reviewed.

Through compliance to applicable statutory, regulatory and contractual requirements, and the standard for Information Security Management ISO/ IEC 27001:2005, CentralNic will demonstrate confidence, integrity and credibility both internally and externally.

5 Planning

5.1 Identification and Evaluation of Risks

To identify CentralNic's management system requirements, three main factors have been considered.

Assessing risks to the organisation.

A risk assessment has been carried out by the CentralNic Information Security Team (IST) to identify threats, vulnerability and the likelihood of a security occurrence. The potential impact has also been estimated.

The legal, statutory and contractual requirements that CentralNic has to adhere to.

The Risk Assessment considers:-

- The identification of assets and their value, together with a list of the type of threats that could affect these assets.
- The harm to CentralNic, its customers, and users of its service likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of information and other assets.
- The realistic likelihood of such failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented within the business.
- The ownership of assets.

The identification and assessment of security requirements is carried out periodically to:

- Consider new threats and vulnerabilities
- Take account of changes to business requirements and priorities
- Confirm that controls remain effective

The assets and risk assessment is reviled annually and updated accordingly.

5.2 Identification of Legal and Other requirements

The IST is responsible for identifying relevant statutory, regulatory and contractual requirements that the company has to adhere to.

CentralNic is obliged to abide by all relevant UK legislation. The requirement to comply with this legislation shall be devolved to employees and agents of CentralNic who may be held personally accountable for any breaches of information security for which they may be held responsible. CentralNic shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Copyright, Designs and Patents Act (1988)
- The Trade Marks Act (1994)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)

- Regulation of investigatory Powers Act (2000)
- Digital Economy Act (2010)

CentralNic is compliant to the contractual requirements concerning the use of material in respect of which there maybe intellectual property rights and on the use of propriety software products.

The Company shall ensure all information products are properly licensed and approved by the CTO. Users shall not install software on the Company's property without permission from the CTO. Users breaching this requirement may be subject to disciplinary action.

Data protection and privacy is ensured as required in relevant legislation, regulations and if applicable, contractual clauses.

5.3 Contingency Planning

5.3.1 Disaster Recovery

CentralNic has a Business Continuity Plan in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Assessments of risks to the business have been addressed by the IST to ensure the Business Continuity Plan has appropriate controls in place. The plan includes actions to address all critical information, applications, systems and networks and to maintain or restore operations, thus ensuring availability of information at the required level, within the required timescales.

The Disaster Recovery Committee (DRC) members include:-

- CEO
- CTO
- Senior Operations Engineer(s)
- Operations Manager
- Finance Director
- Marketing Director

The DRC will be supported by any other employee as directed by the committee. The CTO is responsible for ensuring that all relevant staff are notified and given proper instructions.

These plans are stored in the company's shared DropBox folder, so that they are accessible if an incident renders the company wiki unavailable. Key employees also keep a copy at their homes.

The Business Continuity Plan is reviewed annually to ensure that is up to date and effective.

5.3.2 Protection from malicious software

The Company shall use software countermeasures and management procedures to protect against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on

the Company's property, without the express permission of the CTO or other senior member of the IT team. Users breaching this requirement may be subject to our disciplinary procedure.

All systems will be protected by a multi-level approach involving firewall, router configuration, e-mail scanning, virus and spy/malware protection on all workstations, and on those servers that are vulnerable to malicious software. Networks will be monitored for suspicious activity.

5.4 Objectives

Objectives are established at relevant functions and levels within the company to continually improve the effectiveness of the Management System.

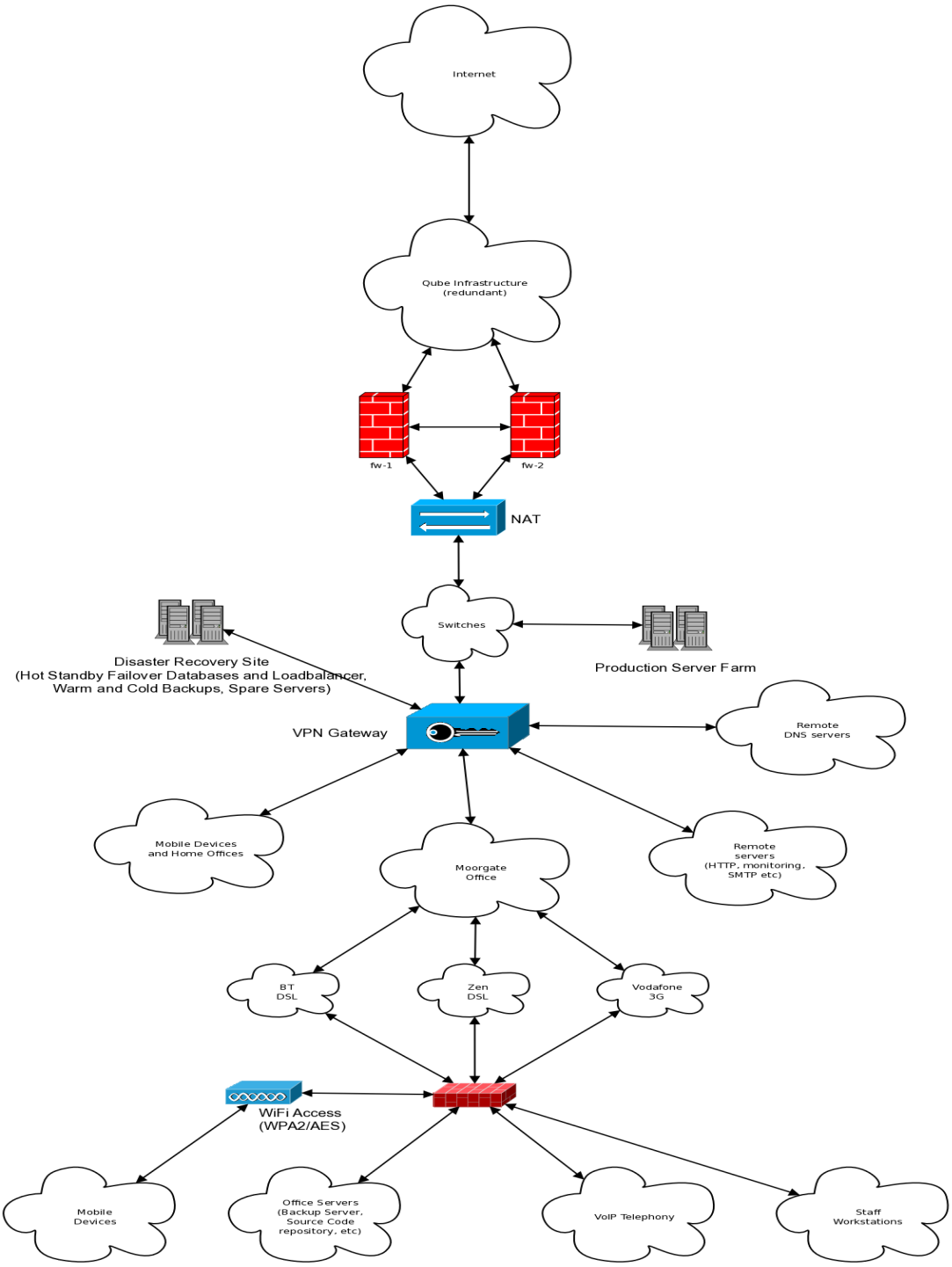
The company objectives are consistent with the company policies and the commitment to continual improvement.

The Quality and Information Security objectives are set by the CEO and the Information Security Team (IST) and are cascaded throughout the organisation. The objectives include a detailed objectives plan, available on the Wiki.

- To successfully achieve ISO 9001 and 27001 certification by Q4 of 2012.
- To achieve a fully integrated management system, combining Quality and Information Security requirements by the Q3 of 2012.
- To raise awareness of quality and security issues company-wide through proactively communicating the Information Security Policy, Information Security Manual and supporting procedures.
- To meet the security requirements for new generic top level domains as specified by ICANN.
- To ensure that personal information about domain name registrants is protected, in according with data protection principles and legislation.
- To ensure that CentralNic's business activities contribute positively to the stability and security of the Internet's Domain Name System.
- To raise awareness of the benefits of CentralNic being ISO 27001 certified to enhance customer loyalty, reputation and strengthen the CentralNic Brand.
- To establish and monitor an effective Information Security Management System to reduce risk to CentralNic, its clients, and users of its services.

5.5 Organization Structure, roles, responsibilities and authorities

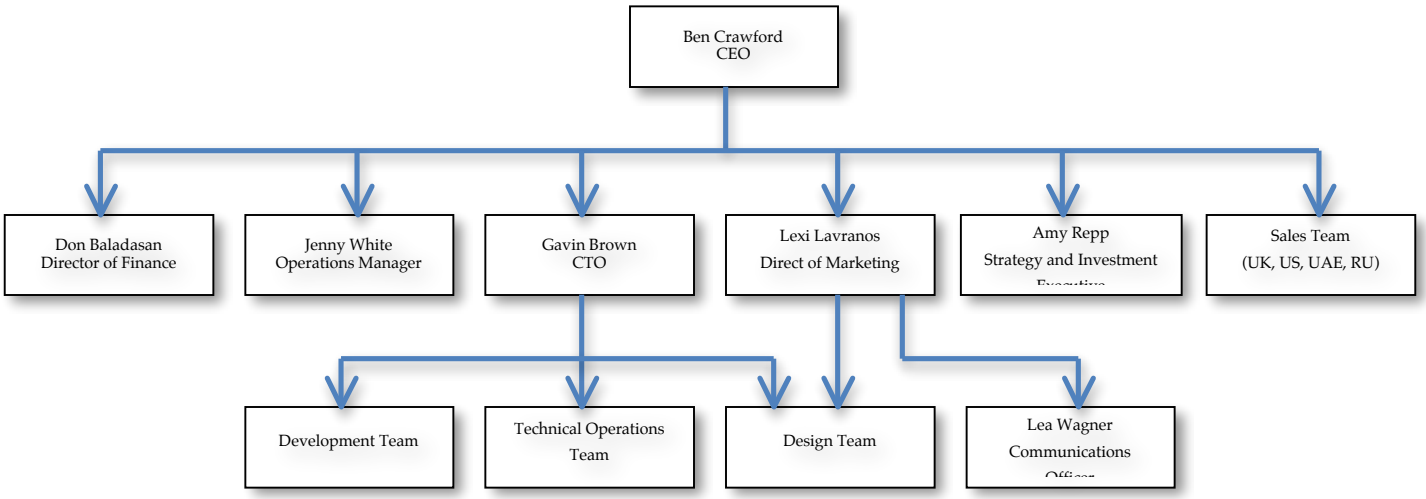
5.5.1 Network Diagram



5.5.2 Company Process Chart

The company process chart is described on the company wiki, links to key system documentation are available from this diagram.

5.5.3 Company Structure



5.5.4 Responsibility and Authority

All employees are empowered to take responsibility for information security and to be vigilant of any potential security threat.

Ultimate responsibility for information security rests with our Chief Executive Officer (CEO).

The CTO is responsible for managing the implementing, monitoring, documenting and communicating of all security information policies, regulated standards, guidelines and practices on a day-to-day basis. The CTO shall keep the CentralNic Board of Directors informed of the information security status of the organisation by means of regular reports and presentations.

Responsibility for the annual review of this policy lies with the CTO for approval by the Chief Executive Officer.

The Line Managers are responsible for the security of their physical environments where information is processed or stored. They are responsible for ensuring that permanent and temporary staff and contractors are aware of:

- The information security policies applicable to their work areas
- Their personal responsibilities for information security
- How to seek advice on information security matters
- Staff – each member of staff is responsible for the operational security of the information systems they use. They shall comply with all information security procedures including the maintenance of data, confidentiality and data integrity. Failure to do so may result in disciplinary action
- Internal/External System User – each individual shall comply with the security requirements that are currently in force and shall also ensure confidentiality, integrity and availability of information they use is maintained to the highest standards

- Contracts with External Contractors – where access is required to the organisations information systems, restricted authorisation is granted before access is permitted
- Visitors to CentralNic's office in Moorgate must be signed in upon arrival. Responsibility for compliance with this policy lies with the person the visitors have come to see, or with the Operations Manager

5.6 Management Commitment

A management framework has been established to initiate and control the implementation of information security within CentralNic. The Chief Technology Officer (CTO) is responsible for coordinating the Information Security Team (IST) quarterly meetings, and is also responsible for chairing those meetings. The minutes from the meeting are stored on the wiki.

As Information Security is core to CentralNic's existence, CentralNic has assembled the following IST to proactively manage information security. The IST is a cross-functional team from relevant areas of CentralNic. These key members of staff are responsible for cascading rules, regulations and information to their respective departments. They are also the first port of call for their departmental staff to report potential security incidences and breaches, the IST are all members of the its@centralnic.com email group.

Name: Gavin Brown	**Name**: Ben Crawford
Job Title: Chief Technical Officer	**Job Title**: Chief Executive Officer
Email: gavin.brown@centralnic.com	**Email**: ben.crawford@centralnic.com
Tel: +44 (0)20 3435 7319	**Tel**: +44 (0)20 3435 7318
Mobile: +44 (0)7930 218898	**Mobile**: +44 (0)7540 723115
Name: Jenny White	**Name**: (TBC)
Job Title: Operations Manager	**Job Title**: Senior Operations Engineer
Email: jenny.white@centralnic.com	**Email:** (TBC)
Tel: +44 (0)20 3435 7307	**Tel:** (TBC)
Mobile: +44 (0)7900 804227	**Mobile:** (TBC)

The responsibilities of the IST include:

- Review and monitor information security threats and incidents.
- Approve initiatives and methodologies to enhance information security.
- Agree and review the Information Security Policy, objectives and responsibilities.
- Review client requirements concerning information security.
- Promote the visibility of business support for information security company-wide.

- Manage changes to 3rd party services that may impact on Information Security
- All employees are empowered to take responsibility for quality and information security and to be vigilant of any potential security threat.
- Ultimate responsibility for quality and information security rests with our Chief Executive Officer .
- Responsibility for the annual review of this policy lies with the CTO for approval by the Chief Executive Officer.
- The Line Managers are responsible for the quality and security of their physical environments where information is processed or stored. They are responsible for ensuring that permanent and temporary staff and contractors are aware of:-
- The quality procedures and information security policies applicable to their work areas
- Their personal responsibilities for quality and information security
- How to seek advice on quality and information security matters.
- Staff – each member of staff is responsible for the quality and operational security of the information systems they use. They shall comply with all quality and information security procedures including the maintenance of data, confidentiality and data integrity. Failure to do so may result in disciplinary action.
- Internal/External System User – each individual shall comply with the quality and security requirements that are currently in force and shall also ensure confidentiality, integrity and availability of information they use is maintained to the highest standards.
- Contracts with External Contractors – where access is required to the organisations information systems, restricted authorisation is granted before access is permitted.
- Visitors to CentralNic's office in Moorgate must be signed in upon arrival. Responsibility for compliance with this policy lies with the person the visitors have come to see, or with the Operations Manager.

5.6.1 Management Representative

The CTO is responsible for managing the implementing, monitoring, documenting and communicating of all quality and security information policies, regulated standards, guidelines and practices on a day-to-day basis. The CTO shall keep the CentralNic Board of Directors informed of the information security status of the organisation by means of regular reports and presentations.

6 Implementation and Operation

6.1 Operational Control

CentralNic has developed and implemented a comprehensive set of operational procedures for the key activities, products and services that the company provides. These are described in:

- Business Development procedure
- Technical Services procedure
- Customer Services procedure
- Software Development procedure

These procedures are complimented and supported by the following:

- Finance procedure
- Marketing procedure
- Human Resources (HR) procedure

6.2 Purchasing

The purchasing process is available on the wiki.

6.3 Third-party Service Delivery Management

To implement and maintain the appropriate level of information and service delivery, third-party service agreements i.e. Service Level Agreements (SLA) should be implemented, operated and maintained by the third-party.

The services, reports and records shall be regularly monitored and reviewed, and audits shall be conducted regularly.

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls shall be manage, taking into account the criticality of business systems and processes involved and re-assessment of risks.

6.3.1 Confidentiality

Third-party suppliers who have access to the company's information assets, either by providing storage or communications services, must either:

1. Address the confidentiality of company information assets in the Terms of Service or Service Agreement, or
2. Sign a Deed of Confidentiality that obliges them to protect company information assets to which they have access.

Third-party supply contracts will be reviewed alongside the service reviews described above.

6.4 Management of Resources

6.4.1 Provision of resources

The company is committed to providing the essential human, physical and financial resources to manage and maintain this management system in order to ensure our customers' requirements are met. Resources will be discussed at management review meetings and any shortfalls addressed accordingly.

6.4.2 Physical & Environmental Security

To prevent unauthorised physical access, damage and interference to CentralNic's premises, information security perimeters are controlled where necessary i.e. isolated Server Room, key fob entry systems. Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

Access rights to secure areas at all sites are regularly reviewed and updated. Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

Access to computer facilities at all sites shall be restricted to authorised users who have a legitimate business need to use the facilities. Access to data, system utilities and program source code shall be controlled and restricted to those authorised users who have a legitimate business needs. Authorisation to use an application shall depend on manager's approval and availability of licenses.

A Disaster Recovery Plan is in place to protect CentralNic in the event of external environmental threats i.e. flood, terrorism, pandemic flu or major network outage.

The Operations Manager is responsible for authorising access to the Moorgate office. Suppliers, clients, stakeholders and members of the public shall sign in upon arrival. External couriers are asked to wait in reception and are not to enter any information processing areas.

Having a record of who is present on site not only tightens security of the building, but it is also necessary for Health and Safety reasons.

Access to the controlled areas (i.e. the server room) are controlled by a locked door, the key for which is only held by the CTO and Operations Manager.

Access to the Goswell Road data centre is subject to the access controls of the building owner, Level 3. Authorized persons are issued a swipe card bearing a photograph and must pass through a reception manned 24x7. The photograph on the card is used to confirm the identity of the bearer. A keypad is also used to restrict access to the technical area and to Qube's suite. The racks themselves are also secured with a combination lock. Access to the combination is restricted to authorized CentralNic and Qube personnel only.

Waste collections and delivery areas are controlled and isolated. Deliveries are dealt with at reception and a CentralNic employee informed.

All employees are encouraged to challenge unescorted strangers.

6.4.3 Human Resources

Confidentiality & Non-Disclosure Agreements

Confidentiality Agreements are signed by all employees prior to employment. Non-Disclosure agreements are signed by third-parties who may have access to CentralNic's assets i.e. contractors, suppliers.

Personnel Security

Personnel security is required to ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. The HR Manager is responsible for retaining HR related documents and records securely.

Security roles and responsibilities of employees are defined in the Employee Handbook and in accordance with CentralNic's Information Security Management Policy. Contractors and third-party users are also expected to adhere to CentralNic's Information Security Policy and Procedures where necessary.

Information security expectations shall be included within appropriate job descriptions.

Personnel Security Screening

Background verification checks on permanent staff are carried out at the time of the job applications. The screening process is documented in further detail in Human Resource Management Process.

The controls within the Guide include the following:-

- Availability of satisfactory references;
- A check (for completeness and accuracy) of the applicant's curriculum vitae;
- Confirmation of claimed academic and professional qualifications;
- Independent identity check (passport or similar document)

Screening of prospective candidates that have been recommended for employment shall be carried out in accordance with relevant laws, regulations and ethics, and are proportional to the business requirements and potential access to sensitive information.

A similar screening process is carried out for contractors and temporary staff. Where staff have been provided by an agency, then the agency should clearly specify their responsibilities for screening.

Management will evaluate the supervision required for new and inexperienced staff with authorisation for access to sensitive information.

Terms and Conditions of Employment

As part of new employees' contractual obligation, they shall agree and sign the terms and conditions of their contract for employment including CentralNic's Confidentiality Agreement.

Confidentiality Agreements

Employees sign a confidentiality agreement as part of their terms and conditions of employment.

Temporary staff and third-party users are also required to sign a confidentiality Agreement prior to being given access to information processing facilities.

The Confidentiality agreements are reviewed periodically.

During Employment

To ensure that all employees, contractors and third-party users understand their responsibility concerning security, an induction takes place which covers the various aspects of information such as the Information Security Management Policy and relevant procedures.

Appropriate information security awareness training is given to employees, in addition to regular updates to refresh and inform them of any changes to the policy, objectives or procedures. This includes security requirements, legal responsibilities and business controls. Training is also given on information processing systems before access to information is granted i.e. log-in procedure.

Authorisation for access to information processing facilities is guaranteed by the operations director.

Employees who commit a serious security breach will be subject to a formal disciplinary.

Termination or change of employment

New Employee IT Request Form is used to process the authorisation to systems.

Upon termination of employment contract, the Operations Manager (Jenny White) raises an *Employee Leavers Form which is* distributed internally to those with responsibility for withdrawing access to CentralNic's assets i.e. access to software, laptops. The IT department will be advised of the date to remove access rights to information processing facilities.

All employees, contractors and third-party users shall return all of the company assets in their possession upon termination of their employment, contract and agreement.

6.4.4 Competence, Awareness and Training

All employees and persons employed in the provision of a service to either CentralNic or our clients will be trained and competent on the basis of either having the appropriate skills or experience required.

Competency requirements for contractors will be established on an as and when basis. Training needs for staff will be identified and discussed at Management review and also during staff appraisals. Where a training need is identified, staff will be trained and feedback sought as to the effectiveness of the training in meeting the company's needs.

Records of staff and contractor competency will be retained by either the Operations Manager or the appropriate member of the management team.

6.4.5 Infrastructure & Asset Management

All major information assets have been accounted for and have nominated owners. Accountability for assets will help to ensure appropriate protection is maintained. Access rights are controlled and documented by the Access Control Policy which is located on the Wiki.

An Inventory of assets is documented within the Business Continuity Plan which is updated annually. It is also retained for other uses i.e. insurance, financial and health and safety. Assets have clearly been identified within the Risk Assessments which provides levels of protection commensurate with the value and importance of the assets.

Assets associated with the information systems are:-

- **Information assets**: databases and data files, system documentation, user manuals, training material, operational procedures, continuity plans, archived information.
- **Software assets**: application software, system software, source code, configuration files, development tools and utilities;
- **Physical assets**: computer equipment (PCs, Switches, monitors), communications equipment (routers, fax machines), magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, accommodation;
- **Services**: computing and communications services, general utilities e.g. heating, lighting, power and air-conditioning.

The rules for the acceptable use of information and assets with information processing facilities are identified, documented and implemented by the IST and are also referenced in the Employee Handbook.

All mobile, valuable assets shall be labelled.

Equipment Security

To prevent loss, damage, theft to equipment and prevent disruption of services, equipment is sited to reduce the risks from environmental threats and opportunities for unauthorised access. This includes protection from power failure; an example of this is the automatic failover to redundant power at the Goswell road data centre.

Equipment is sited to minimise unnecessary access to work areas i.e. location of printers, photocopiers.

Power and telecommunications cabling is protected from interception and damage by having a security controlled environment with an uninterruptible power supply (UPS).

Equipment is regularly maintained to minimise disruption of services.

Security of Equipment Off-premises

Equipment, information or software shall not be taken off-site without prior authorisation from a line manager and or CTO. If a line manager/ CTO is not available, then the next appropriate manager should then authorise it.

Information processing equipment includes all forms of personal computers, mobile phones, paper or other form, which is held for home working or being transported away from the normal work location.

Employees should be vigilant of equipment that is stored off-site i.e. laptops, home computers, smart phones and tablet computers to prevent damage, loss or theft. Equipment and media should not be left unattended in public places.

Risk assessments on home workers are to be carried out where possible to assess suitable controls and are applied as appropriate i.e. lockable filing cabinets, clear desk policy.

Adequate insurance cover is in place to protect equipment both on and off-site.

Password Management

Users are expected to follow good security practices in the selection and use of passwords.

The Password Management Policy is:

- All users should use unique passwords.
- Passwords should be changed every 90 days where systems support this capability.
- Reuse of passwords used elsewhere, (eg webmail, social networking, etc) should be avoided
- Passwords must be a minimum of 8 characters, a minimum of 1 capital, minimum of 1 number and one special character (assuming system support this). i.e. m3llyMe!

If an employee needs to access a colleague's computer, then they need to complete the relevant request form with signed approval from their line manager and submitted to IT. A Bug Tracker report will then be raised.

System Management Passwords

Passwords that control access to systems such as servers, switches and routers, databases, encrypted filesystems and other information processing systems are regularly changed. The Password Update Schedule in Dropbox provides a record of when passwords were changed, and how frequently they should be changed. This frequency is calculated using a similar approach to that used in the Risk Assessment, and is explained in the Schedule.

User Media

Use of removable media of all types is restricted. Those requiring the use of removable media for legitimate business needs require the approval of the CTO. Such media must be fully virus checked before being used on Company property.

6.4.6 Work Environment

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access, loss of, and damage to information during and outside of office hours, CentralNic has introduced a clear desk and clear screen policy.

Where appropriate, paper and computer media should be stored in suitable cabinets, especially outside working hours.

Sensitive or critical business information should be locked away when not required.

When unattended, computers should automatically lock their screens after 10 minutes, and be configured to require a password to unlock the screen. If the computer is unattended for a longer duration then the user should log off the computer.

6.5 Documentation Requirements

6.5.1 Control of Documents & Information Classification

The Control of documents procedure is available on the wiki.

To ensure that information receives an appropriate level of protection CentralNic's information is reviewed where necessary to determine whether a classification of its value and sensitivity are critical to the company.

The classification scheme has been adopted by the IST and communicated to the relevant employees. Any sensitive documents should be labelled private and confidential.

The following classification scheme applies:-

- **Publicly available** – i.e. marketing collateral, website, documentation and specifications
- **Internal Use Only** – i.e. internal policies and procedures, internal Forms, minutes, documentation
- **Private and Confidential** - i.e. finance records, HR records, IT information security records, SRS database data, source code, system configuration files, authentication credentials, cryptographic material (such as DNSSEC keys and SSL certificates)

Information highlighted to the Company as requiring additional security will be individually risked assessed and a bespoke procedure put in place.

6.5.2 Control of Records

Records that are required to demonstrate the effectiveness of the management system will be retained by the CTO for the period defined in the document control register. Following the expiry of the retention period records will be disposed of only using methods that will ensure that information is not lost or passed to other parties. Further details of controlling records can be found on the wiki 'Control of documents and records.'

6.6 Communication

Good communication is a key to establishing a satisfactory working environment. All employees are empowered to share knowledge with employer to develop the business and also communicate suggested improvements to benefit both employees and clients.

CentralNic develops and implements effective methods of communicating with customers in relation to product information, enquiries, contracts or order handling, including amendments and customer feedback, including customer complaints.

6.6.1 Internal Communication

CentralNic has established and maintains internal communication at various levels regarding the processes of the QMS and their effectiveness. Staff feedback is welcomed and may be made directly to the Managing Director. The feedback is presented at the regular quality review meetings.

6.6.2 Customer / Other Parties

CentralNic operates a policy of exceeding clients' expectations. In order for CentralNic to understand and deliver the ever-changing demands of clients the following initiates have been put in place to manage customer relationships and retention: -

Customers are kept up to date with the latest information by providing: -

- Promotional literature - latest exhibition, large screen print offers, product information.
- Email – Information regarding changes to exhibition plans due to external factors i.e. security alerts, site plan changes.
- Exhibition Schedule – outlines clients exhibition arrangements
- Website – Examples and further information on products and services.
- Telephone/meetings – Regular progress updates relating to exhibitions either by telephone or face to face.

6.6.3 Receipt and Processing

CentralNic maintain the security of the information processing facilities that are accessed, processed, communicated to, or managed by external parties.

The risks associated have been assessed through the risk assessment and Statement of Applicability and relevant controls have been endorsed to reduce risk.

All identified security requirements shall be addressed before giving customers access to the company's information or assets.

Agreements with existing third parties have been reviewed and revised as necessary. Any new third-parties shall be vetted through the Approved Supplier process and also made to sign a Non-Disclosure agreement.

7 Performance Assessment

7.1 Monitoring and measurement

CentralNic determines the monitoring, measurement, analysis and improvement processes, including methods such as statistical techniques that are needed to:

- Demonstrate conformity of the product and service;
- Ensure conformity of the Management System;
- Continually improve the effectiveness of the Management System.

7.1.1 Client Satisfaction

To monitor customer perception CentralNic regularly obtain input of variety of sources including:

- Customer Feedback Form
- Client Review Meetings (during project and upon completion of the project).
- Continual Service Improvement Process

The CEO holds review meetings where necessary with clients to determine the level of satisfaction with the service provided by CentralNic. For some clients the frequency of this type of meeting is in accordance with the contract. Day-to-day contact is maintained with the client by means of phone calls and face-to-face contact. When a complaint is made, the client feedback procedure is followed and the client is advised of the outcome.

CentralNic reveals customer feedback and testimonials on the website.

7.2 Evaluation of Compliance

All employees are empowered to ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

IT compliance is regularly checked by the CTO, and any reported non-compliance is logged in the IT Help desk.

7.2.1 PCI Compliance

CentralNic maintains compliance with the Payment Card Industry Data Security Standard (PCI DSS). This is a required by the acquiring bank used for credit and debit card payments.

CentralNic's PCI compliance is certified and monitored by an external assessor, SecurityMetrics, Inc. SecurityMetrics perform periodic network scans and automated penetration tests of CentralNic's online card processing systems and report any nonconformities. Any issues raised by these scans must be addressed using the normal change management procedures (ie Bug Tracker). The CTO is responsible for maintaining PCI compliance and assuring that nonconformities are rectified as quickly as possible.

7.3 Internal audit & Independent Review of Information Security

The Internal Audit Procedure includes internal audits on the Information Security Management System. (Refer to the Internal Audit Procedure).

CentralNic's approach to managing information security and its implementation is reviewed independently at planned intervals by specialists in Information Security Management such as SGS (Certification body) and Blackmores (Consultant).

7.4 Handling of Non Conformities & Responding to security incidents and malfunctions

To minimize the damage from security incidents and malfunctions, quality control concerns, incidents or potential incidents affecting security should be reported as quickly as possible.

Employees should primarily report IT and building related security incidents to an IST member who will ensure that it has been entered into the Bug Tracker. The report may be done verbally or by email, but if verbally, must be followed up by email. If the relevant people are not available, then the incident should be reported to their line manager, who will then take responsibility for reviewing and logging the incident. IST members log all reported incidents in the Bug Tracker. The IST members are listed in section 5.0 (Information Security Responsibilities). Users should not in any circumstances try and attempt to prove any suspected weakness.

Types of incidents that should be reported are:-

- Information system failures and loss of service
- Denial of service attacks
- Errors resulting from incomplete or inaccurate business data
- Breaches of confidentiality

Any software malfunctions should be reported immediately to the CTO. The user should make a note of the symptoms of the problem and any error messages that have appeared on the screen. Users should not attempt to remove the suspected software unless authorised to do so.

Action to recover from security breaches and correct system failures are controlled by the CTO and/or IT department. All information security events shall be subject to our non-conformance procedure. Changes identified following this procedure will be implemented and communicated through our system change controls.

Any quality related non-conformances are also logged via the Bug Tracker, this ensures that non-conformances are logged, root cause identified and action is taken until a satisfactory conclusion is derived.

The Bug Tracker is monitored regularly by the CTO. Any potential, or reoccurring incidents raised should be flagged to the IST and/or the Board. The IST and/or the Board will decide whether enhanced or additional controls are required to limit the frequency, damage and cost of future occurrences.

Where necessary, disciplinary action will be taken for those employees in breach of the Information Security Policy and Procedures.

7.4.1 Incident Reporting

In certain situations, it is necessary that a report is made about an incident. An incident is an event attributable to a human root cause. These incidents can be malicious, unintended or caused by system failure.

Incidents can be broken up into three different classifications as follows:

- **Normal** – a normal event does not affect critical components or require change controls prior to the implementation of a resolution. Normal events do not require the participation of senior personnel or management notification of the event.
- **Escalated** - an escalated event affects critical production systems or requires that implementation of a resolution that must follow a change control process. Escalated events require the participation of senior personnel and stakeholder notification of the event.
- **Emergency** - an emergency is an event which may:
    - impact the health or safety of human beings
    - breach primary controls of critical systems
    - materially affect component performance or because of impact to component systems prevent activities which protect or may affect the health or safety of individuals
    - be deemed an emergency as a matter of policy or by declaration by the available incident coordinator

When an event occurs, it should be reported to the Information Security Team for processing. An event can be reported by an employee, vendor, customer, partner, device or sensor. A report relating to the event is created in the Bug Tracker in order for the IST to resolve the incident. Once the report has been processed and possibly resolved by the IST, it is sent back to the original event reporter.

The reporter will then decide if the event has been adequately resolved or if it needs further escalation. If the event has been escalated to the level that an emergency response is seen as necessary, an incident response coordinator will be assigned, this will be any IST staff member available at the time of the incident. The process is then as follows :

- The incident coordinator assembles the incident response team. This meeting must be attended by the CEO and CTO.
- The meeting minutes capture the status, actions and resolution(s) for the incident. The incident coordinator reports on the cost, exposure and continuing business risk of the incident. The incident response team determines the next course of action:

    - Lock-down and Repair – Perform the actions necessary to prevent further damage to the organization, repair impacted systems and perform changes to prevent a re-occurrence.
    - False Positive – The incident team determines this issue did not warrant an emergency response. The team provides a written report to senior management and the issue is handled as a normal incident or closed.
    - Monitor and Capture – Perform a thorough investigation with continued monitoring to detect and capture the perpetrator. This process must include notification to the CEO, CFO, Corporate Attorney and Public Relations
- Review and analyze log data to determine nature and scope of incident. This step would include utilizing virus, spyware, rootkit and other detection tools to determine necessary mitigation and repair.
- Repair Systems, eliminate vector of attack mitigate exploitable vulnerabilities
- Prepare a Test Report that documents the validation of the repair process.
- Test Systems to ensure compliance with policy and risk mitigation.
- Perform additional repairs to resolve all current vulnerabilities.

- Investigate incident to determine source of attack and capture perpetrator. This will require the use of forensics tools, log analysis, clean lab and dirty lab environments and possible communication with Law Enforcement or other outside entities.
- The "Investigation Status Report" captures all current information regarding the incident. The Incident response team uses this information to determine the next course of action.

8 Improvement

8.1 General

CentralNic continually improves the effectiveness of the management system through the use of the Company policies, objectives, audit results, analysis of data, corrective and preventive actions and management reviews.

8.2 Corrective, preventative and improvement action

CentralNic have established, implemented and maintain documented procedures to initiate corrective and preventive actions for conditions adverse to quality. The company is responsible for Corrective Actions and a feedback system is used to provide early warning of quality problems and for input into the corrective action system.

All corrective and preventive actions are logged via the Bug Tracker, this ensures that non-conformances are logged, root cause identified and action is taken until a satisfactory conclusion is derived. The Bug Tracking system controls the entire corrective and preventive action procedure, and produces reports on the outcome.

Preventive action shall be initiated to prevent occurrence of **potential** problems and risk in the operations of the company. Management Review meetings will also cover the evaluation and review of corrective and preventative action including reduction of risk within the business.

9 Management Review

9.1 General

The management system will be reviewed every twelve months and recorded at planned intervals in order to:

- Ensure its continuing adequacy and effectiveness;
- Consider ongoing compliance to ISO9001 and ISO27001
- Consider opportunities for improvement;
- Review the Quality, and Information security Policies;
- Ensure the management systems effectiveness;
- The need for changes to the management system (including the policy and objectives).

Records of the review shall be taken and maintained for a minimum of 3 years

9.2 Input

Documented on the Management Review meeting template

9.3 Output

The output from the management review includes any decisions and actions related to:

- Improvement of the effectiveness of the management system and its processes;

- Improvement of service related to customer requirements;
- Resources;
- Ensure continual improvement of the management system

10 Operational Procedures

- Business Development procedure
- Technical Development procedure
- Customer Services procedure

- Finance procedure
- Marketing procedure
- Human Resources (HR) procedure