ISO/EIC 27001:2005

Statement of Applicability

Version 1.2
16/01/2013 10:18

Internal Use Only

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
A.5 Security Policy				
A.5.1 Information Security Policy Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.				
A.5.1.1	Information security policy document	An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.	Policy created (Management System) Approved policy Information security policy document Published and communicated. Policies are on display in the office.	MB GB GB
A.5.1.2	Review of the information security policy	The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	Review of the information security policy Document processed (MSM 1.1) Information policy reviewed throughout implementation process	MB
A.6 Organisation of information security Management				
A.6.1 Internal organisation Objective: To manage information security within the company.				
A.6.1.1	Management commitment to information security	Management shall actively support security within the organisation through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.	MSM objectives set (Objectives on Wiki and referenced MSM5.4) Job descriptions provided for all key staff. Created IS Policy (MSM 4.2) Communicated IS Policy (MSM 4.2)	MB JW/GB MB MB/GB
A.6.1.2	Information Security co-ordination	Information security activities shall be co-ordinated by representatives from different parts of the company with relevant roles and functions.	The Information Scurity Team has been initiated (MSM 5.6) Company Structure diagram (MSM 5.5.3)	GB
A.6.1.3	Allocation of information security responsibilities	All information security responsibilities shall be clearly defined.	Allocation of information security responsibilites Updated in Employee handbook. Information security responsibilities & JD's listed Included IST responsibilities in the ISM (5.5.4 & 5.6 and 5.6.1)	HR/MB HR/MB MB
A.6.1.4	Authorisation process for information processing facilities	A management authorisation process for new information processing facilities shall be defined and implemented.	New Employee IT Request form (drop box) faciliates authorisation of new information processing facilities. Reviewed authorisation process i.e. new employee set up. New starter IT request form sent via Jenny and set up account i.e. Email/VPN etc. The form drives the process for new starters. Also discussed with HR.(MSM 6.4.3) Updated Standard Induction Timetable and 'New Starter Checklist'. Updated Contract of employment and signed by NDA.	JW

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
A.6.1.5	Confidentiality agreements	Requirements for confidentiality or non-disclosure agreements reflecting the company's needs for protection of information shall be declined	Confidentiality agreements reviewed and signed. (MSM 6.4.3) New confidentiality agreements drafted if required to include MSM requirements GB has copies of supplier contracts and condfidentionally. Critital supplier services reviewed and confirmed agreemtns in place or NDA's sigend. (MSM 6.3)	JW GB/MB JW
A.6.1.6	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Contact with authorities documented within business continutiy plan. Jenny maintains list of key contacts, landloard, electricity, gas which have been incorporated.	GB
A.6.1.7	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security and professional associations shall be maintained.	No subscription services, however any specialist advice is sought through legal, HR and information security management system services. These services are reviewed annually at the management review meeting	GB
A.6.1.8	Independent review of information security	The company's approach to managing information security and its implementation (i.e. control objectives, control, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur	BQMS (information security and quality management support) + LRQA (certification body) appointed. ICANN (internet governance body) will conduct evaluation of information security policies as part of new top-level domain application evaluation. SecurityMetrics (PCI certification body) appointed to perform quarterly penetration tests and scans as part of PCI compliance.	MB
A.6.2 External Parties Objective: to maintain the security of the company's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.				
A.6.2.1	Identification of risks related to external parties	The risks to the organisation's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.	Risk Assessment procedure created and documened whcih supports the completed Risk assessment. (MSM 5.1)	MB
A.6.2.2	Addressing security when dealing with customers	All identified security requirements shall be addressed before giving customers access to the company's information or assets.	CentralNic operates an automated API (Application Programming Interface) based on the Extensible Provisioning Protocol (EPP) which provides external access to the registry system as well as a web based Registrar Console. Both systems are secured using SSL, with authentication via username and password. The EPP system further requires client IP addresses to be registered in advance, and the use of a client SSL certificate. The Registrar Console supports multiple user accounts for each registrar client, and each account can be given different levels of access to the system. Procedure in place for communications via email, telephone etc.	GB
A.6.2.3	Addressing security in third party agreements.	Agreements with third parties involving accessing, processing, communicating or managing the company's information or information processing facilities shall cover all relevant security requirements	Procedure created. (MSM 6.3)	MB

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
A.7 Asset Management				
A.7.1 Responsibility for assets Objective: To ensure that information receives an appropriate level of protection.				
A.7.1.1	Inventory of assets	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.	The IST have identified all assets by department and included within the risk assessment. (Risk Assessment) Assets are reviewed as part of the management review process and updated accordingly at least annually. (MSM 5.1) (6.4.5) All assets of value to the business i.e. Laptops are labelled and linked to the asset register.	GB
A.7.1.2	Ownership of assets	All information and assets associated with information processing facilities shall be owned by a designated part of the company.	Included in Risk Assessment under 'responsibilities' column. (MSM 5.1)	GB/RS
A.7.1.3	Acceptable use of assets	Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.	Updated Staff handbook, T+C, Internal communication to employee, joining instructions.	MB
A.7.2 Information Classification Objective: To ensure that information receives an appropriate level of protection.				
A.7.2.1	Classification guidelines	Information shall be classified in terms of its value, legal requirements, sensitivity and critically to the company.	Classification system has been adopted company-wide and documented within (MSM 6.5.1)	GB
A.7.2.2	Information labelling and handling	An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organisation.	Information labelling and handling Procedure created (6.4.5 and 6.5.1)	MB

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
A.8 Human resources security				
A.8.1 Prior to employment Objective: To ensure that employees, contractors and third party users understand their responsibility, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.				
A.8.1.1	Roles and responsibilities	Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organisation's information security policy.	Defined and documented security responsibilities for all employees. (summary sheet) Job Descriptions created for IST members. Procedure created (5.5.4)	MB
A.8.1.2	Screening	Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.	Screening procedure updated by MB Procedure created (6.4.3)	MB
A.8.1.3	Terms and conditions of employment	As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the company's responsibilities for information security.	Procedure created (6.4.3). Existing terms and conditions reviewed and amended where necessary. Updated employee T & C	JW
A.8.2.1	Management responsibilities	Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the company.	Procedure created (5.6.1) Company IS objectives Company objectives, policy and MSM approved	MB GB MB/GB
A.8.2.2	Information Security awareness, education and training	All employees of the company and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in company policies and procedures, as relevant for their job function.	Procedure created (6.4.3) Training to raise awareness of changes have been arranged. Included MSM in induction process.	MB MB JW
A.8.2.3	Disciplinary process	There shall be a formal disciplinary process for employees who have committed a security breach.	Procedure created (5.3.1) If there has been a security breach it is referenced in the disciplinary process.	MB HR
A.8.3 Termination or change of employment Objective: To ensure that employees, contractors and third-party users exit the company or change employment in an orderly manner.				
A.8.3.1	Termination responsibilities	Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.	Existing process for employees leaving the company have been reviewed. Changes have been implemented where necessary. Procedure created (6.4.3)	MB/JW

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
A.8.3.2	Return of assets	All employees, contractors and third party users shall return all of the company's assets in their possession upon termination of their employment, contract or agreement.	Return of assets included in contract of employment and 'leavers process'. Procedure created (6.4.5)	MB/JW
A.8.3.3	Removal of access rights	The access right of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, adjusted upon change.	Reviewed existing process and implemented changes where necessary. Procedure created (6.4.3)	MB
A.9 Physical and environmental security				
A.9.1 Secure areas Objective: to prevent unauthorised physical access, damage and interference to the organisations premises and information.				
A.9.1.1	Physical security perimeter	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.	Controls documented in MSM (6.4.2). Access Control Policy on the wiki	GB/MB
A.9.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	Secure areas have been identified and assessed to ensure sufficient controls are in place. Visitors book utilised at CentralNic offices	GB/MB
A.9.1.3	Securing offices, rooms, and facilities	Physical security for offices, rooms, and facilities shall be designed and applied.	Procedure created (6.4.5)	GB
A.9.1.4	Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of disaster shall be designed and applied.	sent Jenny some examples of evidence which were checked on the 8.2.12. Landlord's agreement to be reviewed to check protection from external threats. Qube contract to be reviewed for same	GB
A.9.1.5	Working in secure areas	Physical protection and guidelines for working in secure areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.	Procedure created (6.4.6). GB to review.	GB
A.9.1.6	Public access, delivery and loading areas	Access points such as delivery and loading areas and other points where authorised persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.	GB to reviewed the physical security procedures (5.5.4)	GB/MB
A.9.2 Equipment security Objective: To prevent loss, damage, theft or compromise of assets and interruption to the company's civilities.				
A.9.2.1	Equipment siting and protection	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for	Servers held at Goswell road, building owned by level3, operated by QUBE service provider. Systems owned by CentralNic and DR site in Isle of Man which is	GB

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
		unauthorised access.	virtualised. Procedure created (6.4.5)	
A.9.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Managed services included in Landlords agreement, however CentralNic does own the elements of the power failover equipment.	GB
A.9.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	Controls implemented to protect from interception or damage. Cabling is checked regularly. Cable Management provided by TreeGold	GB
A.9.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Managed as part of warranties that exist. GB to ensure that elements are documented. (MSM 6.4.5)	GB
A.9.2.5	Security of equipment off-premises	Security shall be applied to of-site equipment taking into account the different risks or working outside the organisations premises.	Procedure created (MSM 6.4.5)	GB
A.9.2.6	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	Secure disposal or re-use of equipment is referenced in document. Secure wipes done, two unix rewrites performed. IT Equipment Waste Disposal Policy (Wiki)	GB
A.9.2.7	Removal of property	Equipment, information or software shall not be taken off-site without prior authorisation.	Procedure created (6.4.5)	GB
A.10 Communications and operations management				
A.10.1 Operational procedures and responsibilities Objective: To ensure the correct and secure operation of information processing facilities.				
A.10.1.1	Documented operating procedures	Operating procedure shall be documented, maintained, and made available to all users who need them.	Operational Procedures documented on Wiki. Review and perform audit.	GB
A.10.1.2	Change management	Changes to information processing facilities and systems shall be controlled.	Changes to software, database and server systems are governed by the development procedure. All changes are subject to tracking and peer review.	GB
A.10.1.3	Segregation of duties	Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the company's assets.	Access controls in place to segregate duties. Only designated system administration staff have administration privileges on servers. Network device configuration is monitored and controlled. Version control system is used to enforce configuration, live device config is checked regularly by an automated system. VC system has controls on who can commit. All superuser account activity is logged.	GB
A.10.1.4	Separation of development, test and operational facilities.	Development, test and operational facilities shall be separated to reduce the risks of unauthorised or unintentional modification or misuse of the company's assets.	Environments, - Development, Staging, OT&E (operational tesitng and evaluation), production. Documented by way of a network diagram.	GB

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
A.10.2 Third party service delivery management Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.				
A.10.2.1	Service delivery	It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.	SLA's identified Procedure created (6.3)	GB
A.10.2.2	Monitoring and review of third party services	The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.	Procedure created (7.1). Identified security clauses in key contracts (e.g. Qube).	GB
A.10.2.3	Managing changes to third party services	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking into account of the criticality of business systems and processes involved and re-assessment of risks.	Procedure created (6.3)	MB
A.10.3 System planning and acceptance Objective: To protect the integrity of software and information				
A.10.3.1	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Capacity Management policy in place (Wiki)	GB
A.10.3.2	System acceptance	Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior acceptance.	Software Update Policy (Wiki) governs installation and maintenance of systems. All software must be tested in laboratory conditions before deployment. Software developed in-house is subject to multi-stage testing and deployment.	GB
A.10.4 Protection against malicious and mobile code Objective: To protect the integrity of software and information.				
A.10.4.1	Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.	Antivirus Policy in place (5.3.2). All incoming email is filtered by third-party email service (Symantec Cloud). Unix based servers are less susceptible to malware so AV is not used to avoid performance penalties. All software packages from upstream vendors are digitally signed.	GB

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
A.10.4.2	Controls against mobile code	Where the use of mobile code is authorized, the configuration shall ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code shall be prevented from executing.	Use of Internet Explorer is forbidden (except for web developers testing compatibility) to avoid drive-by downloads of malware, ActiveX plugins, etc (Wiki)	GB
A.10.5 Back-up Objective: To maintain the integrity and availability of information and information processing facilities.				
A.10.5.1	Information back-up	Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed back up policy.	Backup Policy in place (Wiki). Backups are performed on daily basis (some hourly) and are stored in multiple locations. Access to backups is restricted to authorised personnel. Procedures in place to govern restoration from backups. Procedures in place to test backups.	GB
A.10.6 Network security management Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.				
A.10.6.1	Network controls	Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	Network controls documented on Wiki. Networks physically secured using locked comms cabinets and secure cabling in ceilings, flooring or trunking. Arpwatch system used to monitor appearance of devices on network. Separate guest wifi network for visitors.	GB
A.10.6.2	Security of network services	Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	Network service security controls documented on wiki. Encryption (ie SSL) to be used wherever permitted: HTTPs, IMAP/SMTP, VPN etc. Access lists used to restrict access to services to authorised hosts.	GB
A.10.7 Media handling Objective: To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.				
A.10.7.1	Management of removable media	There shall be procedures in place for the management of removable media.	Removable media policy available on Wiki.	GB
A.10.7.2	Disposal of media	Media shall be disposed of securely and safely when no longer required, using formal procedures.	Disposal of media Documented on Wiki.	GB
A.10.7.3	Information handling procedures	Procedures for the handling and storage of information shall be established to protect this information from unauthorised disclosure or misuse.	Information handling procedures Documented.	GB
A.10.7.4	Security of system	System documentation shall be protected against unauthorised	Security of system documentation identified and documented controls	GB

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
	documentation	access.		
A.10.8 Exchange of information Objective: To maintain the security of information and software exchanged within an organisation and with any external entity.				
A.10.8.1	Information exchange policies and procedures	Formal exchange policies, procedures and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.	Privacy Policies in place and published on websites. Privacy Policy for domain registry system in place. Registrar Contact Procedures (Wiki) in place to govern communications with customers.	GB
A.10.8.2	Exchange agreements	Agreements shall be established for the exchange of information and software between the organisation and external parties.	NDAs and confidentiality deeds used with third party suppliers and contractors. Registrar accreditation agreeements include obligations on customers to ensure confidentiality and integrity of exchanged information.	GB
A.10.8.3	Physical media in transit	Media containing information shall be protected against unauthorised access, misuse or corruption during transportation beyond an organisations physical boundaries.	Removable Media Policy in place (Wiki).	GB
A.10.8.4	Electronic messaging	Information in electronic messaging shall be appropriately protected.	Network service security controls require use of SSL where possible: eg when sending/receiving mail via SMTP or IMAP. Corporate XMPP service requires use of SSL. Internal email never leaves the company network. PGP is used where available and appropriate.	GB
A.10.8.5	Business information systems	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business systems.	Business information systems documented.	GB
A.10.9.1	Electronic commerce	Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorised disclosure and modification.	CentralNic collects payments using bank transfers, credit cards, and PayPal. SSL protects all transactions. Credit card information is never stored in any form. All communications with payment gateway (DataCash) are encrypted and protected by IP access list. Fraud Mitigation Policy in place (wiki). Chargeback handling procedure in place (wiki).	GB
A.10.9.2	On-line transactions	Information in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.	CentralNic maintains PCI compliance as per requirement from acquiring bank. Third party compliance assessor (SecurityMetrics) enforces compliance. Regular network scans and penetration tests are performed and reported to Operations team for corrective action as needed. CTO has responsibility for ensuring compliance.	GB
A.10.9.3	Publicly available information	The integrity of information being made available on a publicly available system shall be protected to prevent unauthorised modification.	Web servers and other servers providing public information are secured behind firewalls, access is via SSH from authorised hosts. Website content is managed via CVS, provides full change logs. Data provided via Whois and DNS comes from registry database, access to which is restricted and logged. Changes to website authorised by Marketing Director and made by development/design teams.	GB

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
A.10.10 Monitoring Objective: To detect the unauthorised information information processing activities.				
A.10.10.1	Audit logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	All servers and devices are configured to forward logs to centralised log hosts. Logs are aggregated off-site and signed. All access attempts (successful and unsuccesful) are logged. Access logs will be periodically audited to identify unauthorised access.	GB
A.10.10.2	Monitoring system use	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.	Automated processes are in place which are monitored and reviewed by GB	GB
A.10.10.3	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorised access.	Log files are stored off site and are digitally signed via PGP every 24 hours.Any tampering can therefore be identified. Signatures are copied out so any changes to signatures can also be detected.	GB
A.10.10.4	Administrator and operator logs	System administrator and system operator activities shall be logged.	Access to servers is via individual user accounts authenticated using a public key. Administrators escalate privileges using sudo which logs the commands used to the system log which is then copied off-site as described above.	GB
A.10.10.5	Fault logging	Faults shall be logged, analysed, and appropriate action taken.	Development procedure applies to all fault reports. Support Tickets system is used by customers to report faults. Employees have access to bug tracker. Monitoring systems raise alerts when systems are offline	GB
A.10.10.6	Clock synchronisation	The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised with an agreed accurate time source.	Clock Synchronisation Policy in place (Wiki)	GB
A.11 Access control				
A.11.1 Business requirement for access control Objective: To control access to information.				
A.11.1	Access control policy	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.	Access Control Policy in place (Wiki)	GB
A.11.2 User access management Objective: To ensure authorised user access and to prevent unauthorised access to information systems.				

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
A.11.2.1	User registration	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	New Employee IT Request Form identifies which systems an employee requires access to. Centralised user database used to manage user accounts so when access is no longer required, accounts can be withdrawn easily. Operations staff have user accounts on servers which are managed by the Puppet configuration manager which can immediately revoke access.	GB
A.11.2.2	Privilege Management	The allocation and use of privileges shall be restricted and controlled.	Cover within access control In house system had differering level of access and for the customer base. Role base access control system in place. For customers it is documented in the operations manual.	GB
A.11.2.3	User password management	The allocation of passwords shall be controlled through a formal management process.	ZMG office is heterogeneous (Windows, Macs and Linux) and no central management is possible. Employees instructed to change their workstation passwords every 90 days. Staff Console and Vault force password change on this schedule.	GB
A.11.2.4	Review of user access rights	Management shall review users' access rights at regular intervals using a formal process.	Employee Exit Interview identifies any access privileges an employee has which are revoked upon departure. Access Control Policy (Wiki) provides for quarterly audits of access privileges	GB
A.11.3 User responsibilities Objective: To prevent unauthorised user access, and compromise or theft of information and information processing facilities.				
A.11.3.1	Password use	Users shall be required to follow good security practices in the selection and use of passwords.	Procedure documented (6.4.5) Summary sheet to be created	MB
A.11.3.2	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Procedure documented (6.4.5) Document - screen saver is a blank screen which is password protected....	MB
A.11.3.3	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Procedure documented (6.4.6) Summary sheet created	MB
A.11.4 Network access control Objective: To prevent unauthorised access to networked services.				
A.11.4.1	Policy on use of networked services.	Users shall only be provided with access to the services that they have been specifically authorised to use.	Policy on use of networked services documented	GB
A.11.4.2	User authentication for external connections	Appropriate authentication methods shall be used to control access by remote users.	Documented and referenced. conduit solution, using public/private key, deny hosts, vpn to data centre - x509 certs, wiki uses username / password.	GB
A.11.4.3	Equipment identification in networks	Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.	Documented and referenced. no mac filtering.	GB/RS

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
A.11.4.4	Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports shall be controlled.	Documented and referenced access control policy	GB
A.11.4.5	Segregation of networks	Groups of information services, users, and information systems shall be segregated on networks.	Documented and referenced. DMZ exists. flat network , no vlans, either document	GB
A.11.4.6	Network connection control	For shared networks, especially those extending across the company's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1)	Confirm whether there are no shared networks.	GB/RS
A.11.4.7	Network routing control	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	Documented and referenced. firewall , Have been documented.	GB
A.11.5 Operating system access control Objective: To prevent unauthorised access to operating systems.				
A.11.5.1	Secure log-on procedures	Access to operating systems shall be controlled by a secure log-on procedure.	Secure log-on procedures created and referenced	GB
A.11.5.2	User identification and authentication	All users shall have a unique identified (User ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.	User identification and authentication created and referenced	GB
A.11.5.3	Password management system	Systems for managing passwords shall be interactive and shall ensure quality passwords.	Password management system created and referenced	GB
A.11.5.4	Use of system utilities	The use of utility programs that might be capable of overbidding system and application controls shall be restricted and tightly controlled.	all users require access, non-technical users do not have admin rights	GB
A.11.5.5	Session time-out	Inactive sessions shall shut down after a defined period of inactivity.	Checked whether timeouts exist and document. .	GB
A.11.5.6	Limitation of connection time	Restrictions on connection times shall be used to provide additional security for high-risk applications.	No limitation, not applicable. This requirement is excluded.	GB
A.11.6 Application and information access control Objective: To prevent unauthorised access to information held in application systems.				
A.11.6.1	Information access restriction	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.	Information access restriction documented	GB
A.11.6.2	Sensitive system isolation	Sensitive systems shall have a dedicated (isolated) computing environment.	Sensitive systems documented, vault , dns sec system	GB

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
A.11.7 Mobile computing and teleworking Objective: To ensure information security when using mobile computing and teleworking facilities.				
A.11.7.1	Mobile computing and communications	A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.	Teleworking policy in place (Wiki)	GB
A.11.7.2	Teleworking	A policy, operational plans and procedures shall be developed and implemented for teleworking activities.	Teleworking documented	GB
A.12 Information systems acquisition, development and maintenance				
A.12.1 Security requirements of information systems Objective: to ensure that security is an integral part of information systems.				
A.12.1.1	Security requirements analysis and specification	Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.	Security requirements analysis and specification documented.	GB
A.12.2 Correct processing in applications Objective: To prevent errors, loss, modification or misuse of information in applications.				
A.12.2.1	Input data validation	Data input applications shall be validated to ensure that this data is correct and appropriate.	Location of documents mentioned. referenced in the coding standards document wiithin wiki..... Documented and referenced. main threat is sql injection, database abstraction layer, active record pattern, using a software library, libsenic, dbdata object, php library, main api is not , xsrf token on the main extranet.	GB
A.12.2.2	Control of internal processing	Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	Control of internal processing documented.... Documented and referenced. DNS zone files are validated and compared to previous versions to check for truncation or large unexpected changes. Backups are tested for completeness and unexpected large changes.	GB
A.12.2.3	Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.	Documented and referenced. All outbound email must have a standard signature appended. CentralNic publishes SPF records to permit source validation of email, and out mail service also checks SPF records. See Email Policy (Wiki)	GB

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
A.12.2.4	Output data validation	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	Output data validation documented, dns zones	GB
A.12.3 Cryptographic controls Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.				
A.12.3.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Referenced on Wiki.	GB
A.12.3.2	Key management	Key management shall be in place to support the organisations use of cryptographic techniques.	Key management documented, crypt to be used to handle keys.	GB
A.12.4 Security of system files Objective: To ensure the security of system files.				
A.12.4.1	Control of operational software	There shall be procedures in place to control the installation of software on operational systems.	Control of operational software documented. centos based on rpm and check/verify files on system, copy and verfiy rpm database. non-tehnical users do not have admin access cannot install software	GB
A.12.4.2	Protection of system test data	Test data shall be selected carefully, and protected and controlled.	Protection of system test data documented and captured within risk assessment. production data used in test enviornment.	GB
A.12.4.3	Access control to program source code	Access to program source code shall be restricted	Access control to program source code documented, stored in cvs repository (version control), stored on encrypted file server.	GB
A.12.5 Security in development and support processes Objective: To maintain the security of application system software and information				
A.12.5.1	Change of control procedures	The implementation of changes shall be controlled by the use of formal change control procedures.	Change of control procedures documented utilised bug tracker.....wiki - codereview process, wiki - maintenance, system change control process..., no change control for the network devices or server installs....	GB
A.12.5.2	Technical review of applications after operating system changes	When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on company operations or security.	Technical review of applications after operating system changes documented	GB
A.12.5.3	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.	Referenced software update policy, no COTS software used.	GB
A.12.5.4	Information leakage	Opportunities for information leakage shall be prevented.	Documented and referenced. software installs - pgp install checks are done Documented and referenced. software solution checks signatures when it	GB

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
			downloads software primariliy for the unix environments. Documented and referenced. software update policy updated.	
A.12.5.5	Outsourced software development	Outsourced software development shall be supervised and monitored by the organisation.	Not applicable as software development is outsourced. This requirement is scluded from scope.	GB
A.12.6 Technical vulnerability management Objective: to reduce risks resulting from exploitation of published technical vulnerabilities.				
A.13.1.1	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Security Incident Response Policy (Wiki) covers procedure for reporting and responding to security incidents. All employees are encouraged to report security incidents to IST members as appropriate (see security induction)	GB
A.13.1.2	Reporting security weaknesses	All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.	Security Incident Response Policy (Wiki) covers procedure for reporting and responding to security incidents. All employees are encouraged to report security incidents to IST members as appropriate (see security induction)	GB
A.13.2 Management of information security incidents and improvements				
A.13.2.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Handling of Non Conformities & Responding to security incidents and malfunctions (MSM 7.4)	GB/RS
A.13.2.3	Collection of evidence	Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	Process or details of which external organisation would be used when conducting forensic investigation documented. Included in the T & C. .	MB
A.14 Business continuity management				
A.14.1 Information security aspects of business continuity management Objective: 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.				
A.14.1.1	Including information security in the business continuity management process	A managed process shall be developed and maintained for the business continuity throughout the organisation that addresses the information security requirements needed for the company's business continuity.	Documented as part of Business continuity plan	GB
A.14.1.2	Business continuity and risk	Events that can cause interruptions to business processes shall	certificates / first aiders, extinguishers, fire assemby point,	GB

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
	assessment	be identified, along with the probability and impact of such interruptions and their consequences for information security.		
A.14.1.3	Developing and implementing continuity plans including information security	Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, failure of, critical business processes.	Documented as part of Business continuity plan	GB
A.14.1.4	Business continuity planning framework	A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.	Documented as part of Business continuity plan	GB
A.14.1.5	Testing, maintaining and reassessing business continuity plans	Business continuity plans shall be tested and updates regularly to ensure that they are up to date and effective.	Documented as part of Business continuity plan. annual basis do occur but not documented.	GB
A.15 Compliance				
A.15.1.1 Compliance with legal requirements Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.				
A.15.1.1	Identification of applicable legislation	All relevant statutory, regulatory and contractual requirements and the company's requirements and the company's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the company.	Identification of applicable legislation updated with new compliance section. PCI DSS may need to be added.	MB
A.15.1.2	Intellectual property rights (IPR)	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.	CentralNic maintains several policies in relation to trademarks. Dispute Resolution Procedure operated by WIPO (policy and rules on website). Takedown procedure in place for domains used in phishing and counterfeiting, etc (see website and wiki)	GB
A.15.1.3	Protection of company's records	Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual and business requirements.	Backup Policy in place to ensure CIA of backup files (see wiki). Paper records are securely stored in Moorate office.	GB
A.15.1.4	Data protection and privacy of personal information	Data protection and privacy shall be ensured as required in relevant legislation, regulations and if applicable, contractual clauses.	Documented in Staff Handbook	GB
A.15.1.5	Prevention of misuse of information processing facilities	Users shall be deterred from using information processing facilities for unauthorised purposes.	Rate limiting and automated blocking is used to limit abuse where applicable, eg the Whois service. Repeated failed login attempts causes accounts to be locked until administrator can unlock them.	GB

Requirement		ISO 27001 Control	CentralNic MSM Compliance	Review
A.15.2. Compliance with security policies and standards, and technical compliance Objective: To ensure compliance of systems with organisational security policies and standards.				
A.15.2.1	Compliance with security policies and standards	Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.	Internal audits, CB third party assessments, Blackmores compliance audits. IST members are heads of departments. IST responsibilities.	GB
A.15.2.2	Technical compliance checking	Information systems shall be regularly checked for compliance with security implementation standards.	Compliance checks identified and monitored by GB.	GB
A.15.3 Information systems audit considerations Objective: To maximise the effectiveness of and to minimise interference to/from the information systems audit process.				
A.15.3.1	Information systems audit controls	Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimise the risk of disruptions to business processes.	Audits completed. Audit plan in place for 2012.	MB
A.15.3.2	Protection of information systems audit tools	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.	Standard sys admin tools exists documented in Wiki.	GB