Table of Contents

Table of Contents 1
General Security Policies 2
General IT Security Policies 4
Access Control Policy 12
Document Classification Policy 18
ISMS Process Flow Chart 20
Network Management Policy 21
Removable Media Policy 23
Security Incident Response Policy 25
Software Update Policy 29
System Administration Policy 31
Control Of Documents And Records Procedure 32
Internal Audit Procedure 36

General Security Policies

From CentralNic Staff Wiki
Classification: Internal Use Only

Moorgate Office Keys

Various parts of the Moorgate office are secured by locked doors. This includes the server room, Robert's and Ben's offices, the comms cabinet in the kitchen and various filing cabinets around the office. Each of these areas must be kept locked when not in use.

Keys are held centrally in a locked pedestal cabinet next to Jenny's desk. If you require access to one of these cabinets, please ask either Jenny or Gavin who will issue you with the key.

Keys are given a unique ID which is recorded in a Key List held in a secure Dropbox folder (only IST team members have access to the list). This ensures that if a key is lost, it cannot be associated with a particular area without access to the list.

Some keys are issued to employees on an ongoing basis (eg Jenny and Gavin have a key to the cabinet where the other keys are stored. The Key Assignment List is used to record who has been given what keys. When an employee leaves, this list is consulted to find out what keys they need to return.

Spare keys are held in the safe.

Exchanging Information with Third Parties

Information sharing with external parties must take place within the context of information security. Third parties must be held to non-disclosure and confidentiality agreements, which must be in place before any information exchange takes place.

All suppliers of outsourced information processing services (such as accounting and financial services, legal and HR services, as well as IT service providers) must include sufficient provision for confidentiality and protection of information in their service agreements with us. An additional confidentiality addendum may be required if these provisions are insufficient.

Where we conduct discussions and negotiations with external parties with a view to forming business relationships, a standardised Mutual Non Disclosure Agreement must be used.

Current **Revision:** 1.7338
Last Updated: 2012-07-5 by Gavin

General IT Security Policies

From CentralNic Staff Wiki
Classification: Internal Use Only

Third Party Suppliers

Where we contract with third party suppliers to provide information storage, transmission or storage services, these suppliers must include provision for the security of data as part of their contracts. Third party suppliers must store, transmit and process data securely.

System Administration Policy

All servers and networked devices should be configured to be as secure as possible. Unused services and features should be disabled to reduce their attack surface. Default passwords should be immediately changed and the replacement passwords should be strong and stored securely (see the Password Policy).

All remote administrator access to servers and networked devices should be via secure channels such as SSH or an HTTPS based web interface. Where possible, remote access should be through an unprivileged account, which can escalate to administrator privileges for specific tasks: for example, servers should have the root password disabled, so administrators log in via the unprivileged "cnic" account, and then use "sudo" to perform administrative tasks.

Administrative tasks should only be performed as part of the normal change control process: that is, a bug report must be submitted, the proposed changes reviewed and tested where possible, and then deployed in the production environment.

Configuration files should be stored in CVS: for servers, updates to config files should be done using a CVS checkout, and for other devices which lack CVS clients, the changes should be made directly on the machines, after which the config fles should be copied to a local sandbox and committed.

Access to administrative interfaces should be restricted to only those employees who require access to perform their jobs.

See also: Software update policy

Password Policy

Passwords should be used to restrict access to all systems which permit their use, including:

- servers (via SSH)
- services (ie Staff Console)
- devices such as switches, routers, firewalls etc)
- Employee workstations, laptops, smartphones and tablet computers

Where systems permit, passwords for end users should be changed at least once every 90 days.

Passwords should be at least eight characters, be mixed case, contain at least one number, and where systems permit, a non-alphanumeric character such as !, #, * etc.

End-user computing devices such as workstations, laptops, smartphones and tablets should be configured to lock their screens after being idle for ten minutes.

Passwords used to manage servers and networked devices, and to access third party services, that are not associated with end users, should be securely stored. The Vault should be used to store these password and share them with the appropriate persons. Where passwords need to be stored in config files, for example to permit programmatic access to APIs, these config files should not include the passwords when in CVS (see above) but should be manually added when checked out. These passwords should be changed following the Password Update Schedule in Dropbox.

Information Access

Employees should only have access to information where it is needed to perform their job. For example, a developer may need access to source code, but a customer support representative does not.

Access to information assets should always be via secure channels, ie SSH or HTTPS, and should be logged where possible. Where systems permit, any changes to information should also be logged, in such a way as to permit rollback to the previous state (for example, "Ann edited domain example.uk.com" is unsufficient. Instead, the log message should say something like "Ann changed the expiry date of example.uk.com from 2011-01-01 to 2012-01-01").

Mobile Computing and Telecommunications Policy

Company equipment which leaves the office should always be secured to prevent tampering and intrusion, this includes setting user passwords and configuring screen lock (see the Password Policy above), as well as using encrypted filesystems to secure sensitive information. All mobile devices should also support backup, either to a local server in the office or via a "cloud" such as Dropbox or iCloud. Employees should be aware that information may be at risk of unauthorised disclosure when crossing borders, so they should take steps to minimise the amount of data they take with them when they travel.

If a mobile device is lost or stolen, this constitues a security incident and the IST should be notiified.

Teleworking

Employees may "telework" in two ways: using company owned and configured equipment, or using their own home computers, laptops and other devices.

Company owned equipment should be configured so that remote access to company assets is always via a secure channel, such as a VPN, SSH or HTTPS. As described above, this equipment should also be secured from tampering and intrusion, and configured to back up data to prevent loss from loss or theft.

Employees may use their own devices to access company services and assets. In such cases, these services and assets should be locked down so that they can only be accessed via secure channels: eg, requiring the use of STARTTLS or SSL for IMAP. Employees should be made aware that they are responsible for the security of the company's information assets and should take steps to secure their devices in the same way as company-owned equipment is secured.

Employees should avoid accessing company services using unsecured devices, such as a friend's laptop or a computer in an airport lounge or Internet cafe. If these sorts of devices are used, employees must take care to ensure that any company data is deleted, and all login sessions are terminated when finished with.

Cryptography

The company makes extensive use of cryptography, to secure communications channels and to protect data at rest.

Only well-tested and trusted cryptographic software should be used. This essentially means software distributed as part of operating systems, as well as software tools such as OpenSSL and GnuPG. "Home-brew" cryptographic software and libraries should be avoided. Well-known and known-secure algorithms such as AES and 3DES should be used.

Cryptographic Key Material

Cryptographic keys are used throughout our system. In order to provide real-time access to services and data, these keys must often be stored online and in plaintext format. When this is necessary, these keys must be secured to the extent permitted by the use to which they are put: this includes using file permissions, passphrases and Hardware Security Modules according to the level of risk.

Keys must also be backed up. Private keys must always be backed up using strong cryptographic means, so that they are not compromised if disclosed. For example, SSL private keys and certificates are stored in the Crypt, which is an encrypted loopback filesystem residing on an encrypted physical drive. Portable backups of the Crypt volume itself are also encrypted using GnuPG, so that if they are disclosed to unauthorized persons, there are three layers of encryption which must be broken before the keys can be accessed.

The Vault

The Vault is a web based system that allows the secure storage and sharing of sensitive data. It is particularly used to store company-owned credentials such as usernames and passwords.

Each user account has an SSL key pair: the private key is stored in a secure form using symmetric encryption. When the user logs in, the password they enter is used to decrypt the private key. As the HTTP protocol is stateless, the private key has to be decrypted for each request, so the password must be associated with the user. To prevent it from being stored in the clear, a random nonce is generated and the password is XOR'd against it: the nonce is stored on the server, and the XOR result in a

cookie in the user's browser. When the user next requests a page, the XOR is reversed to retrieve the password. This ensures that the password is never held in the clear on either the client or the server.

Data is stored in a relational database. Data items are both encrypted (using the public key of the intended viewer) and signed (using the private key of the author). When a user accesses a piece of data, the signature is checked using the author's public key. When a user creates a new data entry, it is separately encrypted for each intended viewer, and signed.

Certain users have administrator privileges allowing them to create new user accounts and delete or suspend existing accounts. When a new account is created, a keypair is generated and the private key is encrypted using a random temporary password which is then emailed to the user. Administrators never see the password and if the user forgets it, their account cannot be accessed.

Data Deletion

Any IT equipment that contains sensitive data (such as internal company documents, databases, passwords and cryptographic keys) must be securely wiped before being disposed of. This must be done by CentralNic personnel prior to transfer of the equipment to the disposal agent, or may be done by the disposal agent, under a Data Destruction Contract and using CESG approved methods.

Hard drives may be wiped using specialist software such as "Darik's Boot And Nuke" (DBAN, http://www.dban.org/) or by using a command such as the following:

```
[root@host @~]# dd if=/dev/urandom of=/dev/to/be/wiped BS=1M ; dd if=/dev/zero of=/dev/to/be/wiped BS=1M
```

See also: IT Equipment Waste Disposal Policy

Malware

All Windows and Macintosh systems must have antivirus software installed. This software must be configured to automatically update virus definition files on a daily basis.

Linux based systems are less susceptible to malware but are still vulnerable to worms, etc. For performance reasons Linux servers are not required to

have antivirus software running but to mitigate the risk from malware, the Software Update Policy is in place to ensure that security vulnerabilities are patched in a timely manner. All incoming mail is scanned by MessageLabs to scrub malicious attachments, phishing mails, and so on.

Internet Explorer

IE remains the most popular web browser and is a major target of malware as a result. Therefore IE must not be used unless absolutely necessary (for testing, or for sites which require ActiveX, etc). All Windows workstations must be configured to use an alternate browser (Chrome, Firefox, Safari, Opera) by default.

Network Security

To prevent unauthorised equipment from being connected to the network, all patch panels and switches are physically secured to prevent access.

The Arpwatch daemon is used to detect new devices being attached to the network, and any changes in the mapping between an Ethernet address and IP address.

All devices connected to the network must be locked down, with all default passwords replaced with strong passwords.

Access to network services must be restricted by use of firewall systems. Other security systems such as Intrusion Detection Systems (IDS), and web application firewalls may be used if appropriate. Firewalls should block access to all services, from all hosts, except those specifically permitted.

Networks should also be segregated into different subnets or VLANs where possible. A Demilitarised Zone (DMZ) may also be appropriate depending on circumstances.

Wireless (wifi) networks must be protected with secure encryption. WEP is specifically prohibited due to know vulnerabilities in the protocol.

All remote servers must be protected by on-board software firewalls. Remote administration and logging must be via secure channels (SSH, Syslog over VPN).

Where permitted, network services must support encryption:

- SSH for remote administrator access

- HTTPS instead of HTTP, with HTTP Strict Transport Security (STS) enabled globally
- SMTP over SSL on port 465 instead SMTP over port 25 (STARTTLS is not used to allow port 25 to be firewalled off)
- IMAP over SSL on port 993 instead of IMAP over port 193 (STARTTLS is used as above)
- Infrastructure domains (eg centralnic.net) are DNSSEC signed and resolvers are configured to validate
- The VPN is to be used to protect insecure protocols (eg syslog) when transmitted over the Internet

All services which expose sensitive data must be protected by authentication. This may be a simple username and password, or may take the form of strong mutual client/server authentication (ie client and server SSL certificates, as in the case of the VPN).

Access to Documentation

Documentation about the system and software in place is stored in various places:

1. on this wiki
2. inline with source code (ie PHPDoc comments in PHP code)
3. in Dropbox, either as normal documentation (ie manuals) or as functional specs, etc

In principle it should be the case that having full access to this documentation should not provide any unauthorised third party with a vector with which to attack the system. However, to increase the effort required by a third party who wishes to attack or compromise our systems, access to documentation should be restricted to those who need it to perform their jobs.

Under no circumstances should internal documentation be provided to third parties without prior authorisation from the CTO. External entities who are given access to documentation must sign non-disclosure agreements before being given access. Employees must ensure that documentation that they have access to is not available to unauthorised third parties.

Transport of Physical Media

Use of physical media to transport data assets is governed by the Removable Media Policy. Use of physical media to transmit information between two physical locations or between CentralNic and a third party should be avoided, unless the size of the data would prohibit secure electronic transmission.

In the case of extremely sensitive data such as private keys (particularly DNSSEC key signing keys for TLDs), physical media may be used to transport these keys between locations and organisations. In such cases, CentralNic personnel should accompany and be responsible for the security of the media at all times. Passwords and/or keys used to encrypt the data stored on physical media should not accompany the media but should be shared via an alternative secure channel.

During transport, a full audit trail of all persons in possession of the media should be recorded, with both parties signing the record during hand-off.

Current Revision: 1.7337

Last Updated: 2012-07-4 by Gavin

Access Control Policy

From CentralNic Staff Wiki
Classification: Internal Use Only

Introduction

The purpose of this document is to define the policies that control access to the networks and systems that power CentralNic's business operations. This policy deals with access to network equipment (switches, routers, firewalls, etc), systems and servers.

Scope

This document covers the following aspects of access control:

- Physical access control – refers to physical security restricting access to the devices and systems that power the business.
- Device and server access control – access to the management interfaces of routers, switches, firewalls servers and other devices under CentralNic's control.
- Monitoring of access – this defines the policy that controls how devices and servers are monitored.

Physical Access Control

All servers and devices are housed in physically secure facilities: either the primary operations centre at the Goswell Road Data Centre (GRDC) or the server room at the Moorgate office (ZMG).

Goswell Road Data Centre

- The GRDC site features stringent electronic security control and policies. ID proximity access cards are utilized as the first level of security beyond the 24x7 security desk. All data centres feature CCTV located at points of entry, including common areas within the technical space. CCTV is monitored centrally and remotely and the recordings are digitally archived.
- Access to the GRDC site requires prior approval by authorized senior personnel (typically the CTO or Operations Manager). Visitors to the

data centre must present government-issued forms of identification before they can be granted access.

- All racks at GRDC are physically locked on both sides and suites are configured within the technical space using de-mountable, part solid and part caged, metal partitions. Construction is floor slab to ceiling slab, to maximize security.
- All physical network infrastructure at GRDC is physically secured. Cabling is held within enclosed ducting or in ceiling-mounted cabling trays which are monitored by CCTV on a 24x7 basis by landlord security personnel. Fibre lines are housed in rigid plastic enclosures to protect accidental damage.
- Network equipment such as routers, switches and firewalls are all stored in secure locked cabinets or racks. Links to upstream transit providers also terminate in secure locked racks.
- A record is kept of all switch, router and firewall port assignments. All cables are labelled with the devices which should be connected at each end.

Moorgate Office

- The Moorgate office is located in a multi-tenant building. Access to the building is via a single front entrance which permits access to the main reception. Access to offices is via a lift or stairwell: an RFID key fob must be used to obtain access to these. Logs of key fob use are kept by the building manager. Emergency exits cannot be opened from the outside.
- the door into the office from the stairwell is locked with a PIN entry lock.
- All servers are housed in a secure server room. The door to the server room is kept locked, only authorised personnel have access to the key to unlock it. Network switches are housed in a locked comms cabinet. All cabling is secured above the ceiling, under the floor or in trunking.
- All visitors to the office must sign the Visitor's Log upon arrival, and their time of departure is also recorded. As the office is small and open plan, it is not possible for visitors to wander around unattended or unobserved, so visitor passes are not used. However employees are required to challenge any unknown persons who are present in the office.

Network Access Control

- All servers, systems and devices are protected by firewalls and ACLs applied to restrict access.
- Access to these servers, systems and devices is further protected by passwords. Where possible, access to these servers, systems, and devices is role based, depending on the type of user.
- Strong passwords are encouraged, and enforced where permitted.
- For in-house systems, passwords are never stored, instead the hash of the password and a random salt is stored and this is tested when the user logs in.
- Where software and hardware allow, only secure access methods are allowed (eg HTTPS and SSH).
- Remote access is via encrypted VPN or SSH only. VPN access is based on possession of a signed client SSL certificate. SSH access is via the Conduit SSH gateway and is authenticated via SSH key.
- Remote root access to servers is not permitted. IT department team members access the servers via regular user accounts - each employee has their own account. System administration tasks are performed by using 'sudo'. All usage of the sudo command is logged to the central log system.
- For access to the EPP system, we support validation of client SSL certificates.
- Visitors to the Moorgate office are provided with Internet access using a guest wifi network. This network is logically isolated from the internal corporate network. The guest wifi network is secured by WPA2 using a password which is published on notices in the office and which is regularly changed.

Monitoring of System Access

- Use of access cards and fobs is logged at both the GRDC and ZMG is logged by the building managers. As mentioned previously, all visitors to both sites must sign in and records are kept indefinitely.
- All servers and devices are configured to send system logs to a centralised logging host. Logs are replicated offsite and digitally signed every 24 hours. All access attempts (both successful and unsuccessful) are logged, permitting audit of access attempts.

User Policies

This section outlines policies dealing with assignment and management of users' access rights.

New Employees

On joining the company, depending on role access is granted to:

- Email and webmail
- Corporate Jabber Server
- Staff Console
- Bug Tracker
- Wiki
- CVS
- Review Board
- Conduit SSH Gateway
- Dropbox Shared Folders
- Internal mailing lists

This is determined using the New Employee IT Request Form which may be found in Dropbox.

The subset of systems and services that people are granted access to are dependent on their role within the company, and is determined by line managers.

On induction, users are educated on passwords, and, where possible the above systems enforce secure alphanumeric passwords with a minimum length and password changes and periodic intervals (90 days).

All users have their own credentials for the systems that they use, and passwords should not be shared. All workstations and laptops are protected by a 10 minute screen lock.

Leaving Employees

When an employee leaves the company, a standard Exit Interview is performed using Form EI. This form includes a checklist to confirm the return of all company property and assets, and that any access privileges (especially remote access) for the employee have been revoked.

Change of Role

Access rights granted above are subject to review, including when an employee moves within the business, their access to all of the above is reviewed, and changes are made as appropriate.

Audit

Access rights are audited on an quarterly basis by the Information Security Team as appropriate. Access is audited for all the information processing systems listed above.

Current Revision: 1.7735

Last Updated: 2013-01-16 by Gavin

Change Management Policy

From CentralNic Staff Wiki
Classification: Internal Use Only

The policy applies not only to all IT related activities, but to changes to all company systems, processes, procedures and policies, including finance, marketing, business development and business management.

1. All changes to systems, processes, policies and procedures must be recorded within the Bug Tracker which serves as the change management system.
2. Changes must be acknowledged and/or approved by the appropriate Line Manager or Department Head (which may be the CTO or CEO) before being introduced.
3. A complete specification and rationale for the change should be included in the report on the Bug Tracker.
4. All relevant personnel must be included on the report (using the Cc field) to ensure company-wide acceptance of the change.
5. Changes to source code must be tagged with the bug report number in version control.
6. All time spent on the change must be recorded using the time tracker and timesheet editor built into the Bug Tracker.

Current Revision: 1.7309

Last Updated: 2012-06-25 by Gavin

Document Classification Policy

From CentralNic Staff Wiki
Classification: Internal Use Only

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 procedure, Internal Form, Minutes
- **Commercial in confidence** – i.e. Sales proposals, client MI reports, RFP.
- **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)

Unless otherwise stated and/or protected by an authentication system, any material hosted on our websites may be considered **Publicly Available**. All other material should be considered **Internal Use Only** unless otherwise stated.

Classification of articles on this Wiki

Certain articles on this wiki have been classified. The classification is clearly displayed at the top of each article.

To set the classification of a new or existing article, using one of the followling Wikitext templates at the top of the page:

```
{{Confidential}}
{{CIC}}
{{Internal}}
```

Version Control

The wiki has built-in version control and change logs for every article, but for reasons of clarity (and to assist in organising hard copies), version control information should be included in the main body of the article. To do so, use the following wikitext template at the bottom of the page:

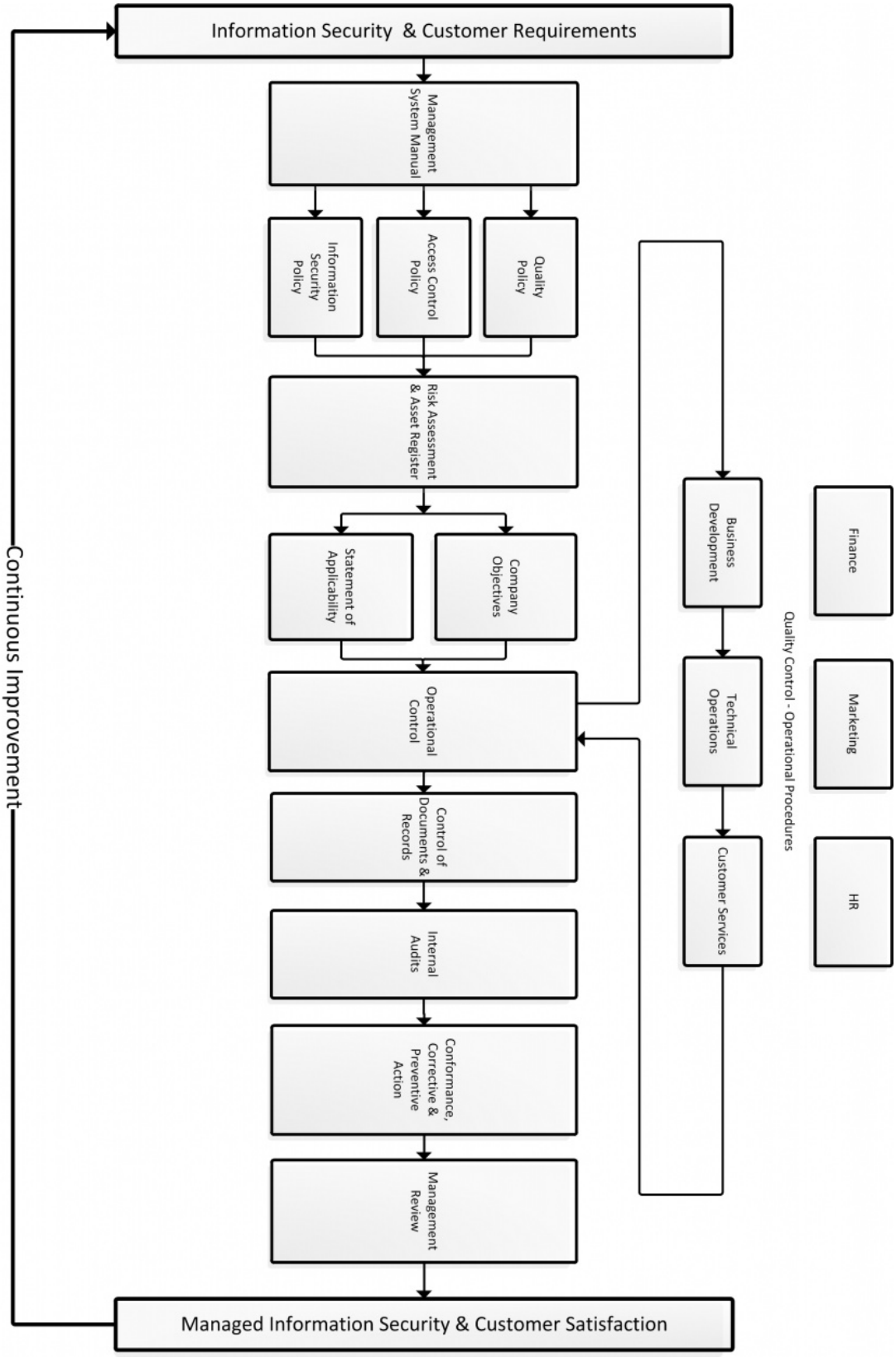
```
{{Controlled}}
```

Current Revision: 1.7296

Last Updated: 2012-06-19 by Gavin

ISMS Process Flow Chart

From CentralNic Staff Wiki
Classification: Internal Use Only



Network Management Policy

From CentralNic Staff Wiki
Classification: Internal Use Only

Introduction

This policy covers all activities related to the management of the physical and logical elements of our network infrastructure, including:

1. cabling, trunking, patch panels and sockets
2. IP address assignment and management
3. routers and switchers
4. firewall configuration

Policy

In general, the policies and procedures described in the Development Process apply to all network management activities. That is to say:

1. all changes must be in response to a requirement recorded on the Bug Tracker
2. all changes must be approved and peer reviewed before deployment
3. any potentially disruptive changes must be scheduled for out-of-hours maintenance windows in accordance with the Scheduled Maintenance Policy

Configuration Management

IP addresses should be recorded to reflect the active IPs on all devices on all networks. Any update or change on any device or any new IP install must be updated. IP address map should be stored in CVS and revised with every change.

Unlike application code, or configuration files for servers, it is generally not possible to deploy configuration updates for firewalls, routers and switches using CVS, since these devices don't have CVS clients. Instead, changes must be manually entered, via a web, telnet or SSH interface.

However, the configuration files for these devices must still be stored in CVS just like other configuration files.

Therefore, if at all possible, planned changes to devices configuration must be made to the configuration files in CVS, reviewed using the Review Board, committed against the relevant bug report, and then deployed by uploading and/or copying and pasting the updated configuration.

If this is not possible, then when changes are made to production systems, the changes must be committed to CVS immediately after the change has been made.

Configuration Enforcement

For the GRDC firewall system, a script called firewall.enforcer runs every 30 minutes and checks the live configuration of the two firewalls against the file stored in CVS. If a difference is found, an alert is raised.

Other tools for configuration enforcement (for example, for switches and routers) may be deployed in the future as needed.

Device Administration

Usernames and passwords used to manage network devices are stored in the Vault. Access is restricted to those employees who need it to perform their duties. Passwords are also subject to periodic change to ensure that they cannot be used if disclosed to unauthorised persons.

Current Revision: 1.7529

Last Updated: 2012-10-5 by Kareem

Removable Media Policy

From CentralNic Staff Wiki
Classification: Internal Use Only

Introduction

This Policy relates to the use by employees of removable media (such as USB flash drives and CD/DVD ROMs).

Removable media represent a significant threat to the security of the business. They are a significant source of malware infection and data loss in businesses.

Policy

1. Employees may only use removable media that has been approved by the CTO or other senior IT officer. Employees are not permitted to bring their own media (such as flash drives or USB keys) into the office or plug them into any company computer.

2. If an employee requires use of removable media for their work, they should submit a request to the CTO.

3. All removable media devices are held by the Operations Manager and issued to staff as required. Devices are signed for when issued and a note is taken when the device is returned.

4. All removable media devices should be returned when no longer needed.

5. Removable media issued by the company remains the property of the company and must be returned upon request or at the end of the employee's employment.

6. All removable media must clearly be labelled with "Property of CentralNic Ltd".

7. Removable media should not leave the company's premises unless it has been properly secured, that is, data on the device has been encrypted to a level commensurate with the classification of the

data upon it. Employees should contact the IT Department who can assist in installing any software necessary to achieve this.

8. If it is necessary to transport removable media containing classified company assets to another location, this media should either:

    1. remain in the possession of a CentralNic employee at all times, and/or:

    2. be transported by a reputable and authorised courier who can provide track and trace of the device.

9. Removable media from unknown sources should never be used, or should be securely wiped by IT prior to use (it is a common attack vector to install malware on USB keys and mail them out as free gifts).

10. If removable media is lost or stolen, this constitues a Security Incident, so the Security Incident Response Policy should be followed to report the loss and decide on further action to be taken.

11. Media (such as CD or DVD ROM disks) which, when no longer required, cannot be securely wiped, must not be used, or must be securely destroyed using best practices for such media (eg shredding, grinding and/or incineration).

Current Revision: 1.7340

Last Updated: 2012-07-6 by Gavin

Security Incident Response Policy

From CentralNic Staff Wiki
Classification: Internal Use Only

CentralNic operates the following Security Incident Response Policy. The policy applies to all events and incidents as defined by the policy, and to all computer systems and networks operated by CentralNic.

Computer Security Incident Response Policy

Definitions

Event: An event is an observable change to the normal behavior of a system, environment, process, workflow or person (components). There are three basic types of events:

1. 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.
2. Escalation – 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.
3. Emergency – an emergency is an event which may:
    1. impact the health or safety of human beings
    2. breach primary controls of critical systems
    3. materially affect component performance or because of impact to component systems prevent activities which protect or may affect the health or safety of individuals
    4. be deemed an emergency as a matter of policy or by declaration by the available incident coordinator

Computer security and information technology personnel must handle emergency events according to well-defined computer security incident response plan.

Incident: An incident is an event attributable to a human root cause. This distinction is particularly important when the event is the product of malicious intent to do harm. All incidents are events but many events are

not incidents. A system or application failure due to age or defect may be an emergency event but a random flaw or failure is not an incident.

Incident response team: The incident coordinator manages the response process and is responsible for assembling the team. The coordinator will ensure the team includes all the individuals necessary to properly assess the incident and make decisions regarding the proper course of action. The Incident team meets regularly to review status reports and to authorize specific remedies. The team should utilize a pre-allocated physical and virtual meeting place.

Incident investigation: The investigation seeks to determine the human perpetrator who is the root cause for the incident. Very few incidents will warrant or require an investigation. However, investigation resources like forensic tools, dirty networks, quarantine networks and consultation with law enforcement may be useful for the effective and rapid resolution of an emergency incident.

Process

Initial incident management process

1. Employee, vendor, customer, partner, device or sensor reports event to Help Desk.
2. Prior to creating the ticket, the help desk may filter the event as a false positive. Otherwise, the help desk system creates a ticket that captures the event, event source, initial event severity and event priority.
    1. The ticket system creates a unique ID for the event. IT Personnel must use the ticket to capture email, IM and other informal communication.
    2. Subsequent activities like change control, incident management reports and compliance reports must reference the ticket number.
    3. The First Responder captures additional event data and performs preliminary analysis. The First Responder determines criticality of the event. At this level, it is either a Normal or an Escalation event.
    4. Normal events do not affect critical production systems or require change controls prior to the implementation of a resolution.
    5. Events that affect critical production systems or require change controls must be escalated.

6. Organization management may request an immediate escalation without first level review – 2nd tier will create ticket.

3. The event is ready to resolve. The resource enters the resolution and the problem category into the ticket and submits the ticket for closure.
4. The ticket owner (employee, vendor, customer or partner) receives the resolution. They determine that the problem is resolved to their satisfaction or escalate the ticket.
5. The escalation report is updated to show this event and the ticket is assigned a second tier resource to investigate and respond to the event.
6. The Second Tier resource performs additional analysis and re-evaluates the criticality of the ticket. When necessary, the Second Tier resource is responsible for implementing a change control and notifying IT Management of the event.
7. Emergency Response:
    1. Events may follow the escalation chain until it is determined that an emergency response is necessary.
    2. Top-level organization management may determine that an emergency response is necessary and invoke this process directly.

Emergency Response

1. Emergency response is initiated by escalation of a security event or be direct declaration by the CTO or other executive organization staff. The CTO may assign the incident coordinator, but by default, the coordinator will be the most senior security staff member available at the time of the incident.
2. The incident coordinator assembles the incident response team. The team meets using a pre-defined conference meeting space. The CTO and/or CEO must attend each incident team meeting.
3. 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:
    1. 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.
    2. 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 (see page 1), or closed.

3. Monitor and Capture – Perform a thorough investigation with continued monitoring to detect and capture the perpetrator. This process must include notification to the following senior and professional staff:
    1. CEO and CFO
    2. Corporate Attorney and Public Relations
4. 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.
5. Repair Systems, eliminate vector of attack mitigate exploitable vulnerabilities
6. Prepare a Test Report which documents the validation of the repair process.
7. Test Systems to ensure compliance with policy and risk mitigation.
8. Perform additional repairs to resolve all current vulnerabilities.
9. 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.
10. 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.

Software Update Policy

From CentralNic Staff Wiki
Classification: Internal Use Only

Updating software packages on production systems should be a relatively safe procedure. However we have been stung too many times to trust that upstream packagers and distributers will never ship update packages without bugs. Therefore, the following policy is in place to cover when and how we do software package updates:

1. **Always update software packages when a security vulnerability is announced and an errata published.** This is especially true of network service daemons (eg bind, httpd, openssh), low-level libraries (glibc, openssl) and programming languages (php and perl). We have a designated **patch manager** (currently Alex) whose job is to monitor mailing lists for disclosures of vulnerabilities. The patch manager will co-ordinate security updates as and when required.
2. **Updates should always be tested.** Install the updated software in a sandbox environment, staging server or OT&E, and conduct tests before updating the production environment.
3. **Disruptive updates should be scheduled for maintenance windows.** If a kernel update requires a reboot, or the update requires more than a trivial amount of downtime, we should always notify registrars of a scheduled maintenance window.
4. **Always perform targeted updates.** Never perform a full system update (ie yum update) on a system in production. Instead, only update the specific package that must be updated. A full update should always be done on a machine following a fresh OS install.
    1. **This policy especially applies to systems running operating systems that do not offer long-term support** (ie Fedora, Ubuntu) and which do not guarantee API/ABI stability and backwards compatibility, and/or which use 3rd party software for which we do not have support contracts in place (ie mod_epp).
5. **Prepare a rollback plan in the case of an issue.** The yum-allowdowngrade package allows us to roll back software packages to previous versions, but it usually requires some planning to make use of. For example, you can't roll back httpd without removing all its dependencies first: you can then install the older version, but will also have to install the appropriate dependent packages. You may

also need to back up config files for packages that are removed and re-installed.

6. **Check package/release ChangeLogs before updating.** ChangeLogs may include "known issues" lists that could affect our systems. Small updates that only address a few specific versions are much more preferable to large updates that contain substantial code rewrites, API/ABI changes, etc.

Current Revision: 1.7758

Last Updated: 2013-01-23 by Gavin

System Administration Policy

From CentralNic Staff Wiki
Classification: Internal Use Only

This Policy documents CentralNic's rules and procedures for the administration and management of its servers.

Security

Servers should be hardened against all security threats. This includes the following actions which should be taken when a new server is configured:

- use of a strong root password
- disabling of all network services not required in normal operations
- configuration of remote system logs using the syslog-ng system (over the VPN if the server is located outside GRDC or ZMG)
- use of SSL/TLS to secure all network services (SMTP, HTTP, etc)
- use of SSH keys to add additional security to remote logins

Configuration Management

All configuration files should be stored in the revision control system so that they be managed. This allows us to audit changes to configuration settings and eases the deployment of configuration across multiple servers.

We have a standard Apache config which should be used to replace the default config files shipped in the RPMs.

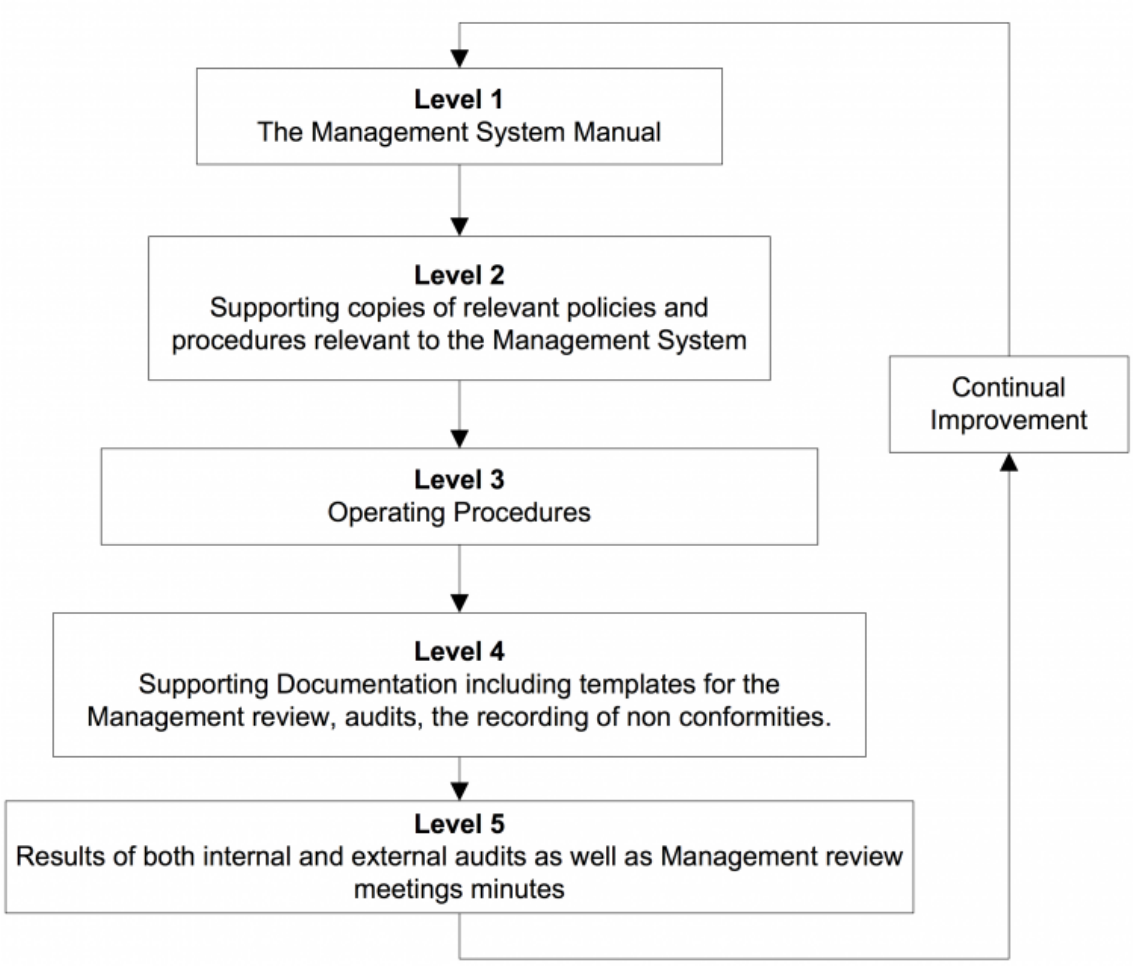
Change Control

All commits on configuration file changes should be tagged with the relevant bug report. If a change is required, a bug report should be raised to cover it. Changes to system configuration are subject to our Code Review Policy.

Control Of Documents And Records Procedure

From CentralNic Staff Wiki
Classification: Internal Use Only

The structure of the Management system documentation is detailed below:



The system is accessible by all employees electronically via the Wiki or Dropbox, or alternatively, a controlled copy can be found in the CTO's office. The CTO retains a controlled manual copy of the Management System Manual (MSM). Uncontrolled hard copies of the MSM must be suitably marked 'uncontrolled'.

Management System Manual

The purpose of this Manual is to document the policies and procedures used by Centralnic to assure the quality of its products and services conform to the international quality standard BS EN ISO 9001 and information security standard ISO 27001.

Control of Documents and Records

CentralNic has established, implemented and maintains documented procedures to control all documentation and data that relate to the company requirements, to include documents of external origin such as standards.

It is the responsibility of the CTO to ensure company documentation is maintained.

Documents and data are reviewed and approved for adequacy. These controls ensure that:

1. All documents, instructions and procedures are adequate for their intended purpose.
2. Correct documents, instructions and procedures are available at affected work locations and/or accessible to appropriate personnel.
3. Obsolete documents are promptly removed from all points of issue or use.
4. Revision levels of documents can be readily identified.

CentralNic implements and maintains documented procedures for the identification, collection, filing, storage, maintenance, retrieval and disposition of quality records.

All records are identifiable and retrievable. An inventory of records including the retention periods is held in the Control of Records Register. Management are responsible for ensuring that quality records are maintained.

The CTO is responsible for the preparation, distribution and the maintenance of the Management System. The CTO is also responsible for ensuring that the Management System editing rights are disabled on the Wiki and Dropbox.

Once an amendment has been approved the documentation will then be amended and identified within the Management System and relevant parties will be informed of the amendment.

A record of amendments is retained as part of the WIKI or Dropbox document audit trail.

Where practical, change identification is referenced by highlighting the change in 'blue'. The revision levels are assigned in numeric order, starting with "1" for the original issue and increasing by one with each revision.

Obsolete documents will be disposed of securely if the information is of a sensitive nature.

Records include internally-generated documents, client documents. A Control of Records register is maintained of which records are to be held and the retention period required. All records are controlled effectively and take into account any relevant legal requirement. The various types of records that are to be retained are reviewed annually by the CTO. The records are legible, identifiable and retrievable.

It is the responsibility of each employee to maintain and control their department records. Employees will ensure that any documents that contain sensitive information concerning internal/external customer data is stored securely. If an employee wishes to dispose of such a document, it will be dealt with as part of the in-house paper recycling process.

The Operations Director will monitor the compliance of the control of Documents and Records procedure.

For documents that are shared by different people within the company, primarily those that are edited by different people, we use Dropbox. The files shared using this system can be broadly categorised into the following:

1. Accounting information:
    1. CAPP spreadsheet
    2. Invoices issued outside of our automated billing system
2. Marketing material:
    1. Graphics and logos
    2. Promotional material (banners, flyers, leaflets)
3. Technical:
    1. Software and hardware manuals from vendors
    2. Project specifications and project plans
    3. Network diagrams

    4. Customer documentation (operations manual etc)
    5. Asset registry, server list
    6. Reference material: white papers, essays and presentations from third parties
4. Policy documents
5. Business proposals

Dropbox

Dropbox (www.dropbox.com) provide a system whereby files saved into a local "Dropbox" folder are synchronised to the Dropbox cloud server (they are encrypted in transit and at rest on Dropbox's servers). They are also automatically replicated to other computers linked to the user's account. The Dropbox service provides a version control system, allowing deleted or overwritten files to be restored. Folders within Dropbox can be shared with other users.

Shared Dropbox folders are used to provide access to company records and policies. Different folders are used to segregate material to control access: only authorised personnel have access to the IST shared folder, for example.

Wiki

The wiki is also used as a repository of policies and procedures. Most articles in the wiki are freely accessible to all users, however most policies and procedures are restricted so that only authorised users can make changes.

Protected articles may only be edited by the "Administrators" group which corresponds to IST members.

Classified and version-controlled articles are tagged using the appropriate templates, which provide visual indication of the article's classification level and/or version.

Current Revision: 1.7345

Last Updated: 2012-07-9 by Gavin

Internal Audit Procedure

From CentralNic Staff Wiki
Classification: Internal Use Only

The main objective of the Centralnic Management System is to provide a foundation on which the business can:

- Provide a consistently high level of performance to ensure client satisfaction
- Enable the business to continually review its performance and implement improvements where necessary
- Ensure effective risk management by adopting a uniform approach to project delivery.

In order to ensure that the Management System remains effective, periodic reviews of the Management System and the requirements of the business will be undertaken during internal audits. These audits will also assess the documented procedures of the Management System against the requirements of ISO 9001 and ISO 27001.

Internal Audit Programme

The CTO shall annually publish an audit programme which will cover all aspects of the business activities as the 'checking' process of the "Plan-do-check-act" improvement cycle.

The internal audits will be undertaken by the CTO or a representative from Blackmore Quality Management Services (an outsourced Management System support service).

Ownership of the internal audit programme remains with the CTO. All internal audit records shall be maintained in an electronic format for a minimum of 3 years.

Internal Audit Process

The audit process will involve recording comments and observations during planned assessments to identify best practice together with areas for

improvement. Notes will be made during the audits recording objective evidence together with positive and negative results.

These items in turn will then be recorded onto an audit report, describing the observations and stating the action to be taken to, first of all correct the situation and prevent re-occurrence. Where possible comments will also be made to indicate any foreseeable preventive action to be discussed / implemented regarding possible problems in the future.

Audit reports will be given a timescale and responsibilities for action identified. On receipt of confirmation that all points have been addressed a follow-up audit, or review, will be carried out to ensure action taken is effective, and when satisfied the report will be closed-out ready for review and analysis during the management review meetings.

The audit programme will be continually updated to show those audits carried out, future audits planned, and follow-up audits planned, and those audits still awaiting action to be addressed.

Monitoring and Measurement of Processes

The company has implemented and maintains comprehensive methods for monitoring and measuring the Management System processes, which demonstrate the ability of the processes to achieve planned results. When planned results are not achieved, corrective actions are implemented and monitored for effectiveness.

Monitoring and Measurement of Product

The company has implemented and maintains comprehensive methods for monitoring and measuring products against planned requirements.

When planned results are not achieved, corrective actions are implemented and monitored for effectiveness.

Current Revision: 1.7291

Last Updated: 2012-06-19 by Gavin