Security Policy Customer version

Document Number:	UK-Q045
Document Classification:	Claranet-Confidential
Version	4
Updated	24SEP2018
Author	Michelle Reilly

Contents

Document Control

Document Name	Security Policy – Customer version
Document Reference	UK-Q045

Date	**Version**	**Author**	**Description of change**
17JAN2014	1	Michelle Reilly	Original
01JUN2015	2	Michelle Reilly	Review and minor updates
08JUN2015	2.1	Michelle Reilly	Minor updates
24MAY2016	2.2	Michelle Reilly	Review and minor updates
23MAY2017	3	Michelle Reilly	Review and minor updates
24SEP2018	4	Michelle Reilly / Matt Flanagan	Review, GDPR updates, data retention policy updates

Disclaimer

The information that is contained in this document is the property of Claranet. The contents of the document must not be reproduced or disclosed wholly or in part or used for purposes other than that for which it is supplied without the prior written permission of Claranet Limited.

1.0 Scope

This document describes Claranet's approach to managing information security management internally and in the delivery of services to its customers. In particular, it describes the measures adopted to support Claranet's customers who are governed by regulatory requirements and industry standards such as ISO9001, ISO 27001 and the Payment Card Industry Data Security Standard (PCI-DSS).

The intended readership of this document is:

- Customers and prospects of Claranet
- External assessors when establishing a base-line for security audit purposes,
- Claranet employees and contractors, for the purposes of awareness and training.

The document explains:

- How Claranet organises its staff and processes to manage security
- How resources and assets are managed to mitigate the risks of threats and vulnerabilities

This document is a summary of Claranet's larger internal security policy and associated processes. It is not intended as a full disclosure of sensitive information management practices.

Claranet are accredited for ISO9001, ISO27001, ISO22301 and Cyber Essentials and operate an advanced integrated management system to manage these standards. Additionally all key Claranet Data Centres are accredited for PCI-DDS, physical security.

2.0 Security Policy Statement

The data held by Claranet is an extremely valuable asset. This data exists in many formats throughout the business including electronic media, hardcopy and the knowledge and experience of our staff and associates. Information is stored in a variety of locations on a variety of media and can arrive and leave the business through a variety of routes.

The Directors and Senior Management of Claranet are committed to ensuring that an appropriate system of information security management is fully implemented, maintained, and continually improved to protect this data, and that this system is subject to regular audits to ensure that it meets its objectives.

The objectives of our Information Security Management System are to ensure that this information is accessible only by appropriate persons and that its integrity and confidentiality is preserved at all times. Claranet strives to maintain business continuity and to protect both the company and its customers from all threats to the security of data.

It is our policy to ensure that we have relevant and up to data security objectives managed from a process driven approach and supported by appropriate controls, systems and resources and that we comply with all known legislation, customer specific requirements and the requirements of all standards and accreditations with which Claranet are associated.

Michel Robert, MD, Claranet UK
Charles Nasser, CEO, Claranet Group

Issue 7: September 2018

2.1 Purpose and objectives of the Security Policy

The purpose of the Policy is to protect Claranet and its customers' assets from all threats, whether internal or external, deliberate or accidental. It is the policy of Claranet to ensure that;

- All data assets will be protected against unauthorised access.
- Threats to all data assets will be assessed, controlled or mitigated.
- Confidentiality of information will be assured.
- Integrity and availability of information will be maintained.
- All specific regulatory and legislative requirements will be met.
- Business Continuity plans will be produced, maintained and tested.
- Security training is available to all staff and contractors.

The objectives of managing information security are to ensure business continuity, minimise business interruption and to protect Claranet customers by preventing and minimising the impact of security incidents.

Procedures exist to support the policy. These include risk assessment, access control, virus control, passwords, and business continuity.

- Business requirements for the mitigation of risks from threats to assets will be assessed.
- Business requirements for the availability of information and information systems will be met.
- The Head of Security & Compliance (HOSC) has direct responsibility for maintaining the Security Policy and providing advice and guidance on its implementation.
- All managers are directly responsible for implementing the Security Policy within their business areas, and for adherence by their staff.
- It is the responsibility of each member of staff to adhere to the Security Policy.

3.0 Risk Management

The data held by Claranet is an extremely valuable asset. This data exists in many formats throughout the business including electronic media hardcopy and the knowledge and experience of our staff and associates. Information is stored in a variety of locations on a variety of media and can arrive and leave the business through a variety of routes. Effective Risk Management is therefore very important.

Claranet operates a Risk Treatment Plan that describes the risk methodology in use. A fully managed risk register is used log all risks and their associated risk rating, the mitigation in place, response required and acceptance sign off criteria. This register is reviewed at least twice a year to maintain an up to date assessment of all known risks.

In deploying the Claranet Information Security Management System (ISMS), the Management Team aim to maintain existing known risks at their current low level and ensure that new and changing risks are assessed and managed in an equally consistent and professional manner.

4.0 Organisation of Information Security

4.1 The Security Team

This is a forum of representatives from across the business who have responsibility for the key business and information assets governed by Claranet's security management policy. The team is led by the Head of Security & Compliance who has overall responsibility for security at Claranet.

The team's responsibilities are to;

- Establish, document, and distribute security policies and procedures.
- Remind staff of security responsibilities.
- Monitor and analyse security alerts and information, and distribute to appropriate personnel.
- Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations
- Administer user accounts, including additions, deletions, and modifications
- Monitor and control all access to data.
- Audit the application of process and policy to ensure compliance with the security objectives of the company and relevant standards such as ISO9001 and ISO27001

4.2 Human Resources Team

The HR Department is responsible for:

- Maintaining appropriate employee policies with respect to business and information security
- Ensuring security responsibilities are conveyed in contracts of employment, job descriptions and HR policy documentation
- Security screening of employees and prospective employees, to assess their suitability for the roles they are/ will be performing
- Ensuring that all employees receive adequate security training, and that records of such training is maintained; the Director of Security and Compliance is responsible for devising and delivering Security Training
- In association with line management and the Director of Security and Compliance, to oversee any employee disciplinary processes relating to security
- Ensuring that relevant areas of the business are informed of starters, leavers and changes in employee status so that security controls (access rights, passwords and permissions) are adjusted in a timely manner.

4.3 The Data Centre Management Team

The Data Centre Management Team are responsible for the management of Claranet Data Centres including their physical security and day to day management. The team managed by the Head of Data Centres meets every four weeks to specifically address tactical and operational management issues such as;

- Oversight of DC operational and security improvement initiatives
- Operational process alignment and interoperability between data centres
- General DC resourcing, maintenance, capacity planning and other operational matters
- Compliance with prevailing standards

4.4 Claranet Employees

All Claranet employees are required to comply with the security policy and have signed an employment contract with an NDA to confirm this. Security Training is given at the start of employment and annually thereafter. Staff security responsibilities include;

- Working in a secure, legal, ethical and professional manner, in compliance with Claranet's security policy
- Reporting any suspicion of a security breach in line with the Incident Response Plan
- Managing their systems and physical access levels in a professional manner and ensuring that they are not shared or used inappropriately

5.0 Asset Management

5.1 Hardware Asset

Claranet maintains an ITIL based configuration management database of all physical assets which contains details of the product and service elements provided to each customer. This includes model numbers, serial numbers, physical location, software version and any other information relevant to the management of physical assets. In addition Claranet maintains a database of all infrastructure and IT assets which is included in a weekly patching schedule.

Processes are in place to ensure the correct decommissioning of servers, network devices and firewalls, and for the secure disposal of data storage devices. Claranet work with approved secure disposal companies to ensure that assets are effectively destroyed when they reach the end of their useful life.

5.1 Data Classification

Claranet's Data Standards Policy describes how data is classified to ensure that it is handled appropriately. The policy uses 4 classification types;

- Unclassified – this is uncontrolled data that does not need to be protected, an example of this type of data would be marketing material
- Internal – this is data that can only be shred internally amongst all employees, an example of this type of data would be sales performance information
- Restricted – this is data that can only be shared between a defined groups of employees. Confidential. An example of this type of data would be audit reports.
- Confidential – this is data shared between Claranet and its customers. Any data marked as 'confidential' should not be passed on the third parties in accordance with the non-disclosure agreements between Claranet and is customers

6.0 Human Resources Security

6.1 Organisational controls

Claranet’s organisational structure provides clear segregation of duties throughout. Claranet maintains well defined job descriptions, contractual obligations and working practices for all staff, outlining security roles and responsibilities.

Access to any of the following is only granted to those employees with a direct business need, based upon job role:

- Claranet internal systems and sensitive data
- Claranet platforms, networks and data used to manage customer services
- Claranet Customer and supplier information

Access rights are only granted with management approval, and are strictly controlled through Claranet’s Starters, Transfers and Leavers Process.

6.2 Ensuring Secure Handling of Customer Sensitive Information

Claranet’s role is to provide, connectivity, managed infrastructure and hosting facilities for the safe storage and transportation of customer’s applications and data. Claranet is not in itself an information processor of customer data and therefore does not access the informational content of any traffic passing across its networks (other than for virus and malware scanning, or for the detection of intrusion, abuse or criminal activity). Therefore customer data is not likely to be disclosed to employees through the routine management and administration of the customer’s network, except where Claranet has accepted specific responsibility for database management.

Employees and contractors are expected to treat all customer data as confidential and handle it accordingly. This includes but is not limited to customer names, contact details and account details.

As a condition of their employment all new employees at Claranet are required to sign a non-disclosure agreement and a contract of employment which includes acceptance of company policy.

Additionally Claranet has the following measures in place for new employees to ensure the safe and secure handling of customer data;

- Criminal records check
- Past employment references
- Credit history check

All of these checks must be completed before the employee is given access to company data.

- Contractors and relevant trusted third parties are required to sign a contract which includes confidentiality and non-disclosure terms.

6.3 Security Awareness and Training

Claranet maintains a high-level of security awareness within the organisation by ensuring that all employees attend security training annually. Claranet conducts regular internal auditing of employee adherence to security policies.

Employees are made aware that information security is an integral part of the day-to-day operation of company business; understand their individual responsibilities, and are aware that business and information security is important to the company and to customers. Training is enhanced throughout employment on an 'as needed' basis through periodic briefings, on-the-job training, bulletins and advisory e-mails on specific security issues. Training is reviewed annually as part of each individual's appraisal and personal development plans.

7.0 Physical and Environmental Security

Claranet has data centres located in London, Bristol, Hoddesdon, Kent and Manchester. Claranet's offices are located in London, Gloucester, Manchester, Birmingham, Leeds and Warrington. Physical controls are in place at all sites to protect Claranet's premises and provide security around customer environments.

7.1 Organisational controls

An organisational structure exists which provides clear segregation of duties in the administration of customers' hosted environments. Only those employees with a legitimate and direct business need are granted physical access to locations storing customers' systems and data.

7.2 Physical security features

A variety of features are in place to maintain physical security at Claranet Data Centre facilities and offices. The location of each site determines the external security features. Where a data centre is located off-street palisade fencing is used with access control gates. All sites have external and internal CCTV monitoring, intruder alarms and security guards. All doors have swipe card access in place. Claranet operate an ISO27001 complaint access control process which staff, customers and suppliers must adhere to gain entry to each data centre. A copy of the customer facing process can be requested from our Service Desk.

Claranet avoids unnecessarily advertising the locations of its data centres to the general public. Addresses are not published on our web sites and signage at the sites is kept to a minimum.

7.3 Environmental security features

Our data centres have been designed with a high degree of resilience to reduce or mitigate vulnerabilities to major threats. Data centres have the following in place:

- Uninterruptible Power Supply (UPS) protection from power failure, including stand-by diesel generators
- Mains filtering and stabilisation
- Fire detection and suppression
- Water/leak detection
- Air conditioning and other environmental controls

Essential elements of our infrastructure have been designed with a high degree of technical resilience and are monitored 24x7 by our network and hosting operations centres using IBM Tivoli monitoring. Claranet is able to provide similar monitoring as a service for hosted customer equipment.

8.0 Operations Management

8.1 Operational procedures and responsibilities

Claranet strives to continually improve the effectiveness and security of its internal operations, and in the way it delivers service to our customers. To support this goal Claranet are an ISO9001 and ISO27001 accredited company. Operating procedures are documented and maintained throughout the business and regularly reviewed by the internal and external auditors to ensure they remain fit for purpose.

8.2 Change Management

Claranet operate strict change control procedures. Before any significant change is made to processes or systems, the employee responsible is required to properly plan the change and seek appropriate levels of quality review and approval. Change planning takes consideration of:

- Need and justification for the change, including assessment of cost and benefit
- Assessment of risk and potential business impact
- Scheduling of the change to reflect urgency, whilst avoiding conflict with other activities or incompatibility with existing systems and processes
- Contingency plans in the unlikely event that the change results in unforeseen adverse consequences
- Quality checks by line management or peer review

Where ever possible and practical, new systems and processes and changes to existing systems and processes are verified in a separate development and test environment before being launched into production.

Changes are scheduled through the Change Management Team who meet twice per week to consider any new change requests and review the effectiveness of recently implemented changes. The Change Management Team ensure that each proposed change has been properly planned and includes test and back out plans. Where a change has an effect on service availability, this is communicated promptly and effectively to customers.

Emergency Changes are handled by an Emergency Change Process. This process will only be initiated when the change requirement is so urgent that the normal change approval timeframe presents a significant risk to Claranet or its customers.

8.3 Third Party Service Delivery Management

Claranet's Vendor Management team is responsible for ensuring that services provided to Claranet and our customers are delivered in line with service level agreements, and maintain appropriate levels of information security. Claranet conducts regular service review meetings with suppliers to monitor quality of service delivery. Root cause and corrective action is sought for any periods of service loss or impairment, particularly those that impact or threaten adherence to agreed service levels. Where appropriate, the explanation and remedies for such service impairments are explained to our customers in our Major Incident reports.

Service issues caused by 3rd party providers are monitored as a part of Claranet's incident management process to identify trends in service degradation or underperformance so that prompt corrective action can be taken. Vendors are required to provide 'Reason for Outage' (RFO) reports in the event of a service impacting major incident.

8.4 System Monitoring and Capacity Management

Claranet uses IBM Tivoli™ and other monitoring tools extensively throughout our network infrastructure, customer delivery systems and internal corporate networks to track the operational state and wellbeing of the devices used for service delivery.

Claranet has in place a Service Operations Department which includes a dedicated Monitoring Team. This team supports the services provided from data centres, and is able to respond to system and network failures. This team also addresses alerts automatically raised when pre-set capacity or performance thresholds are crossed.

System capacity and network usage are actively monitored, and growth trends are identified to ensure that services continue to run effectively, and that upgrades are planned in a timely manner.

In the event of major operational or security events, Claranet will activate a Major Service Incident Management Process which can quickly call upon the right management and technical resources to work on resolving the issue, irrespective of the time of day. Claranet maintains a rota of on-call engineering teams for this purpose.

8.5 Protection against Malicious and Mobile Code

Claranet uses a variety of incident detection and prevention tools as well and web scanning protection as a core element of our security controls. This is designed to protect from a wide range of threats to confidential information, unauthorised re-direction to inappropriate web locations, and loss of network performance. It employs multiple world leading signature scanning engines to deliver protection from the most sophisticated and targeted web based threats, including spyware, Trojans or other malware. It ensures that web requests (including web pages, images and larger files such as PDFs, or media) are free from malicious code before they reach our employees. The service also includes the latest URL filtering and DDOS protection and blocking functionality.

Claranet has installed anti-virus software on all corporate PCs and laptops. Virus signatures are kept up to date by an automated process which pushes updates to end-user devices as these become available. In addition to this, Claranet also scans its internal networks on a weekly basis to ensure that viruses and malware have not been able to enter by any other means. Regular vulnerability scanning is used to detect weaknesses in externally facing ip addresses.

Claranet has a process for monitoring logs of internally averted viruses and investigating the source of the vulnerability, to verify that acceptable usage policy is being followed.

8.6 System Back-up

Claranet performs daily backups of essential business information and software. A two-week cycle of backups is maintained, allowing data to be recovered to any point during that period. Additionally, up to 14 versions of changed files are retained, irrespective of whether these changes occurred within the last 14 days or not. Claranet retains business transaction records indefinitely in a database management system. Claranet does not provide a full archive retrieval service to customers *as standard*. Claranet is able to offer a bespoke backup service to customers who specifically request it. This is agreed between Claranet and the customer during implementation planning, and is set up accordingly by our operations team.

8.7 Network Security Management

Within Claranet's internal corporate environment, a range of network controls are in place to achieve and maintain security, some details on network security measures are considered restricted and so not listed externally. The following controls form part of those measures;

- A private corporate MPLS network connecting together Claranet's offices. This connects to the Internet via a resilient pair of firewalls, allowing outbound and inbound network traffic to be channelled and controlled
- SSL VPN connection and an MFA tool for employees requiring remote secure access to the corporate network
- DDOS detection and prevention tools
- Subscriptions to security/exploit lists
- BGP monitoring services to detect upstream changes to routing tables
- L3/L4 security firewalls around infrastructure platforms
- Regular review of firewall policies as part of normal change processes
- Microsoft Active Directory provides user authentication onto the network for access to general office applications (Word, Excel, Outlook etc). System policies are set to enforce password complexity and change intervals. Only "strong" passwords are allowed, and rules are set to prevent re-use of existing passwords

- Further user authentication is required to access Claranet's corporate business systems. Role based access rights are implemented to enforce segregation of duties and financial approval levels
- Physical and logical segregation exists between Claranet's internal corporate network and the networks Claranet uses to provide service to customers
- An employee Acceptable Usage Policy is in place to govern the use of company ICT assets. This forms part of the contractual agreement between Claranet and its employees

8.8 Multi-Protocol Label Switching (MPLS)

Claranet's core network infrastructure is fully enabled for MPLS which provides excellent traffic isolation and differentiation without substantial network overhead. This allows Claranet to create highly effective and secure virtual private networks for its customers, managed over a common infrastructure.

8.9 Data Retention

Claranet holds data about our customers in order to provide services to them and as part of our normal marketing activities. This data is retained for legitimate business purposes and disposed of when no longer required in accordance with the guidelines provided by the UK Information Commissioners Office (ICO).
The principles of the GDPR are diligently applied throughout the business. We operate a Subject Access Request (SAR) Process and a Right To Be Forgotten (RTBF) Process which can be initiated by contacting privacy@uk.clara.net.
Further information can be found in our privacy policy which is available on our website; https://www.claranet.co.uk/legal/privacy-policy.

8.10 Data Disposal

Data hosted by Claranet on behalf of customers is destroyed at the end of the contracted service term. The destruction method will depend on the storage media. Data stored on dedicated services will be deleted when the hard discs are removed from the server and wiped to military standards. Hard discs that are end of life will be quarantined and physically shredded on site by a secure disposal partner.
Data stored on private and public cloud services becomes unreadable once the cloud account is cancelled. The data is then overwritten by the storage array, effectively destroying it.
Claranet will also engage our secure disposal partner to shred and storage media used by the business including removable storage devices.
Secure confidential paper disposal bins are in place at all sites. This waste is shredded on site by a secure disposal partner. In addition, paper shredders are available in many office locations.

9.0 Information Systems Acquisition

Wherever possible and practical, Claranet implements Commercial Off-The-Shelf (COTS) applications taking advantage of out of the box ‘vanilla’ business processes, in preference to developing bespoke systems in house. Where Claranet has access to, or develops, source code, this is restricted to only those with a direct need as a part of their job function.

Claranet’s security requirements are defined during the specification of systems, and verified during evaluation and selection. Claranet maintains separate development/test and production environments to reduce the risks of damage, unauthorised access or untested changes to the live environment.

Stringent change control processes are in place to ensure that new software and functionality updates are only released onto operational systems once they have been through thorough testing and are not released into production without final validation in pre-production.

The following are assessed during the evaluation, selection and test of new systems, or enhancements to existing information systems:

- Verification that the defined security requirements have been met and that the Supplier Approval Process has been followed.
- Data entry validation checks to detect any corruption of information through processing errors or deliberate acts
- Confirmation that controls exist to ensure the authenticity and integrity of messages and reports
- Data output checks to ensure that the processing of stored information is correct and appropriate to the circumstances

Where appropriate to the level of risk, encryption is used for the protection of sensitive information during transfer and storage, taking advantage of in-built application security and encryption that comes as standard. Cryptographic keys or certificates are kept securely and protected from unauthorized disclosure or use.

10.0 Security Incident Management

Claranet has procedures in place for reporting, investigating and managing security and operational events and incidents. These are supported by a register to record events and track them to successful resolution.

There are 3 types of security incident;

- Breach in Physical security (or attempted breach)
- Breach in Network security (or attempted breach)
- Disclosure of sensitive or confidential data (accidental or deliberate)

The response to security incidents involves;

1. Discovery
2. Immediate Response
3. Preservation of Physical Evidence
4. Inform & escalate

Escalated security incidents are recorded in the security register and owned by the Security Team. The nature and severity of incidents is recorded. Each incident is assigned an owner who is responsible for managing the incident through to resolution. This includes communication with, and engaging the efforts of all relevant parties, including customers and suppliers where necessary.

An internal report is produced which includes lessons learnt, improvement opportunities and a review of controls. Where the incident has an effect on Claranet's customer base a report is made available to the customer on request through our service desk.

An analysis of incidents is performed every 6 months to identify underlying trends and to ensure that improvement opportunities identified have been acted on.

11.0 Business Continuity Management

11.1 Claranet's Approach to Business Continuity Planning

In the delivery of product and service to customers, Claranet has ensured that reasonable and practical measures are in place to provide resilience and incident management to minimise the effects of major events. We have achieved ISO22301 compliance to ensure that our Business Continuity Plan is kept up to date and regularly tested by an external party. We have a number of supporting processes that ensure the business runs efficiency during any kind of business or service interrupting event;

- Major Service Incident Process – to manage incidents where the availability of services provided via Claranet to customers are impacted.
- Security Incident Process – to manage incidents where the security of Claranet infrastructure or data has been compromised
- Business Continuity Process – to manage incidents which effect Claranet's ability to carry out day to day operations.

Claranet regularly tests its business continuity plans. Performance is monitored during these sessions and used to drive refinements to processes, tools and resilience measures.

11.2 Customer Responsibilities

Having IT solutions managed by Claranet takes away a great deal of day-to-day hassle from our customer's business. However customers remain responsible for their own business continuity planning. Using additional products and services from our standard service offering, Claranet is able to provide higher degrees of resilience and redundancy to those customers whose services are absolutely business critical.

12.0 Compliance

12.1 General Data Protection Regulation (GDPR)

Claranet complies with the GDPR and is registered with the Information Commissioners Office as an Information Processor. Training is given to all staff at the start of their employment to ensure that its implications are understood and implemented throughout the business. To comply with the principals of the act Claranet never stores hosted data outside of the EU economic area. For further information on Claranet's approach to Data Protection in line with GDPR, please refer to the Privacy Policy on our website.
https://www.claranet.co.uk/legal/privacy-policy

12.2 Right of Investigatory Powers Act (RIPA) and the CLOUD Act

The Regulation of Investigatory Powers Act 2000 (RIPA) imposes a general prohibition on the interception of communications without the consent of both the sender and recipient, unless a warrant is issued by the Secretary of State. Claranet will comply with the legal requirements of the act.

Further, the U.S. have recently passed a law called the 'Clarifying Lawful Overseas Use of Data Act' ('CLOUD Act'). The CLOUD Act is a U.S. federal law enacted as part of the Consolidated Appropriations Act, 2018 (H.R. 1625). The CLOUD Act amends the Stored Communications Act of 1986 ("SCA") to allow United States law enforcement to compel U.S. based companies, through warrants or subpoenas, to provide data they hold on their servers regardless of whether the data is stored domestically or in a foreign jurisdiction.

The CLOUD Act was only signed into law in March 2018, so, we are monitoring developments specifically for the following:

1. clarifying regulations or case law for how the law will be interpreted or enforced by the courts, or how the relevant legal test of enforcement will be applied;

2. clarification for how the CLOUD Act can or will be applied to foreign subsidiaries of U.S.-based companies, as well as U.S. subsidiaries of foreign-based companies; and

3. finally, in the wake of GDPR that came into effect in May 2018, we need clarification on whether the CLOUD Act meets or will be amended to meet the legal requirements of the EU's most comprehensive data protection law.

For now, Claranet is fully GDPR compliant and unless or until the EU and the U.S. agree a treaty with regard to the transfer of data from service providers (data controllers or processors) to U.S. investigative authorities, Claranet will continue to comply with its' obligations under the GDPR which prevent such a transfer.

12.3 ISO27001

Scope: The provision of internet services, integrated hosting, network and application managed services.

Our scope of cover means that all processes used in the development, solution design, delivery and on-going support of all of our products meets ISO27001:2013 standards. This includes the physical security of our data centres and offices.

12.4 PCI-DSS

PCIDSS physical security provider

Claranet are committed to complying with the requirements of section 9 and 12 of the PCIDSS standard. This means that our data centres meet the physical security requirements for sites storing card data and have annual reassessments conducted by a QSA to ensure those requirements are maintained. This level of compliance will assist those customers who want to engineer their own compliant solutions and store them with these data centres.

12.5 ISO9001

Scope: This system covers the provision of internet services, integrated hosting and application managed services to Customers.

Although not strictly a security standard, ISO9001 compliance ensures that a business has documented processes, clear objectives and continuous improvement plans in place across all customer affecting areas of the business. Claranet have held this accreditation since 2007 and believe it to be an integral part of our day to day business operations, providing a consistent approach to the way in which we work

12.6 ISO22301

Scope: The protection of Claranet's ability to continue and maintain hosting and network design, delivery and support of solutions throughout the customer lifecycle.

Claranet recognises the importance of business continuity management in securing the well-being and prosperity of our organisation, and thereby maintaining delivery of services to our customers. For this reason we are accredited for ISO22301, the internationally recognised standard for business continuity. Claranet is committed to ensuring it delivers an exemplary service to its customers and to maintaining a professional relationship, at all times, with its suppliers, employees and other interested parties. As part of this commitment the leadership team recognizes the importance of operating a comprehensive Business Continuity Management System (BMCS) to ensure the ability of Claranet to continue to maintain its high standards of delivery and to ensure that our services are maintained, even throughout periods of extreme business disruption.