OUTSOURCERY®
THE CLOUD EXPERTS

Data Security Policy

Issue Date: 07/07/2016

Classification: Public

Audience: Public

Version: 2.3

Document Type: Company Policy

Distribution List (if applicable): Click here to enter text.

TABLE OF CONTENTS

1. INTRODUCTION

GCI Network Solutions Ltd understands the importance of data security and makes every effort to ensure that customer data held on systems and within the data centres are fully protected.

The company recognises that the confidentiality, integrity and availability of information and data created, maintained and hosted by GCI and its customers is vital to the success of the business.

The management of GCI views these as primary responsibilities and fundamental to best business practice and as such has adopted the Information Security Management System Standard ISO27001:2013 as its means to manage and meet the following objectives:

- Comply with all applicable laws, regulations and contractual obligations including the Data Protection Act 1998.
- Implement continual improvement initiatives, including risk assessment and treatment strategies, while making the best use of its management resources to meet and improve information security system requirements.
- Communicate its Information Security objectives and its performance in achieving these objectives, throughout the Company and to interested parties.
- Maintain a security manual and procedures that provide direction and guidance on information security matters relating to employees, customers, suppliers and interested parties who come into contact with the Company's work.
- Work closely with customers, business partners and suppliers in seeking to establish Information Security Standards.
- Adopt a forward-looking view on business decisions, including the continual review of risk evaluation criteria, which may have an impact on Information Security
- Constantly strive to meet, and when possible exceed, customer and staff expectations.
- Information Security shall be considered in job descriptions and when setting staff objectives where applicable.
- Appropriate Information Security training and awareness shall be provided to all staff to ensure responsibilities, principles and practices are embedded in company culture.

2. PURPOSE

The purpose of this document is to provide information about the procedures GCI implements to ensure the security of its customers' data, software and systems and ensure transparency in complying with appropriate legislation.

This policy is in place to ensure that:

- all employees (permanent, fixed term and temporary), workers and contractors comply with the Data Protection Act 1998
- the rights of our employees, workers, customers and partners are protected
- we are open about how we store and process information
- we protect GCI and its Customers from the risks of a data breach

This policy applies to all GCI employees or any other individual or supplier working for GCI.

The GCI management team are responsible for ensuring full compliance with this policy.

3. SCOPE

This policy applies to GCI's data assets and security considerations to support the contracted services as defined in the Product Descriptions.

GCI's data assets include but are not limited to:

- Intellectual Property owned by GCI or provided by a third party
- Financial information relating to our employees, clients or other third parties
- Other public and non-public data or information assets deemed the property of GCI

4. DATA PROTECTION ACT 1998

4.1. The Data Protection Act regulates the use of "personal data". Policies and processes will be put in place, and staff made aware of their responsibility, to ensure that data is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

4.2. For the purposes of the Act, data means information which is:

- being processed by means of equipment operating automatically in response to instructions given for that purpose
- recorded with the intention that it should be processed by means of such equipment
- recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system

4.3. For the purposes of the Act, personal data means data which relate to a living individual who can be identified from those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. Personal data includes any expression of opinion about the individual and any indication of the intentions of any person in respect of the individual.

4.4. For the purposes of the Act, sensitive personal data means personal data consisting of information as to the data subject's:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- membership of a trade union
- physical or mental health or condition
- sexual life
- the commission or alleged commission by him of any offence
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of proceedings or the sentence of any court in such proceedings

The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data.

4.5. Potential data protection risks include, but are not limited to:

- **Breaches of confidentiality** i.e. information being given out to or taken by individuals who are not authorised and/or have no requirement to have the information
- **Misuse of stored data** i.e. use of customer details for marketing where this hasn't been made clear to the customer
- **Inaccurate data** i.e. failing to update customer details, which could result in billing or contractual information being sent to the wrong address
- **Reputational damage** resulting from any of the above

5. Business Data

It is GCI's responsibility to ensure that reasonable steps are taken to maximise the integrity of business data. It is the responsibility of all employees and workers that the following steps are taken to ensure the accuracy of all data:

- Avoid duplication of data and storage in multiple locations / systems
- Confirm customer and partner details when speaking to them
- Ensure it is a simple and transparent process for customers and partners to update their details
- Update information as soon as discrepancies are identified

All Data used within the course of business processes is subject to regular risk assessment and the Company's Information Classification Policy, which stipulates the use, storage and destruction of all data assets according to recognised commercial and public sector standards and legislation.

6. Customer Authentication

All employees and workers should verify who they are speaking to by asking a number of qualifying questions prior to providing any information or answering any questions to avoid any potential data protection breaches. If in doubt, no information should be provided. Details of appropriate questions to authenticate users can be found in local procedures.

Particular care needs to be paid to any requests for specific usage or financial data. Please ensure this is sent directly to an address specific to the business and secured according to the Information Classification Policy.

7. Physical Security

GCI's data centre facilities are diversely located within the UK and connected by secure, resilient high speed back-up links. Our data centres incorporate industry standard security controls, covering physical perimeter, CCTV and monitoring, room and rack access. These controls are supported by industry recognised certifications, such as ISO 27001 and ISO 22301. Unaccompanied access to data centre facilities is not permitted, and is detailed in the Data Centre Security Policy and Access Control Policy.

8. Logical Access Control

Access to GCI's internal systems, hosting platform and customer servers is permitted for authorised personnel only. All persons must be positively identified by providing a secure User ID and password before being given access to system resources.

All servers, routers, firewalls and network equipment are protected by password access controls. All passwords are randomly generated for optimum security to prevent intruders gaining unauthorised access to systems and data.

Only GCI's Engineers have full access to the hosted platforms, each engineer having their own individual login for optimum security. Authorised support staff have Admin access to hosted services in order to provide technical support to customers. Where Engineers require access to GCI's network and systems remotely via VPN, advanced RSA security is implemented providing two factor authentication.

9. NETWORK SECURITY

The data centres all have secure back-up links for network redundancy and security, and multiple internet breakouts across redundant and geographically disparate networks using BGP peering.

Within our data centre facilities, fully layered networks are implemented with no single point of failure, designed with n+1 redundancy for bandwidth, multiple network paths, DDOS mitigation, and separated networks for traffic types and Quality of Service (where applicable). RSA authentication is implemented to control access to GCI's network and systems remotely via secure VPN. Dedicated private connections or cross connections are also supported, for those customers wanting complete separation, enhanced security and/or Quality of Service.

All laptops used by GCI staff to connect into the network are encrypted using Bitlocker, which prevents release of the contents in the event of loss or theft.

Access to the Cloud Management Network is securely controlled and restricted within GCI engineering teams. This environment and the hosting network is routinely tested for vulnerabilities, using internal tools and a formal IT Health Check (ITHC).

Resilient firewall pairs protect the hosted platforms from the outside world and application load balancers manage fail over between primary and secondary services on both sites. Resilient edge firewalls are used for email security, consisting of an integrated hardware and software solution that provides complete email protection. Firewalls, internet connections, and production networks are all pro-actively monitored with the network designed without any single points of failure. All customer solutions hosted within GCI's data centres are protected by either a shared or virtual dedicated firewall. Monitoring and alerting is performed 24x7x365 via the GCI Network Operations Centre (NOC).

10. SOFTWARE SECURITY

GCI's Engineers are responsible for all software security updates on our hosting platforms. For customers with dedicated solutions, Engineers manage the availability and control of security updates released to customers.

In addition, GCI operates a strict software security policy throughout the organisation to provide increased security across the network; this is governed by an IT Code of Conduct. All software loaded onto GCI's IT systems must be legally purchased and licensed and authorisation to install programmes is limited to members of the internal IT Department. Any executable file launched on GCI's infrastructure must have its suitability verified by GCI's IT Department prior to rollout.

11. Disposing of Removable Media and Data

Where removable hardware or storage media requires disposal, all data is wiped from the device in advance using a CESG approved programme. Where a hardware component becomes faulty within a customer's server and it is necessary to return the hardware to a third party supplier or manufacturer, this is done via trusted support partners.

Disks that are not accessible through normal disk mounting processes will be securely destroyed or degaussed by an approved third party. Certificates of destruction are provided as evidence of secure and ethical destruction. Disks under warranty are replaced by the suppler only after the data removal process has been carried out.

Following the termination of a customer's service, after 30 days of being in a decommissioned state the virtual machine and related data are removed. This includes data from storage device and configuration from compute and network devices.

12. Auditing and Monitoring

GCI implements Border Gateway Protocol (BGP) for network routing based on path, network policies and rule sets. In the event of an issue being identified, an escalation process is in place whereby engineers are alerted by Service Request. Upon completion of the remedial work and resolution of the fault, the Service Request is closed. Where necessary, a Service Request will be escalated to the Head of Infrastructure and, for major incidents, the Chief Operating Officer.

13. Contingency Planning

GCI operates and tests its Business Continuity and Disaster Recovery procedures. A full disaster recovery plan is in place across multiple geographic locations for complete network redundancy and data security. This plan is built in line with guidelines and best practice derived from ISO 22301 – Business Continuity Management. GCI's Business Continuity Policy is available on request.

In addition, GCI reserves the right to restrict, suspend or terminate any aspect of a customer's service if it is believed that the use of the service constitutes a security threat to GCI or any other users on the hosted platforms or GCI network.

14. Personnel Screening

All candidates employed by GCI are subject to Baseline Personnel Security Standard checks. As part of this process, all references are followed up for new employees and security training is included within both the induction training programme and also ongoing. GCI implements an internal IT Code of Conduct that all employees must adhere to so as to ensure security and integrity of software, systems, hardware and data, in line with the requirements of ISO 27001:2013.

15. Competency

Line Managers are responsible for identifying key competencies required for a role and ensuring these are reviewed a minimum of annually and within recruitment and in-post development interviews. GCI is a Microsoft Gold Partner and has employees that have achieved various Microsoft competencies and certifications.

16. Providing Information Following a Formal Request

All formal written requests for information under the Data Protection Act 1998 should be forwarded to the Information Security & Compliance Manager immediately. Employees should not seek to complete these requests themselves.

Law enforcement agencies do not need the consent of the data subject to obtain information. Any requests of this nature must be passed to the Information Security & Compliance Manager immediately. The Information Security & Compliance Manager will take steps to ensure that the request is legitimate prior to providing the requested information, clarifying with GCI's legal advisor if required.

17. Raising a Security Concern

GCI continues to review and develop its security policies, processes and procedures on an ongoing basis in order to both maintain and improve these levels, in line with GCI's ISO 27001 certification.

Should an employee, customer or partner believe that their information has been misused or that the Group is failing to ensure its security, they should contact the Information Security & Compliance Manager immediately at the below address:

Any suspected breaches or incidents should be reported immediately via security@outsourcery.co.uk, the postal address below or via the internal GCI Security Incident Process.