

Information Security Management System Policy



Issue Date: 08/07/2016

Classification: Public

Audience: Public

Version: 5.1

Document Type: Company Policy

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

1. DOCUMENT PURPOSE

GCI's Business Vision is to be the leading provider of cloud services based on Microsoft technologies outside Microsoft, delivering to customers with high quality cloud-based IT solutions.

The Company's strategic objectives are to:

- Develop and maintain market leading cloud based services that have key USPs in the UK and international market.
- Develop thought leadership and technology guidance to customers and partners moving to the cloud.
- Be the Cloud Service Provider of choice for Hybrid cloud deployments spanning public, private and on-premises.
- Empower customers and partners of all types to adopt Cloud on their terms: Small, Medium or Enterprise, public or private sector.
- Ensure an exceptional level of experience when adopting Cloud during service delivery and in life support.

The Company's integrated management system provides the business with a clear strategic and operational framework to enable it to achieve the above objectives through a culture of continuous improvement. The key management policies and processes within the framework are formulated in line with the ISO standards listed below, relevant legislation and industry best practice with a view to ensure all implications and interested parties are addressed.

- Quality Management System Standard ISO 9001:2008
- Information Security Standard ISO 27001:2013
- Environmental Standard ISO 14001:2004
- Business Continuity Standard ISO 22301:2012
- Service Management Standard ISO 20000-1:2011

The Company's Information Security Management System aims to:

- Promote a relationship of trust and credibility with the business community by ensuring process and products comply with governance legislation and seek continual improvement to match and exceed industry best practice.
- Ensure that all assets including data, utilised pursuant to the Company's business objectives are secured to and/or processed appropriately as deemed by the Company's risk assessment and specific 3rd party or legislative requirements including the Data Protection Act, during normal and abnormal operations.
- Ensure changes in risk, legislation or interested parties' requirements are reflected in procedures and practices across the business alongside a commitment to continual improvement and alignment to industry best practice.

2. IMPLEMENTATION

The approval and effective implementation of this policy is the responsibility of the GCI Board, represented by Chief Operating Officer, with accountability delegated to the Head of Business Operations with the support of the Information Security Forum.

The Information Security Forum is made up of employees with appropriate responsibilities for maintaining and managing the key areas of the Management System, and has the collective responsibility for operational objectives in line with this policy and reviewing performance against these objectives and other security related trends to identify improvement opportunities.

The Forum is also responsible for communication and the awareness of information security implications and processes within the organisation and externally to interested parties as appropriate and identifying changes for escalation to the Executive Management Team.

Interested parties include but not exclusively:

- Customers – current and prospective
- Employees
- Suppliers
- Shareholders & Financial Institutions
- Local community and government to operating locations
- The wider Business IT Market and influencers
- Legislative and relevant Public Sector Bodies
- The general public interest

3. SCOPE & STATEMENT OF APPLICABILITY

The scope of this policy includes all significant aspects of the business operations supporting the former Outsourcery Products and Platforms including relevant third parties.

The Statement of Applicability details the relevant control objectives in accordance to ISO27001:2013 Annex A. A copy is available internally and on application.

Management Reviews of the Integrated Management System take place a minimum of annually to ensure the business context, scope and relevant interested parties are captured and reflected within the strategic objectives. This Policy and the Statement of Applicability will be reviewed at this time or following changes to the organisation, activities undertaken, services provided and any other change that materially alters the risks and controls required as deemed by the Information Security Forum.