OUTSOURCERY®
THE CLOUD EXPERTS

Business Continuity Management System Policy

Issue Date: 08/07/2016

Classification: Public

Audience: Public

Version: 3.1

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 Business Continuity Management System aims to:

- Promote a relationship of confidence in the Company's ability to **react and recover** from a business impacting event with the business community, employees and shareholders.
- Ensure that all assets including data are available as required and according to contracts and service definitions, during normal and abnormal operations.
- Ensure that all plans supporting business continuity and disaster recovery are tested for current suitability and are continuously evolving.

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 Business Continuity Management (BCM) Forum.

The BCM 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 business continuity related trends to identify improvement opportunities.

The Forum is also responsible for communication and the awareness of business continuity implications and processes within the organisation and externally to interested parties as appropriate and identifying changes for escalation to the GCI 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

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

4. IMPLEMENTATION OF BUSINESS CONTINUITY MANAGEMENT

Functional Managers will identify key services together with their supporting assets, physical, human resource, process, information or system and maintain a risk analysis in-line with the Risk Assessment Procedure.

Each asset or asset group has a nominated owner who, in association with the Information Security Management Systems Forum, will:

- Support and maintain the Risk Assessments for their asset.
- Put risk mitigation activities in place to reduce the impact of disruption on key services and assets.
- Ensure a Business Continuity Plan is developed, implemented and maintained for any High Risk asset (s).
- Ensure the plan is periodically tested, recorded and report results to the Business Continuity Management Forum.
- Provide professional support to improve resilience of critical activities and resources that support key services.

The recovery of Customer Services is be governed by:

- Service Descriptions
- Related Disaster Recovery Plans as appropriate

5. BUSINESS CONTINUITY PLAN

The Business Continuity Plan(s) define the conditions for activating the plan, how situations are assessed and by whom.

All Business Continuity Plan(s) identify affected Services and related assets and the nominated owner tasked with activating the plans in that area to consider and cover as necessary:

- Emergency actions to be taken immediately after an incident occurred.
- Fall back procedure to be implemented to move essential business activities or support services to alternative systems/locations as necessary.
- Temporary operational procedures to follow pending completion of recovery and restoration.
- Resumption procedure to return to normal business operating procedures.
- Communications Plan for Internal and External Stakeholders defaulting to the Major Incident process as appropriate.
- Schedule for testing and updating the plan.
- Training and awareness requirements so that employees understand relevant plans and their impact on its effectiveness.
- Allocation of responsibilities, including alternate people in absence of named individuals.

All Business Continuity Plans will ensure, where possible, that information is controlled in line with the Information Classification Policy. Where, due to the nature of the event, this cannot occur a Security Incident will be raised and any interested 3rd Party notified of the breach.