VIRTUS BUSINESS CONTINUITY POLICY

Business Continuity Management (BCM) is concerned with improving the resilience of VIRTUS Data Centres. This means developing our ability to detect, plan, prevent, minimise and where necessary effectively manage the impact of disruptive events. During and in the aftermath of an incident, it will enable service delivery activities to continue and in the longer term it will expedite a return to "business as usual".

VIRTUS Data Centres aims to develop, implement, maintain and resource a BCM System that will enable us to respond to and manage any disruptions that occur. The BCM System has the following key objectives:

- To raise the profile of Business Continuity within VIRTUS Data Centres. This includes staff awareness & training arrangements and to make them aware of their roles and responsibilities detailed in Business Continuity Plans
- To identify urgent or priority (time critical) activities at our data centres and develop suitable business continuity arrangements for them
- To itemise Business Continuity in the VIRTUS Risk Management System in an attempt to identify all risks requiring a Business Continuity Plan
- To establish defined structures to plan for and respond to incidents
- To have an ongoing routine of review, audits and exercises (testing) to further enhance the BCM System
- To design, develop and critique the BCM System for continual improvement, with reference to best practice such as BS EN ISO22301:2014 *Societal Security - Business Continuity Management Systems - Requirements* and BS EN ISO22313:2014 *Societal Security – Business Continuity Management Systems – Guidance*
- To embed Business Continuity into the culture of the Company so it becomes an integral part of decision making
- To communicate our BCM System and work with all key service providers ensuring that the BCM System holistically addresses the entirety of VIRTUS Data Centres' services
- To satisfy and support the requirements of business continuity planning and disaster recovery elements/conditions found in supporting international standards such as BS EN ISO9001:2015 *Quality Management Systems*, BS EN ISO14001:2015 *Environmental Management Systems*, ISO/IEC27001:2022 *Information Security Management Systems* and ISO/IEC20000-1:2018 *Information Technology – Service Management – Part 1: Service Management System Requirements*.

Scope:

This policy applies across the group companies at our head office and all live data centres and all departments within the group companies. This policy should be communicated to key service providers engaged by VIRTUS who fall within scope of the BCM System and/or who have a responsibility under the holistic assurance provided by the BCM System.

Responsibilities:

The company is responsible for maintaining the BCM System, communicating the requirements and ensuring adherence to its protocols. This is achieved through designating specific roles and responsibilities in related manuals, such as the VIRTUS Operations Manual and individual roles and responsibilities detailed in exclusive Business Continuity Plans.

During the review of and exercising Business Continuity Plans VIRTUS Senior Operational Staff will ensure that all involved parties will be engaged to produce the most accurate and credible way of managing disruptive events/incidences. The includes the participation of the Facilities Management Company.

The VIRTUS Data Centre Managers, their support staff and the communication channels managed by the VIRTUS Service Management Centre will be responsible for enacting Business Continuity Plans for the effective control of disruptive events/incidences.

The VIRTUS Risk Manager with input from VIRTUS Operations Staff will regularly identify, register, evaluate and treat (tolerate or mitigate) all risks requiring Business Continuity Plans. VIRTUS Operations staff will be made aware of any emerging physical or technical security threats that may require BCM improvements.

The BCM System is mainly focused on the continuation of VIRTUS' service delivery. Termed '*Critical Data Centre Facilities'* our data centres perform the task of provision of power, cooling, security and connectivity to customers populating our data halls. Customer-owned IT Infrastructure remains the responsibility of the customer and therefore is resolved through customer specific BCM. A priority activity is one that would impact the reputation of the company or would seriously impact the provision of power & cooling, security & safety and connectivity of customer's equipment positioned in our data centres if it was not delivered or resumed within a defined period.

This Policy will be available at all sites and offices and to the general public via the company website. This Policy will be reviewed on an annual basis by the management team or sooner if required. This policy will be communicated to involved parties who have a responsibility to maintain, provide services and perform testing/assessments to ensure the continuation of VIRTUS' service delivery.