Business Continuity Policy

Introduction

This Business Continuity Policy outlines how Interr Limited will implement an effective business continuity management system that is aligned to the international standard – BS EN ISO 22301:2019 and BS EN ISO 27001:2017. Interr is required to maintain plans to ensure the company can continue to deliver its critical services and respond to emergencies in the event of a disruption to its normal business processes.

This policy also supports the implementation of sub-control objectives of Business Continuity: Information Security Continuity, and Information Security Aspects of Business Continuity Management. This will also ensure that our reputation with our clients is maintained through confidentiality, integrity and availability; and management will ensure business, legal, regulatory requirements and contractual security obligations are taken into account.

Interr defines a business continuity incident as:
"An event or occurrence that disrupts, or might disrupt, an organisation's normal service delivery, below acceptable predefined levels, where special arrangements are required to be implemented until services can return to an acceptable level. This could be a surge in demand requiring resources to be temporarily redeployed."

Business Continuity Management (BCM) is a process that seeks to ensure that there is minimal disruption to critical services, information assets and core business in the event of a major interruption / breakdown / incident and assists departments to reinstate normal services as quickly as possible. Business continuity (BC) is a key component of resilience, and all Interr departments have been asked to align their business continuity arrangements with the requirements this policy and the company's Business Continuity Plan.

Scope

Due to the integration and complexity of the Interr Limited, the business continuity management system is required to cover the entire organisation to ensure all interdependencies can function in times of disruption.

Therefore, this policy shall apply to all Interr services and departments delivering services on behalf of Interr. This policy applies to all employees of and those delivering services on behalf of Interr.

In order to ensure the organisation meets its corporate and business continuity, the services deemed as critical are defined within Appendix A.

The scope of this standard is also limited to the IT infrastructure, and the data and applications of the Interr's IT environment.

The internal and external interdependencies of these services require all other areas to have robust business continuity plans to ensure the critical functions of Interr are maintained at times of disruption irrelevant of cause.

As part of the business continuity management system, each department will ensure they have reviewed and assessed their stakeholders and interested party's needs, such as, but not limited to communications and supply chain.

Purpose

Strategic Aim

The aim of this policy is to establish a business continuity management system that enables Interr to be a resilient organisation, capable of providing excellent service, and supporting our clients and staff, whenever required.

Objectives

Interr will take all reasonably practicable measures to ensure the continuation of its critical services during any period of service disruption.

Interr will conduct a business impact analysis in order to determine and prioritise its critical services. Interr will determine strategies for mitigating the impact of specific risks and threats. Interr will maintain plans detailing business continuity arrangements. Interr will ensure plan validity and staff competency through continual review, training and exercising. Interr will collate incident and near miss reports, to identify lessons which can be learned from service disruptions.

Definitions

Business Continuity (BC)
Strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.

Business Continuity Management (BCM)
Holistic management process that identifies potential threats to an organisation and the impacts on business operations that those threats, if realised. It provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and values.

Business Continuity Management Lifecycle
Series of business continuity activities which collectively cover all aspects and phases of the business continuity management programme.

Business Continuity Management Programme
Ongoing management and governance process supported by top management and appropriately resourced to ensure the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products and services through training, exercising maintenance and review.

Business Continuity Plan (BCP)
Documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical activities at an acceptable predefined level.

Business Impact Analysis (BIA)
Process of analysing business functions and the effect that a business disruption might have upon them.

Critical Activities
Those activities which have to be performed in order to deliver the key products and services which enable an organisation to meet its most important time sensitive objectives.

Disruption
Event, whether anticipated (e.g. Flooding or severe storm) or unanticipated (e.g. fire or loss of power), which causes an unplanned, negative deviation from the expected delivery of products or services according to the organisation's objectives. More recently we have seen Corona Virus cause significant disruption impacting on staff and service delivery.

Maximum Tolerable Period of Disruption (MTPD)
Duration after which organisation's viability will be irrevocably threatened if product and service delivery cannot be resumed.

Recovery Time Objective (RTO)
Target time set for resumption of product, service or activity delivery after an incident.

Roles and Responsibilities

The Chief Executive Officer will:
Ensure that the Executive receives regular reports, at least annually, regarding emergency preparedness, including reports on exercises, training and testing undertaken by the organisation. Designate Interr Leadership to be responsible for emergency preparedness on behalf of the organisation – the Accountable Emergency Officers. Ensure an appropriate level of priority is given to emergency management and business continuity in all strategic planning.

Accountable Emergency Officers (AEOs)
The Accountable Emergency Officers have overall responsibility for ensuring effective business continuity management within business unit/department. The Accountable Emergency Officer will be consulted when analysing the Business Impact Analysis (BIA) results to determine priorities for protection and recovery. The Accountable Emergency Officer will take lead on promoting a culture of business continuity within the each business unit/department.

Policy Detail / Course of Action

The processes laid down in this section are to be followed to develop and approve Business Continuity Plans for individual service areas and departments within Interr.

Departmental Business Continuity Arrangements
Interr will ensure that business continuity arrangements are in place for all departments, however it remains the responsibility of the AEOs that plans are developed and approved, maintained and reviewed. The CEO will ensure that there is available full guidance and support as required.

Interr's business continuity plan template must be completed by the departments. The template will lead the plan owner in a step by step logical order through the process, including identification of critical business activities, a business impact analysis, (including maximum tolerable periods of disruption, recovery time objectives), resource requirements, strategies for restoration of critical business activities, roles and responsibilities and escalation processes.

Department business continuity arrangements (plans) must take into account key risks, including for staff shortage, loss of utilities, denial of access, loss of facilities, and IT systems / telecom outage.
Department managers should also consider other risks unique to their services and activities when developing their business continuity arrangements.

Departmental business continuity arrangements must cover all activities identified as critical to Interr. The arrangements should however cover all activities undertaken by the department.

Completed business continuity arrangements (plans) should be forwarded to the CEO for review and assessment. Once reviewed and any necessary changes suggested, the plans should be signed off and made available to all department staff.

Departmental business continuity arrangements must be reviewed every twelve months or after significant organisational change.

Incident Management

Incidents resulting in a low level impact / disruption to normal service delivery should be managed locally within the affected department, by a supervisor, team leader or manager. If additional support is required, the supervisor, team leader or manager should contact their head of department. Most low level impact incidents will be managed using existing procedures and normal working practice.

Incidents resulting in a moderate level impact / disruption to normal service delivery should also be managed locally, but with an enhanced level of support from the senior leadership within that department. Most moderate level

impact incidents will be managed using existing procedures, but there is the potential to require changes in working practice.

Incidents resulting in a significant, severe or critical level impact level / disruption to normal service delivery should be managed by the AEOs (silver commanders), and reported immediately to the CEO (gold commander).

The CEO will assess the incident and determine whether Executive involvement is required based on Interr's Incident Response Plan.

Incident Logging and Document Management

All incidents resulting in an adverse impact to Interr's services must be appropriately documented.
Leadership responsible for maintaining or recovering a service during a disruptive event must ensure that their decisions are recorded.

All documents produced by Interr related to business continuity management, and in particular those in relation to a disruptive event, must be be stored, handled, and processed appropriately.

All documents relating to a business continuity incident / disruptive event must be submitted to the CEO via the HR & Compliance Director, for audit and storage. These documents will be retained indefinitely.

Documents relating to business continuity management, and in particular those relating to a disruptive event, must not be released to any third party without consultation with the CEO.

Stand Down

Stand down will be a co-ordinated approach when returning to "business as usual". This co-ordination will be carried out through the Operations Control Centre and the AEOs or the CEO.

This approach:

Could be progressive and to predefined levels in response to a reduction in the impact of ongoing disruption

Should take into account all related departments and stakeholders and their ability to meet their requirements.

Should take into account the information provided in the completed situation report (as located in the BC Plan Template) to determine priorities, timescales, resources and staffing required to return to business as usual.

Reporting Service Disruption and Business Continuity Incidents

All incidents resulting in an adverse impact to Interr's services must be reported as soon as reasonably practicable (no later than 24 hours after the onset of the incident) to the CEO via the Director of HR & Compliance.

The relevant AEO for the affected department must also be notified of the incident.

The HR & Compliance Director, or effected the AEO in the absence of the CEO, will notify Interr's Executive of the incident, and provide regular updates as required.

Any incident not resulting in an adverse impact to the Interr's services, but that is considered to be a 'near miss', must also be reported to the Director of HR & Compliance and Department AEOs.

Leadership must inform the AEOs, and they the CEO of all incidents, so that the media can be handled appropriately, in line with current Interr policy.

Interr should always aim to proactively, rather than reactively, engage with clients, the media and the public regarding serious disruptions to service.

Investigation of Service Disruptions and Business Continuity Incidents

Any incident that adversely impacts on service delivery, no matter how minor, must be properly investigated.

A 'hot debrief' must be undertaken by the incident manager, AEO or the CEO where appropriate, immediately after the resolution of the disruption. This applies to all incidents resulting in an adverse impact to Interr's services.

All incidents that significantly impact on Interr's services will require a formal debrief of those involved. This may be conducted by the CEO, and an external SME may be contracted to support.

The CEO, or the HR & Compliance Director, or AEO acting on their behalf, will investigate the cause of the service disruption, determine the level of impact, and review the actions taken to manage the disruption to assess and take corrective action if necessary to ensure continual improvement in the Business Continuity Management Systems.

All Interr employees are required to provide reasonable assistance during the course of the investigation including, but not limited to, the timely release of information relating to the incident and the resulting business impact.

The information gathered during the investigation will be combined with the outcome of the incident debrief(s), and a report produced for the CEO and Executive. This report should include recommendations of where action could be taken to mitigate future disruptions and improve overall resilience.

The Accountable Emergency Officer, in conjunction with the CEO and Executive where appropriate, will consider the incident report and determine any points which should be actioned to improve resilience.

Information security aspects of business continuity management

The five sub controls in this policy are designed to reduce the impact and likelihood of the information security threats.

Planning information security continuity

The organisation's business areas must identify and agree the criticality of its IT services with its Interr's IT service providers.

Implementing information security continuity

The organisation's business areas must establish, document implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

Information and Data Transfer Resilience

The organisation shall have alternative networks, communications bearers and transmission paths for its critical sites and services.

Verify, review and evaluate information security continuity

The organisation's business areas shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. This will happen through planned business continuity tests and unscheduled events.

Lessons learned

Major and significant incidents must include root cause analysis to ensure appropriate remediating action is taken to protect against future incidents and improve security measures.

Training and Exercising

It is important that staff fully understand the need for Business Continuity Management, as well as their role in response to any invocation.

Interr's AEOs, together with the HR & Compliance Director and CEO, will develop and deliver an initial training programme which meets the needs of the Business Continuity Management and members of staff with operational roles in our Business Continuity Plan.

Interr's AEOs, together with the HR & Compliance Director, will make all Business Continuity Management Policies and Plans available for all relevant staff to view.

Interr's AEOs, together with the HR & Compliance Director and CEO, will ensure that the lessons learned from exercises are implemented throughout the organisation.

Monitoring Compliance and Effectiveness

Monitoring of the programme will be via the CEO and Executive, with overall responsibility held by the CEO.
Business continuity will be a standing item on the agenda of the above group, with an update report delivered by the CEO.
Reviews and lessons learned from any incidents where Business Continuity Plans have been invoked will be monitored by the CEO and Executive, via the HR & Compliance Director

The table below outlines the policy compliance measures that will be monitored.

Compliance Measure	Assessed by	Timescale
Business Impact Analysis to be completed for all service areas	CEO	Annual
Recovery time / point objectives set for all activities	CEO	Annual
Business continuity arrangements in place for all service areas	CEO	Annual
Hard copy business continuity plans accessible at all working locations	HR & Comp Dir	Annual
Departments are undertaking tests / exercises of their business continuity arrangements.	HR & Comp Dir	Annual
Reporting to executive	CEO	Annual
Departments are reporting business continuity incidents / service disruptions	HR & Comp Dir	Six Monthly
Internal Audit of Business Continuity Arrangements aligning to the requirements	HR & Comp Dir	Annual

Policy Review and Assessment

This policy may be amended by Interr at any time in order to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.

Mick Tabori - CEO
July 2022