1. Purpose

1.1. The purpose of this policy is to establish:

1.1.1. The individuals and teams with responsibility for preparing the organization to recover from disruption.
1.1.2. The minimum requirements for departments, divisions and countries to be adequately prepared to respond and recover from disruptions to their operations.
1.1.3. Steps departments, divisions and countries must take to improve their level of preparedness, in order to minimize the negative impact of disruptions to operations.

This policy is **applicable** globally.

2. Change History

Rev. #	Date	Author	Revision History
1.0	11/19/2015	Mark Armour	Policy Development
1.1	02/02/2017	Mark Armour	Updated all sections and changed to new template
1.2	02/03/2017	Mark Armour	Updated to reflect current program approach
1.3	02/06/2017	Mark Armour	Minor verbiage updates
1.4	7/12/2017	Mark Armour	Expanded Roles definition and addition of Technology Recovery and Response Management
1.6	8/10/2017	Mark Armour	Updated TR policy for Cloud solutions
1.7	8/21/2017	Mark Armour	Addition of Third Party Section (6.5)
1.8	10/2/2017	Rob Hess	Legal Dept review / input
1.8.1	10/27/2017	Mark Armour	Minor verbiage changes to Section 6
1.8.2	12/5/2018	Mark Armour	Changed dates only
1.9	8/29/2019	Mark Armour	Updated with more concise verbiage and requirements

3. References

3.1. Principles: see **GITP-001 Global IT Policy Manual Principles** document (version 1.0).

3.2. Definitions: see **GITP-002 Global IT Policy Definitions** document (version 1.1).

3.3. Compliance: All employees, contractors and consultants are required to comply with this policy. An employee found to have violated any Brink's policy may be subject to disciplinary action, up to and including termination of employment. If a

contractor violates a Brink's policy, Brink's may pursue its remedies under the contract, including without limitation, termination of the contract. Management should seek guidance from Human Resources and the Legal Department on these issues.

4. Authorization

This policy is authorized by:

_____

Mark Armour
Director, Global Business Continuity
Brink's, Incorporated

Policy Owner: Mark Armour, Director Global Business Continuity.

5. Roles and Responsibilities

5.1. Global Business Continuity:

5.1.1. This function is led by the Business Continuity Director and is responsible for enterprise level Business Continuity (BC), Technology Recovery (TR), and Response Management (RM) functions. This includes:

5.1.1.1. Developing and maintaining the policies and procedures necessary to support and execute BC, TR and RM activities.

5.1.1.2. Developing and maintaining tools, resources and templates to facilitate BC, TR and RM activities.

5.1.1.3. Providing guidance and support to departments, divisions and countries in the execution of their BC, TR and RM programs and activities.

5.2. Country Level Leadership:

5.2.1. This includes both the country General Manager and the local IT Leader.

5.2.2. Overall responsibility for compliance with Global Business Continuity Policies, including the designation of individuals to carry out and manage related activities.

5.3. Department / Branch level management:

5.3.1. While not assigned a specific role within BC, TR or RM, Department and Branch managers are responsible for understanding the program requirements, particularly the structure in place to facilitate response and recovery efforts following a disruption. These individuals are also responsible for the execution of such individual preparedness activities as may be assigned to them. This group may also have a defined role / authority in responding to disruptive events.

5.4. Employees:

5.4.1. Brink's employees are responsible for maintaining awareness of applicable BC, TR, and RM policies and procedures, following the direction of management and leadership with regards to preparedness activities and initiatives.

5.5. The below Roles are assigned by Country Level Leadership. Responsibilities for each role may be assigned to separate individuals or to a single owner. Individuals assigned separate Roles will work cooperatively to ensure that planning and response activities can be performed without duplication of efforts or unnecessary complexity.

5.5.1. Individuals assigned these roles will provide status and metrics to the Global Business Continuity Team for periodic reporting to leadership.

5.5.1.1. Annual reporting of country and service-level Business Continuity metrics will be made available to Brink's board of directors.

5.6. Country Level Business Continuity (BC) Owner:

5.6.1. This is delegated by Country Level Leadership and is responsible for the oversight of all BC related activities within their country.
5.6.2. Ensures compliance with Global BC Policies, applicable country-level regulations and contractual obligations.

5.7. Country Level Technology Recovery (TR) Owner:

5.7.1. This is delegated by Country Level Leadership and is responsible for the oversight of all TR related activities within their country.
5.7.2. Ensures TR strategies and activities conform to Global BC Policies, country-level regulations and contractual obligations.

5.8. Country Level Response Manager:

5.8.1. This is delegated by Country Level Leadership and is responsible for managing country level response to disruptive events and significant threats. This includes:

5.8.2. Defining and continually improving the process for the reporting and escalation of issues and incidents that impact or could threaten Brink's ability to deliver services or meet its contractual obligations.

5.8.3. Facilitation of the response and communications process following disruptive events and threats.

6. Policy Statement

6.1. Approach:

6.1.1. Brink's takes a LEAN based approach to Business Continuity (BC). The focus of all activities should be to improve the organization's ability to effectively respond and recover from any disruptive event. This starts with measuring the current state and identifying where improvements can be made to A) shorten response and recovery timeframes; B) reduce the cost of executing recovery strategies; or C) to increase capacity or functionality available in the post-event environment.

6.2. Capabilities Assessment:

6.2.1. The Capabilities Assessment replaces the Business Impact Analysis and Risk Assessment and should be conducted quarterly for each service performed within a country. The purpose of this document is to:

6.2.1.1. Provide transparency and a realistic understanding of the organization's ability to effectively recover from a loss or disruption.

6.2.1.2. Enable country and enterprise level leadership with the ability to make informed decisions about how and where resources should be applied in order to improve recoverability.

6.2.1.3. Ensure that the proper expectations exist should disruptions or losses occur.

6.2.2. Capabilities are communicated to leadership via a report that defines:

6.2.2.1. Workspace, staff, IT resources and third parties needed to conduct business and deliver products and services to customers.

6.2.2.2. The ability to continue services in the event of a serious loss associated with each dependency (workspace, staff, IT resources and third parties).

6.2.2.3. Service-level recoverability based on three factors needed to effectively respond and recover from such a loss. These are:

6.2.2.3.1. Resources: these are tools, equipment, materials and systems

6.2.2.3.2. Procedures: the processes and steps followed

6.2.2.3.3. Competencies: the skills, training and awareness needed by individuals to properly utilize defined resources or execute procedures effectively.

6.2.3. The results of the Capabilities Assessment Process are used to identify opportunities for improvement. Improvements can be made in any one or a combination of factors:

6.2.3.1. Acquisition or expansion of available resources

6.2.3.2. Creation or improvement of processes and / or procedures

6.2.3.3. Development / improvement of individual and team competencies

6.2.4. Prioritization of improvement activities is the responsibility of leadership with input and guidance from the Business Continuity Team. Factors that drive the prioritization of efforts include:

6.2.4.1.1. Operational or service recovery capabilities at risk due to commitments or requirements associated with the applicable service(s).

6.2.4.1.2. Cost and effort of remediation

6.2.4.1.3. Anticipated improvements in recovery time and / or capacity or functionality.

6.2.5. Upon review and approval of defined improvement initiatives, actions must be assigned to an owner. The Global Business Continuity Team tracks and reports progress to leadership, while providing support and assistance to the responsible team(s) or individual(s).

6.3. Exercises

6.3.1. Periodic exercises shall be conducted to ensure teams with responsibility for response and recovery are adequately trained / skilled in the execution of the responsibility and to validate / confirm any requirements, constraints or assumptions associated with recovery of the resource or service. Specifically, exercises should be used to satisfy any or all of the following objectives:

6.3.1.1. Improve the skills and competencies among individuals with roles in the Response and Recovery Processes.
6.3.1.2. Measure / validate the time needed to execute response and / or recovery activities.
6.3.1.3. Measure / validate the capacity of the recovery environment to handle normal production volumes.
6.3.1.4. Measure the functionality of the recovery environment, including identification of any lost capabilities.
6.3.1.5. Measure / validate the effort of executing recovery strategies (personnel needed, man-hours, support services, etc.).
6.3.1.6. Measure / validate the direct and indirect costs of executing recovery strategies.

6.3.2. At a minimum, all exercises must include all staff and resources necessary to fully execute the defined recovery strategy.
6.3.3. Where possible, exercises must provide opportunities to involve affected audiences in validation routines. This includes:

6.3.3.1. Internal businesses / departments
6.3.3.2. Clients / customers
6.3.3.3. External support partners (service providers, contractors and consultants)
6.3.3.4. External services (emergency responders, utility providers, competitors, etc.)

6.3.4. For any exercise performed, a summary report must be completed that includes:

6.3.4.1. The objectives defined for the exercise (ideally from the list under section 6.3.1)
6.3.4.2. A list of exercise participants, by role.

6.3.4.3. Resources and activities within scope.

6.3.4.4. Identification of issues encountered and any opportunities to further improve

6.3.4.5. Any applicable measurements, such as

6.3.4.5.1. The time needed to execute recovery strategies / procedures.

6.3.4.5.2. The capacity / functionality of the recovery environment as compared to production.

6.3.4.5.3. The cost and / or effort (i.e. work hours, # of participants, etc.)

6.3.4.5.4. Any constraints or risks associated with execution of the recovery strategy (required resources, tools or access, specific user skills / expertise, etc.).

6.3.5. Events that necessitate assembly of the Incident Response Team AND execution of at least one defined recovery strategy may be substituted for a scheduled Exercise as evidence of recovery capability. In all such cases, the response and recovery must be documented and a report completed that covers exercise requirements listed above.

6.4. Technology Recovery (TR)

6.4.1. TR defines the means by which technology resources can be restored in the event of some kind of loss or disruption that impacts the ability to deliver systems and applications to the customer / end-user. Any strategy for the recovery or technology resources must:

6.4.1.1. Include a means to ensure delivery of the system or application to the customer / end user from the recovery environment

6.4.1.2. Include a strategy for the recovery of the delivery mechanism itself (i.e. network or connectivity redundancy)

6.4.1.3. NOT be at risk of being disrupted by the same threat(s) as the production technology environment

6.4.1.4. Be robust enough to sustain full production operations in the event of execution.

6.4.1.5. Be sufficiently tested to ensure confidence that the strategy will be effective if executed in response to an actual event.

6.4.2. The following specifications are a requirement for all new TR projects. Exceptions to this policy must be formally approved by Country Level Leadership. TR environments in place at the time this policy was adopted will be exempted for a period of 2 years, after which, they must conform to this policy or be granted an exemption by Country Level Leadership.

6.4.2.1. Production environments that are hosted on premise using Brink's managed infrastructure must use a TR environment that is geographically diverse and not subject to the same risks and threats as the production data center. Specifically:

6.4.2.1.1. Utility services, such as electrical power, water and natural gas, provided to the TR environment must be delivered from a different source (provider, sub-station, reservoir, etc.) than the production environment.

6.4.2.1.2. The TR environment must not be subject to the same weather-related threats as the production environment. This includes risks of flooding, wind damage (such as from tornadoes or tropical systems), wildfires, as well as issues arising from winter weather threats like snow and ice.

6.4.2.2. TR for Cloud-based production environments must also conform to the above and include robust controls sufficient to eliminate any risks, (such as data corruption or WAN connectivity) that can affect both production and TR environments. Otherwise, the DR strategy must utilize a different solution, such as on premise, or a different cloud carrier for the TR environment.

6.4.2.3. All constraints associated with the execution of the TR strategy must be documented and approved by the business owner. This includes:

6.4.2.3.1. The time needed to successfully execute the strategy.

6.4.2.3.2. The maximum amount of potential data loss resulting from unavailability of the production environment.

6.4.2.3.3. Any direct costs associated with the execution of the strategy.

6.4.2.3.4. Any variances in capacity or functionality between the production and TR environments.

6.4.2.3.5. Resource requirements, such as access and permissions, skills, or training required on the part of individuals and teams needed to execute the strategy.

6.4.2.3.6. At a minimum, each system-level TR environment must execute its recovery strategy annually and the above constraints updated to reflect the actual results.

6.5. Third Party Recovery

6.5.1. The following is required for any vendor agreements that involve the outsourcing of services, particularly those that are essential for the delivery of services to Brink's customers:

6.5.1.1. Business Continuity and / or Technology Recovery requirements must be defined within the third party contract / service agreement.

6.5.1.2. The language must specify the requirements of the vendor's program and detail any actions or deliverables needed to ensure conformity to Brink's BC standards and customer commitments.

6.5.1.3. A process must be in place to review the vendor's evidence of compliance with the above contractual requirements.

6.5.1.4. In the absence of contractual requirements and proper vendor management routines, strategies for the resumption or restoration of services must be developed in the event of a disruption of the third party, including:

6.5.1.4.1. Recovery of services by Brink's

6.5.1.4.2. Movement of services to another third party

6.5.1.4.3. Strategies to continue operations in the absence of the service

7. Appendices

7.1. Not Applicable