1. Purpose and Scope

The policy provides the basic boundaries for more detailed procedures and standards. In the event of a conflict between these policies and applicable law, applicable law will take precedent.

This policy applies globally to all Brink's employees, contractors, and vendors doing business on behalf of Brink's, and all legal entities and business processes.

The objective of Business Resilience at Brink's is to improve the organization's ability to deal effectively with disruptive events. This objective is achieved by:

- Measuring current capabilities to identify opportunities for improvement
- Making informed decisions about how and where to improve
- Using exercises and events as opportunities to practice and improve

The scope of this policy is to establish:

1.1. The individuals and teams with responsibility for preparing the organization to recover from disruption.

1.2. The minimum requirements for departments, divisions, and countries to be adequately prepared to respond and recover from disruptions to their operations.

1.3. Steps departments, divisions and countries must take to improve their level of preparedness, to minimize the negative impact of disruptions to operations.

2. Policy Statement

2.1. Approach:

2.1.1. The focus of Business Resilience activities is 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.

2.2. Capabilities Assessment:

2.2.1. Capabilities Assessments must be conducted periodically for each service performed within a country. The purpose of this process is to:

2.2.1.1. Provide transparency and a realistic understanding of the organization's ability to effectively recover from a loss or disruption.
2.2.1.2. Enable leaders to make informed decisions about how and where resources should be applied to improve capability.
2.2.1.3. Ensure that proper expectations exist should disruptions or losses occur.

2.2.2. Capability Assessments define the ability to continue service(s) in the event of a serious loss of workspace, workforce, equipment, technology resources or third parties. This is determined based on three components:

2.2.2.1. Resources: people, tools, equipment, materials, and systems
2.2.2.2. Strategies: plan, method or procedures for responding to losses and / or continuing services following a loss.
2.2.2.3. Competencies: the skills, training and awareness needed by individuals to respond to the event and execute strategies.

2.2.3. Improvements to capabilities can be made in any one or a combination of ways, including:

2.2.3.1. Acquisition, expansion or accessibility of available resources
2.2.3.2. Creation or improvement of strategies
2.2.3.3. Development / improvement of individual and team competencies
2.2.3.4. Delegation of specific authority / responsibility to enable rapid response

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

2.2.4.1. Risks related to commitments or requirements associated with the applicable service(s).
2.2.4.2. Cost and effort of remediation.
2.2.4.3. Anticipated improvements in recovery time, capacity, functionality, or a combination.

2.2.5. Upon review and approval of defined improvement initiatives, the Global Business Resilience Team will track and report progress to leadership, while providing support and assistance to the responsible team(s) or individual(s).

2.3. Exercises

2.3.1. Periodic exercises shall be conducted to:

2.3.1.1. Practice and validate strategies and procedures.
2.3.1.2. Improve the skills and competencies of individuals with a role in Response and Recovery.
2.3.1.3. Measure capabilities and identify opportunities to improve.

2.3.2. At a minimum, exercises must include the staff and resources necessary to fully execute the defined recovery strategy.

2.3.3. Where possible, exercises must provide opportunities to involve affected audiences in validation routines, including:

2.3.3.1. Internal businesses / departments
2.3.3.2. Clients / customers
2.3.3.3. External support partners (service providers, contractors, and consultants)
2.3.3.4. External services (emergency responders, utility providers, competitors, etc.)

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

2.3.4.1. Exercise participants, by role.
2.3.4.2. Resources and activities within scope.
2.3.4.3. Identification of issues encountered and any opportunities to further improve.

2.3.4.4. Capabilities measured and opportunities for improvement.
2.3.4.5. Any applicable risks, constraints or assumptions identified.

2.3.5. Events that necessitate assembly of the Incident Response Team and / or execution of at least one defined recovery strategy may be substituted for a scheduled exercise as evidence of recovery capability. The response and recovery must be documented, and a report completed that conforms to the exercise requirements listed above.

2.4. Third-Party Recovery Capability

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

2.4.1.1. Business Resilience (BR) and / or Technology Recovery requirements must be defined within the third-party contract / service agreement.
2.4.1.2. The language must specify the requirements of the vendor's program and detail any actions or deliverables needed to ensure conformity to Brink's BR standards and customer commitments.
2.4.1.3. A process must be in place to review the vendor's evidence of compliance with the above contractual requirements.
2.4.1.4. 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:

2.4.1.4.1. Recovery of services
2.4.1.4.2. Movement of services to another third-party
2.4.1.4.3. Strategies to continue operations in the absence of the service
2.4.1.4.4. Any combination of the above

3. Roles and Responsibilities

3.1. Compliance: All employees, contractors and consultants are required to comply with the policies. 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 or vendor 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 HR and the Legal Department on these issues.

3.2. Global Business Resilience:

3.2.1. This function is led by the Global Business Resilience Team and is responsible for enterprise level Business Resilience (BR) and Response Management (RM) functions. This includes:

3.2.1.1. Developing and maintaining the policies and procedures necessary to support and execute BR and RM activities.
3.2.1.2. Developing and maintaining tools, resources, and templates to facilitate BR and RM activities.
3.2.1.3. Providing guidance and support to departments, divisions, and countries in the execution of their BR, Technology Recovery (TR) and RM programs and activities.

3.3. Country Level Leadership:

3.3.1. This includes both the country General Manager and the local IT Leader.
3.3.2. Overall responsibility for compliance with Global Business Resilience Policies, including the designation of individuals to carry out and manage related activities.

3.4. Department / Branch Level Management:

3.4.1. While not assigned a specific role within BR 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 individual preparedness activities as may be assigned to them. This group may also have a defined role as well as designated authority to respond to events that affect their department, branch, or service(s).

3.5. Employees:

3.5.1. Brink's employees are responsible for maintaining awareness of applicable BR and RM policies and procedures as well as following the direction of management and leadership with regards to preparedness activities and initiatives or when events affect their ability to deliver services.

3.6. 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.

Individuals assigned these roles will provide status and capabilities assessment to the Global Business Resilience Team for periodic reporting to leadership.

Periodic reporting of country and service-level Business Resilience metrics will be made available to Brink's Board of Directors.

3.6.1. Country Level Business Resilience (BR) Owner:

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

3.6.2. Country Level Response Manager:

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

3.6.2.1.1. Defining and continually improving the process for the reporting and escalation of issues and incidents that could impact or threaten Brink's ability to deliver services or meet its contractual obligations.
3.6.2.1.2. Facilitation of the response and communications process following disruptive events and threats.

4. References

4.1. Principles: see GITP-001 Global Technology Policy Manual Principles document.

4.2. Related: GITP-010 Global Technology Recovery Policy

5. Definitions

5.1. Not applicable

6. Authorization

This policy is authorized by:

James Holley
Vice President, Chief Information Security Officer

Policy Owner: Mark Armour, Sr. Director, Business Resilience

Additional Stakeholders: Mary Hamre, Global Business Resilience Manager

7. Change History

Revision	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	07/12/2017	Mark Armour	Expanded Roles definition and addition of Technology Recovery and Response Management
1.6	08/10/2017	Mark Armour	Updated TR policy for Cloud solutions
1.7	08/21/2017	Mark Armour	Addition of Third Party Section (6.5)
1.8	10/02/2017	Rob Hess	Legal Dept. review / input
1.8.1	10/27/2017	Mark Armour	Minor verbiage changes to Section 6
1.8.2	12/05/2018	Mark Armour	Changed dates only
1.9	08/29/2019	Mark Armour	Updated with more concise verbiage and requirements
2.0	03/23/2021	Mark Armour	Removed Technology / Disaster Recovery specific details
2.1	01/21/2022	Vanessa Gonzalez	Review

2.2	08/08/2022	Carrie Rogers	Updated to current template and review
2.3	8/10/2022	Vanessa Gonzalez	Review
3.0	8/25/2022	Carrie Rogers	Minor updates to template, policy name change and review
3.0	10/21/2022	Mark Armour	Review and update
3.0	11/10/2022	Vanessa Gonzalez	Review
3.0	12/08/2022	Jeff Gibson	Review
3.0	12/14/2022	Greg Osgood	Review
3.0	12/16/2022	Mark Armour	Update to Purpose and Scope
3.0	12/22/2022	Kristina Keller	Legal review and feedback
4.0	6/18/2024	Mark Armour and Global Business Resilience Team	Review and Updates
4.0	10/24/2024	Carrie Rogers	Review and Cleanup of policy
4.0	10/29/2024	James Holley	Review and Approval