BRINKS

Global Technology Recovery Policy

Document Classification: Internal Use Only

Policy No: GITP-010

Version: 1.3

Last Publish Date:
11/13/2024

1. Purpose and Scope

The purpose of this policy is to document the basic principles and policies that are fundamental to Brink's Global Technology in accordance with industry best practices. The policy assists in the following:

- Assuring a secure and stable technology environment,
- Managing and decreasing the risk of exposure and compromise,
- Protecting and maintaining the confidentiality, integrity, and availability of digital information and related infrastructure assets.

Additionally, the policies provide 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 scope of this policy is to establish:

1.1. The objectives and scope of technology recovery (TR) activities.

1.2. The minimum requirements for departments, divisions and countries to be adequately prepared to restore technology services.

1.3. The individuals and teams with responsibility for ensuring the ability to restore technology services

2. Policy Statement

2.1. Definition, Objectives and Scope:

2.1.1. The **Definition** of Technology Recovery is the ability to restore technology services in the event of a loss of the Production Environment

2.1.2. The **Objective** of the Technology Recovery function is to improve – through the development and testing of strategies – the ability to deliver technology services in the event of a loss of, or lack of access to, the production environment.

2.1.3. The **Scope** of Technology Recovery efforts is restricted to enabling and improving the ability to restore technology services from a loss affecting the ability to run from the production environment. This scope <u>Does</u> <u>Not</u> include:

2.1.3.1. The strategies and capabilities necessary to recover from application level losses and outages.

2.1.3.2. The strategies and capabilities used to recover from component level (i.e. hardware, server, database, etc.) losses.

2.1.3.3. The strategies and capabilities to restore local network or network access.

2.1.3.4. The means by which systems are recovered due to a loss or corruption of data.

2.2. **Recovery Strategies** are the means by which technology services are restored in the event of a loss of the production environment / location. Such strategies must ensure the restoration of 3 chief components necessary for the delivery of technology services: 1) the **Physical Environment**, 2) the **Data**, and 3) the **Delivery Mechanism**.

2.2.1. The **physical environment** includes the hardware needed as well as any environmental components necessary (i.e. electricity, cooling, connectivity, etc.) to run the technology service(s). Dedicated recovery environments must be geographically diverse and not subject to the same risks and threats as the production environment. Specifically:

2.2.1.1. 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.
2.2.1.2. 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.

2.2.2. The **Logical / Data** component. For recovery strategies to be viable, data must be made available from a source other than the production environment. The logical component of TR must provide for the means to run the technology service itself as well as the data being managed by the application.

2.2.3. The **Delivery Mechanism**. Recovery strategies must also include the means by which the technology service is delivered to the end user. This must account for how it is accessed in the alternate physical environment.

2.3. **Constraints** associated with the execution of the TR strategy must be identified by the business owner. Constraints are defined by customer obligations, regulatory requirements, corporate policies as well as any standards that may exist to which the business must conform to. Constraints include:

2.3.1. Time commitments, such as contractual obligations with regards to recovery objectives or service downtime.
2.3.2. The maximum amount of potential **Data** loss that can be incurred as a result of the unavailability of the production environment.
2.3.3. Performance / capacity requirements for the ongoing delivery and usage of technology systems.
2.3.4. Functions or functionality required of technology systems.
2.3.5. The direct **Costs** associated with the execution of the recovery strategy. This may also include penalties that may be incurred should strategies not be adequate to satisfy customer or regulatory mandates.
2.3.6. Human Resource requirements, such as access and permissions, skills, or training required on the part of individuals and teams needed to execute the strategy.

2.4. Recovery Strategies must be **Tested** upon implementation of any new technology service and at least annually thereafter. The purpose of such testing is to:

2.4.1. Validate the ability of defined recovery strategies – and Brink's investment in such strategies – to deliver technology services in the event of a loss of the production environment.
2.4.2. Set expectations among business owners for the restoration and delivery of technology services following a loss of the production environment.
2.4.3. Build competence in the execution of such strategies by responsible teams and individuals.
2.4.4. Identify gaps that may exist between the recovery environment and any identified constraints.

2.4.5. Identify opportunities for improvement of the recovery environment, the execution of recovery strategies or the competence of individuals and teams in the execution of recovery strategies.

2.5. The results of each recovery test must be clearly documented and disseminated to responsible parties and made available to leadership. Such **Recovery Test plan and Summary Reports** must include the following:

2.5.1. The specific technology systems and services validated as part of the recovery test activity.
2.5.2. The means by which the functionality and performance of the recovery environment was validated (i.e. execution of production work, QA test scripts, other).
2.5.3. Individuals and teams with responsibility for the execution of the strategy and / or validation of the recovery environment.
2.5.4. Conformity to constraints, including identification of any constraints not met.
2.5.5. Learning and improvement opportunities identified.

2.6. The ability to restore technology services is defined as the **Recovery Capability**. Business leaders must be informed of the Recovery Capability that exists for technology services that support their operations and the delivery of business services. This must be communicated at least once annually. Capabilities are determined based on:

2.6.1. The type and reliability of the defined recovery strategy.
2.6.2. The availability of tools needed to execute the strategy.
2.6.3. The time elapsed since the last test of the recovery strategy.
2.6.4. The number of outstanding issues encountered that affected the outcome of any past recovery test objectives.
2.6.5. The competence of the individual(s) and / or team(s) with responsibility for the execution of the strategy.

2.7. Exceptions to the above policy must follow the Global IT policy exception process and procedures.

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 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 Shared Services:

3.2.1. This function is led by the Sr. Director, Global IT and is responsible for enterprise Technology Recovery. This includes:

3.2.1.1. Developing and maintaining the policies and procedures necessary to support and execute TR activities.

3.2.1.2. Developing and maintaining tools, resources and templates to facilitate TR activities.
3.2.1.3. Providing guidance and support to departments, divisions and countries in the execution of their TR programs and activities.
3.2.1.4. For Production Environments that are managed by Global IT Shared Services, this also includes:

3.2.1.4.1. Quarterly reporting of Technology Service Recovery Capabilities.
3.2.1.4.2. Coordinate and facilitation of recovery testing.
3.2.1.4.3. Completion of Recovery Test Summary Reports.

3.3. Country Level Leadership (this includes both the country General Manager and the local IT Leader).

3.3.1. Overall responsibility for compliance with Global Technology Recovery Policies, including the designation of individuals to carry out and manage related activities.
3.3.2. Understanding the capability that exists to restore technology services supporting their operations in the event of a loss to the production environment.
3.3.3. Scheduling and facilitation of recovery testing.

3.4. Technology System / Application Owner:

3.4.1. Responsible for understanding the resilience for their IT Systems / Applications, including:
3.4.1.1. Backups and restoration testing results, frequency
3.4.1.2. Recovery capabilities and testing results
3.4.1.3. Risks, such as single-points-of-failure or end of life / end of support (EOL / EOS) components (application, database, Operating System, etc.)
3.4.1.4. Critical dependencies
3.4.2. Responsible for ensuring the ability to restore technology services is properly understood by the business service owners supported by the applications and systems they manage.
3.4.3. Conducts annual recovery testing following the policies and guidance in Section 2.4
3.4.4. Identifies any gaps in the ability to satisfy known constraints defined in Section 2.3
3.4.5. Participates in and helps manage recovery testing for Production Environments that are managed by Global IT Shared Services.

4. References

4.1. Principles: see GITP-001 Global Technology Policy Manual Principles document.
4.2. Related: Standard number or other references, when applicable.

5. Definitions

5.1. **Technology Recovery** (TR): the ability to restore technology services from a loss of the Production Environment.
5.2. **Production Environment:** The primary, physical location in which technology services are run.
5.3. **Technology Services:** The means by which technology capabilities are used by end users> This includes A) the physical infrastructure from which technology systems are run, B) the logical / data components stored and managed by technology systems, and C) the means by which

systems are delivered (run on a user's device, local network within the building, wide-area networks connecting to a data center environment, etc.).

6. Appendices

6.1. Not Applicable

7. Authorization

This policy is authorized by:

James Holley
Vice President, Chief Information Security Officer

Policy Owner: Mark Armour, Sr. Director Global Resilience

Additional Stakeholders: Roberto Garcia de Paredes, Technology Resilience Director

8. Change History

Revision	Date	Author	Revision History
1.0	03/26/2021	Mark Armour	Policy Development
1.0	09/14/2021	Carrie Rogers	GRC Review
1.0	10/18/2021	Jeff Gibson	Review and Approval
1.1	08/10/2022	Vanessa Gonzalez	Review
1.1	08/25/2022	Carrie Rogers	Update of template and review
1.2	09/15/2022	Jeff Gibson	Update of roles (3.2) and review
1.2	10/21/2022	Mark Armour	GRC Review
1.2	11/28/2022	Greg Osgood	Review and Approval
1.2	12/09/2022	Lisa Marshall and Kristina Keller	Global Ethics and Compliance and Legal Review
1.3	10/03/2024	Mark Armour	Minor update to Roles and Responsibilities Section
1.3	10/23/2024	Carrie Rogers	Minor update to References Section and Authorization Section
1.3	11/07/2024	James Holley	Review of updates and approval