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, and
- 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 define the system backup requirements needed to prevent the loss of data in the case of a system failure or the accidental deletion of the data on any system. The aim of the policy is to ensure that it is always possible to recover the information and application systems.

2. Policy Statement

2.1. Backup Method

2.1.1. All production servers that store business data must be backed up at least once a day using a suitable backup method.

2.1.2. A full backup of business data must be performed at least once a week.

2.1.3. An appropriate storage medium must be used. This includes, network backup, or mirrored servers at a remote site.

2.2. Backup & Restore Procedures

2.2.1. Data backups must be tested once a year to ensure backup processes are working as designed.

2.2.2. A restoration test must be performed at least once per year for systems being backed up.

2.2.3. Procedures will be documented with sufficient detail to allow an experienced user of the backup software to restore the data.

2.3. Backup Status

2.3.1. The backup software will be configured to inform an administrator as to the status of any backup performed.

2.3.2. The backup status will be reviewed on a daily basis and any faults identified will be rectified.

2.3.3. Notifications will be sent to application owners if incremental backups are missed after a week or full backups are missed after two weeks.

2.4. Backup Storage

2.4.1. All backups (daily, weekly and monthly, etc.) will be stored in a secure location and conform to enterprise security standards.

2.5. Backup Frequency

2.5.1. The backups of the managed servers should take place at least once every day. A full backup of each managed server should be performed at least once a week. For each backup run, an incremental or differential backup should be performed for each business system when/if a full backup is not being performed.

2.6. Backup Verification

2.6.1. Where prescribed, an annual test of restoration from backup may be required to ensure that both the backup media and procedures function properly.

2.7. Restore Requests

2.7.1. Requests to restore data should be initiated by the Business System Owner through a catalog entry in Service Now, and be forwarded to the local system administrator group or IT Manager as appropriate.

2.8. All backups must be encrypted.

2.9. Technology other than primary storage is to be utilized for backups. Using virtual machine snapshots and clones as substitutes for backups is prohibited.

3. Roles and Responsibilities

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 Human Resources and the Legal Department on these issues.

Local IT Teams and Application Owners are responsible for ensuring backups are performed and in compliance with this policy for the production systems they own. Global IT Shared Services Operations are responsible for the management of backup systems and processes for the IT Data Center environments they support.

Restore Request: All Restore Requests must be submitted by the Business Application Owner / Application Owner through a catalog entry in Service Now.

Data Restore Validation (Backup Verification): Business Application Owner / Application Owners must execute the data validation at a minimum of once a year and report any issue with the data integrity to Global Shared Service Team.

Backup Request: Business Application Owner / Application Owner must submit request for backing up lower environments and components, including any change (adding or removing) of this component.

Audit Reports: Business Application Owners / Application Owners must submit request for evidence or information regarding self-audits.

4. References

4.1. Principles: see GITP-001 Global IT Policy Manual Principles document.
4.2. Related:
4.3. A full list of controls can be found on the Brink's Resource Library.
Applicable SOX Control #:
Applicable Brink's Common Control #: 19, 20, 22, 32

5. Definitions

5.1. Application Owner: team or manager responsible of the proper functionality and delivery of the application and components.

5.2. Business-critical system: critical business systems are defined by the business application owners.

5.3. Backup Types

- FULL: The most efficient and effective backup method is where a full image of the system is put on a Backup Job on a daily basis.
- INCREMENTAL: This is a method of backing up a system where only changes from the last full or incremental backups are copied.
- DIFFERENTIAL: This is a method of backing up a system where one tape set contains a full image of the system and the subsequent tape sets contain copies of the files that are different or that were updated after the full image backup.

6. Authorization

This policy is authorized by:

Greg Osgood
Vice President Global IT & Shared Services

Policy Owner: Tom Weir, Sr. Director - IT Infrastructure and Operations

Additional Stakeholders: Jeff Gibson, Sr. Director - Architecture

Mark Armour, Sr. Director, IT Governance, Risk and Compliance
Ron Banks, Director, Information Security

7. Change History

Original Issue/Publish Date: 07/6/2016

Revision	Date	Author	Revision History
3.0	07/06/2016	Mustapha Kebbeh	No changes
3.1	08/11/2017	Huan Do	Changed template.
3.2	08/12/2019	Mustapha Kebbeh	Section 4- Updated title
3.3	03/01/2021	Carrie Rogers	Update to new policy template
3.3	03/25/2021	Miguel Araya & Tom Weir	Owner review and update
3.3	03/26/2021	Jeff Gibson, Mark Armour, Mustapha Kebbeh	Stakeholder Reviews
3.3	03/29/2021	Tom Weir	Review and Update
3.3	04/19/2021	Tom Weir & Greg Osgood	Review/Approve
3.3	04/26/2021	Legal Department	Review/Approve
3.4	08/25/2022	Carrie Rogers	Updates to template
3.4	10/17/2022	Carrie Rogers	Update to template and Section 6
3.4	10/27/2022	Ron Banks & Angel Mosley	Review
3.4	11/03/2022	Jeff Gibson	Review
3.4	11/15/2022	Mark Armour	GRC Review
3.4	12/06/2022	Thomas Weir	Review
3.4	12/16/2022	Greg Osgood	Review
3.4	12/22/2022	Kristina Keller	Legal review and feedback