1. Purpose and Scope

The purpose of this policy is to set forth the basic principles that are fundamental to Brink's Global Technology and represent industry best practices as viewed by Brink's. This Global Technology policy provides the basic boundaries for more detailed procedures and standards. In the event of a conflict between applicable law and Brink's Technology Policies, the 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 reduce the risk of business outage or disruption, by establishing standardized methods that accurately record, authorize, and promptly address requested changes. By enforcing the requirements detailed in this Policy, we will:

- Manage changes to IT controlled environments with the aim of reducing disruption to users
- Reduce the number of change failures or change-induced outages
- Eliminate unauthorized changes.

This policy is applicable for anyone making changes within or connected to the IT controlled environments defined below. All employees, contractors and vendors are required to comply with the Change Management policy, with the exception of vendors who maintain external environments that Brink's shares with other customers - they are outside the scope of this policy.

The IT controlled environments are defined as follows:

1. For application changes, the controlled environments include all Production environments regardless of location.
2. For infrastructures changes, the controlled environments include all Production environments regardless of location, and planned maintenance activities in all lower environments regardless of location.

Change examples include, but are not limited to:

Infrastructure Changes	**Application Changes**
Modify, Add, Promote, Remove, or Restart:	Modify, Add, Promote, Remove, or Restart:
Physical Hardware	Software Code
Virtual Hardware	Interface/GUI
Network Hardware	Configuration Files
Network Configuration	Services
AD OU add/remove/update	Batch Files
Database Schema/Design	Bulk Data Loads
Database content/data	Patching
Operating Systems	Security configuration
Patching	Operating Systems
Security configuration	
Security penetration tests aka "Pen Tests"	Security penetration tests aka "Pen Tests"

2. Policy Statement

2.1. Change Documentation All IT changes require proper documentation in the form of a Change Request record using the established IT Service Management (ITSM) tool, according to the published Change Management process and procedure. Required documentation includes testing confirmation, an implementation plan, post-change validation steps, and a backout plan.

2.1.1 All changes have a defined Type and Scope**,** based on their timing and impact potential.

Type	Definition
Normal	• Planned with sufficient lead time to follow the established daily change review cycle • Moderate and High Risk changes require formal Tech Review • Requires approval by IT management • Global scope changes and Region scope/High Risk changes require formal Change Advisory Board (CAB) Review and approval
Emergency	• Unplanned, with little or no lead time • Requires expedited review/approval by IT management and DOES NOT wait for formal weekly review
Standard	• Pre-approved, low risk changes submitted via the Standard Change Catalog and executed with no lead time requirement • Standard Change proposals must have had at least 4 documented examples of successful execution within the last 6 months and include the expected frequency & monthly volume of the change

Scope	Description

Global	• Potential risk/impact to the entire enterprise
	• Global scope can include:
	  ○ Global Backbone Networks
	  ○ Global Telecom Services (VoIP, Teleconferencing)
	  ○ Global Data Center infrastructure
	  ○ Global Data Center Network connectivity
	  ○ Global Data Center Production Maintenance / Management (backup/recovery, monitoring, patching)
	  ○ Major Changes to Global Shared Services (Exchange / Office 365 / Skype / Active Directory / Azure / AWS)
	  ○ Major releases of core business applications

Region	• Potential risk/impact to a single region • Approved by local IT leadership and relevant regional service owners
Country	• Potential risk/impact to a single country or single site • Approved by local country IT leadership

2.1.2 All changes must be assessed for **Risk** on a scale of 3 levels, with Risk level 1 as High risk and Risk level 3 as Low risk. Risk is calculated based on conditions documented by the Change Leader on the Change Request form.

Risk	**Example Conditions**
High	• Scope is 'Global' or 'Region' • Change Environment is 'Datacenter Production' • Solution Tested is ''No' • Unavailability Required is 'Yes' • Scheduled Window is 'Peak times of the month/year, or within blackout dates' or 'Business hours' • Implementation Time Required is more than 2 hours • Validation Time Required is more than 2 hours • Number of CIs is more than 10 • Number of tasks is more than 6 • User validation is 'End-User/Customer cannot validate within window' • Backout ability is 'not feasible'
Moderate	• Scope is 'Region' or 'Country' • Change Environment is 'Datacenter non-Production', 'Corporate Office / Headquarters', 'Multiple Branches' • Solution Tested is ''Yes' • Unavailability Required is 'No' • Scheduled Window is 'Non-business hours' • Implementation Time Required is 1-2 hours • Validation Time Required is 1-2 hours • Number of CIs is 6-10 • Number of tasks is more than 4-6 • User validation is 'End-User/Customer will verify within window' • Backout ability is 'Moderate' or 'Difficult

Low	• Scope is 'Region' or 'Country' • Change Environment is 'Single Branch' • Solution Tested is ''Yes' • Unavailability Required is 'No' • Scheduled Window is 'non-Business Hours' or 'within maintenance window' • Implementation Time Required is less than 1 hour • Validation Time Required is less than 1 hour • Number of CIs is 5 or less • Number of tasks is 3 or less • User validation is 'No user validation required' • Backout ability is 'Easy'

2.2 Change Planning All changes must be submitted, planned, tested, *peer reviewed, and executed according to the authorized Change Management process and procedure, and the IT team planning / coordinating / executing a change will be accountable for its full life cycle.

*****Note: Peer Review assignments are automated based on a pre-defined matrix and workflow which does not allow a Change Leader to peer review their own tasks.

2.3 Change Approval All changes require management approval. All requested approvals must be received before a change is considered authorized for deployment.

2.4 Change Governance All changes require governance by Global IT Service Management, who will routinely audit change to ensure policy compliance. All items within the policy are auditable.

2.5 Change Closure All changes must be closed in a timely manner according to the documented Change Management process and procedures, and closure documentation must accurately describe the results of the change.

2.6 Emergency Change Exception for Outage Response If an outage in an IT-controlled environment is causing ongoing business impact (or business impact is imminent) and remediation requires a change, the IT team that manages that environment is authorized to move forward with remediation prior to formal documentation and approval of a change record, subject to the following:

2.6.1 An Incident record must be submitted to document the production impacting event.
2.6.2 Approval must be obtained from either **A**) the IT Director responsible for the impacted Environment OR **B**) the Major Incident Manager engaged in the triage event, IF the type of change required to restore service is on the list of approved change types specified in the Major Incident Management Emergency Change Approval Procedure document.
2.6.3 The team's manager, director, Global IT Change Management, and Global IT Operations must be notified via email that they intend to respond immediately to restore service.
2.6.4 The remediation must be documented as an emergency change and formally approved as soon as possible after service has been restored.

2.7 Change Freezes Brink's Global IT will adhere to documented process guidelines for change freezes (aka "blackout schedules").

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, vendor or consultant violates a Brink's policy, Brink's may pursue its remedies under the contract, including without limitation, termination of the contract and pursuit of financial damage awards.

3.2.

Role	Responsibilities
Change Manager Champion, Advocate, Design Lead, Coach and Protector of the Change Management Process	• Ensures that the Change Management process and working practices are effective and efficient • Ensures alignment and continuity between Change Management processes and other related processes • Is the primary source of management and stakeholder information about the Change Management process • Ensures compliance to the Change Management policy, process, and procedure • Produces regular and accurate management reports that deliver business value • Ensures only authorized changes are implemented and Change Requests that do not meet the defined requirements get rejected • Chairs the CAB meetings, ensures that the CABs are authoritative and effective • Reviews all implemented changes (post-change reviews) • Analyzes change records to detect any positive trends or problems and proposes actions to rectify
Change Leader The role of the Change Leader applies to any IT staff given responsibility for submitting, planning, and implementation of a specific change	• Follows the Change Management procedure for submitting a Change Request • Exercises "lead" responsibilities for the lifecycle of the change • Coordinates planning, scheduling and communication with business and technology stakeholders, including implementation teams • Locates, identifies and requests resources used to build, test and implement changes • Initiates change implementation to specified environment • Manages and monitors assigned task/change implementers, ensures the change proceeds according to scheduled dates/times • Provides additional information regarding the change when requested

	• Reviews, verifies, and ensures proper documentation of the task/change completion, and follows the Change Management procedure steps to close the change record. Participates in the post-change reviews as needed.
Change Approvers Approvers may include technology and/or business representatives, and application, infrastructure, andsupport management	• Authorize that all required information has been completed and agreed upon between business, implementation resources, and support teams, and that the change aligns with business objectives, events or other changes, in a manner that minimizes the risk of service disruption. • Authorize that the documented change plan aligns with the requested objective, and is fit for purpose
Change Advisory Board (CAB)	• Reviews and approves all changes categorized as Global in scope, or Region in scope and High Risk • Authorizes that the changes align with business needs, strategic objectives, and projects • Authorization to reject changes that do not align with business needs, strategic objectives, and projects

4. References

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

4.2. Related:

- Brink's Global IT Change Request PROCESS v202105
- ServiceNow_Global IT Change Request PROCEDURE_Normal & Emergency_v2020-02
- Major Incident Management Emergency Change Approval Procedure
- ServiceNow KB article KB0010292 “Global IT Change Management Policy / Process / Procedure”

4.3. A full list of controls can be found on the Brink’s Resource Library.
Applicable SOX Control #:
Applicable Brink’s Common Control #: 12, 16, 18

5. Definitions

5.1. **A change is defined as**: The addition, promotion, modification, removal, restart or any other activity that affects the running state of any applications/application components/infrastructure components in the IT controlled environments.

5.2. **A ‘Normal’ change is**:

- Planned with sufficient lead time to follow the established daily change review cycle
- Requires approval by IT management
- Requires formal Tech Review if Risk is moderate or high
- Requires formal CAB Review and approval by the Global IT CAB if Scope is “Global” or Scope is “Region” and risk is high

5.3. **An ‘Emergency’ change is**:

- Unplanned, with little or no lead time
- Requires expedited review/approval by IT management and DOES NOT wait for formal weekly review

5.4. **An 'Standard' change is**:

- Pre-approved, low risk changes submitted via the Standard Change Catalog and executed with no lead time requirement
- Standard Change proposals must have had at least 4 documented examples of successful execution within the last 6 months and include the expected frequency & monthly volume of the change

6. Appendices

6.1. Not Applicable

7. Authorization

This policy is authorized by:

Greg Osgood
Vice President Global IT & Shared Services

Policy Owner: Charles Finklea, IT Director Global IT Service Management / Change Management Process Owner

Additional Stakeholders:

Global CAB (Change Advisory Board) Members

Jeff Gibson
Mustapha Kebbeh
Tom Weir
Chuck Williams

8. Change History

Revision	Date	Author	Revision History
2.0	07/20/2016	Charles Finklea	No changes
2.1	08/08/2017	Huan Do	Changed template
3.0	10/18/2017	Charles Finklea / Jay Lenz	Policy update / expansion
3.5	12/16/2018	Charles Finklea / Sarah Jackson-Butler	Policy update
4.0	01/01/2019	Charles Finklea	Policy update / formatting
4.1	09/01/2019	Charles Finklea	Policy revision
4.2	11/16/2020	Charles Finklea	Policy review and update
4.2	2/10/2021	Carrie Rogers	Policy review and update
4.3	04/27/2021	Charles Finklea	Policy update
4.4	05/20/2021	Charles Finklea	Policy update

4.4	09/2021	Greg Osgood	Review and Approve
4.4	10/15/2021	Kristin Keller/Legal	Policy review
4.4	11/29/2021	Charles Finklea	Policy review
4.5	2/10/2022	Charles Finklea	Policy updates
4.6	8/25/2022	Carrie Rogers	Updates to template