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 define requirements for the management of incidents that affect the Brink's IT environment. An effective IT Incident Management Policy helps the organization reduce the negative consequences of IT incidents by speeding the response and effectively executing processes to restore of IT services to normal.

2. Policy Statement

Incident Management is the process for responding to unplanned interruptions or reduction in the quality of IT services.

The Incident Management Policy is intended to achieve the following:

1. Standardize Incident Management Processes
2. Standardize performance metrics of the incident life cycle to enable improvement efforts
3. Provide a common understanding of the Incident management process
4. Provide a repeatable process for documenting and communicating outages with customers

Brinks will utilize the best practice framework for the implementation of all Incident Management classifications within Information Technology.

a. Incident Management

Incident Prioritization

The priority of an Incident is determined by its impact and urgency. Brink's Incident Levels are defined below:

Incident Level	Description
Priority 1 Critical	An incident causing a **complete disruption or extreme degradation** Affects the delivery of service(s) to the customer, or operation of the business environment. Service(s) impacted do not have a contingency plan or work-around. The impact of the incident is national or regional, or the incident has the potential for a significant loss of revenue.

	Core Process Applications for Money processing, CIT, ATM, File Transfer App, client communications (CSC and Support desk), Interfaces, Data center outages (shared environment), Shared Services Scenarios: • Complete disruption of datacenter network or system services • All branches, all users, and all components of an application • Disruption to a business process causing revenue impact on a top 5 countries • 15 minutes of anticipated non planned disruption • Direct safety to Brink's drivers / Couriers • Is risking Company Revenue **This is considered a Major Incident**.
Priority 2 High	An incident causing **significant disruption in service delivery** Affects service(s) for one or more clients or operation of the business environment that can lead to a complete disruption. A contingency plan or work-around may exist to mitigate impact and / or restore partial functionality until restoration of the affected IT service(s). Core Process Applications for Money processing, CIT, ATM, File Transfer App, client communications (CSC and Support desk), Interfaces, Data center outages (shared environment), Shared Services Scenarios: • Service, application, or infrastructure is still functioning with degraded performance • Network or power outage in 1 location within a country • Disruption to a business process causing revenue impact on a NON top 5 countries **This is considered a Major Incident.**
Priority 3 Medium	An incident causing **minimal disruption or deterioration in service delivery** Affects the client or operation of the business environment. This includes issues impacting unique groups of users. A contingency plan can be implemented (either automatically or manually) if feasible and with no additional impact.
Priority 4 Low	An incident **with no impact on production service delivery**. Affects a minimal number of staff impacted and/or able to continue operation of the business environment. The client/customer is impacted or inconvenienced but not in a significant way. The user may or may not have a work around.

Incident Escalation

The IT support teams will determine if the incident can be resolved at Level 1 or if an escalation to a higher skill set (L2, L3) is required (functional escalation). All P1 or P2 incidents must be escalated to the IT-Service Desk, IT-Application Support, or IT-Operation Center.

Root Cause Analysis (RCA)

In the event of a Major Incident, or at the request of business or IT leadership, the Major Incident Manager will work with Problem Management for RCA delivery.

The following policy is established for Incident Management (including Major Incident Management):

i. All calls to the Service Desk must be logged.

ii. All IT related Incidents must be reported, recorded, managed, and appropriately communicated through the Brinks approved Incident Management tool - ServiceNow. This allows for a centralized repository for historical record keeping

iii. The Incident Management Practice will have a Process Owner and a Process Manager. This is required to ensure proper resources are secured to carry out the Incident Management process to completion.

iv. All IT Managers and Support Group Managers are responsible for ensuring the incident Management Process is followed.

v. When a resolver group utilizes a knowledge base article to resolve an incident they are required to select "Solved with knowledge" in the resolved type of the ITSM incident resolution information tab.

vi. Upon resolution of an incident, the affected end user(s) will be notified that the incident has been resolved and restored to normal business function.

vii. This policy will complement and not supersede compliance policies such as those associated with the Security Incident Response Team (SIRT) or any other applicable Brinks compliance requirements.

b. Major Incident Management

A Major Incident is categorized as a Priority 1 – Critical or Priority 2 – High. A Major Incident can only be declared by one of Brink' IT-Major Incident Managers (MIM) or Director of Global IT Operations.

A Priority 1 Incident indicates significant impact to the business and demands immediate response and resolution. A P1 incident can be declared critical only for Core applications and scenarios as defined in the Prioritization Matrix.

A Priority 2 Incident indicates a significant disruption to service delivery. A P2 incident must be declared high priority only for core applications and scenarios as defined in the Prioritization Matrix.

The following policy applies only to Major Incident Management and is in addition to the policy for all Incident Management:

1.2.1. The Major Incident Process owner is the Director of IT -Global ITSM and the Process Manager is the Incident and Major Incident Manager.

1.2.2. All Priority 1 and Priority 2 incidents must be escalated to or created by the IT-Operations Center

1.2.3. All Major Incidents must be reported by Phone to the IT-Operations Center. (No P1 or P2 incidents will be managed by email or Chat)

1.2.4. On a major incident, the “reported by” or impacted person must join the bridge until issue is resolved.

1.2.5. The Incident Manager or Major incident Manager is the only person who can approve a technician to hang up from the Technical Bridge.

1.2.6. All configuration changes being made by the technical owners in pursuit of resolution must be communicated according to Major Incident Management Procedures for documentation and approval, to ensure awareness of fix/upgrades/changes applied during a Major Incident. Verbal approval must be obtained from the IT Director responsible for the impacted environment or Major Incident Manager of the incident.

1.2.7. If an On-Call resource is needed to resolve an incident, the priority of the incident must be P1 or P2. On-Call resources will not be engaged for P3 or P4 incidents.

1.2.8. On-Call schedules must be defined and updated, if necessary, by the respective Managers of the resolvers Groups.

1.2.9. Resolver groups (On-Call) must respond and join the call based on agreement and commitments made with the Managers of the respective groups.

1.2.10. All support groups will document resolution and tasks executed in the incident ticket.

1.2.11. Notification and communications for Major Incidents will follow the definitions of the Communication procedure. For all the major incidents, the major incident manager will engage with BCP team to handle communications with the business and customers.

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.

Role	Ownership

End User	The End User is the person using an IT resource. This role is responsible for: • Reporting Incidents and IT requests through the IT-Service Desk. • Providing details and information needed for troubleshooting • Being available to perform testing or validate functionality. • Coordinating with in country users to perform test and validations • Coordination within country Vendors.
IT Staff	IT Organization Staff members. This role is responsible for: • IT infrastructure • The delivery of IT Services • Reporting Incidents or possible Incidents through the IT-Service Desk.
IT-Service Desk/IT-Operations Center Manager (SD/ITOC)	The IT-Service Desk Manager is responsible for: • Day-to-day management of the IT-Service Desk function • Assisting with all management escalated issues.
IT-Service Desk (SD)	The Service Desk Analyst provides Level 0 Support and is responsible for: • Day-to-day communication with all End Users • Facilitating the resolution and fulfillment of Incidents and Requests.
IT-Operations Center Analyst (ITOC)	The IT-Operations Center Analyst provides Level 1 Support and is responsible for: • Day-to-day communication with all End Users • Facilitating the resolution and fulfillment of Incidents and Requests.
Incident Manager	The Incident Manager is responsible for: • Process design • Day-to-day management of the process. • Managing Incidents effectively through First, Second, Third Level Support.
Incident Analyst	The Incident Analyst is responsible for: • Implementing and executing the Incident process as defined by the Incident Owner/Manager • Being a point of contact for escalated issues, questions, or concerns.
Support Level 2/3	Level 2/3 group(s) have greater technical skill level than Level 1 Support. These groups are separated from “End User first point of contact” responsibility and typically have longer timescales to perform incident diagnosis and resolution tasks. Escalation to these groups may be direct from Level 1/Level 0 Support or from Level 2 Support based on the Priority and Complexity of the issue. • Level 2 Support is responsible for handling Incidents that Level 0 and Level 1 Support cannot resolve.
	• Level 3 Support is responsible for handling Incidents that require specialized and in-depth technical skills.
Resolving Group	The incident will be set to a Resolved state once the issue is remediated. At that point, the Resolving Group owns restoration of failed IT Services. Ownership may be with Level 0 (IT-Service Desk), Level 1 (IT-Operations Center) or Level 2 and Level 3 teams as they appear in ServiceNow: IT-Systems L3, T-Telecom, IT-Middleware Support Team, or IT-Application Support. Each level of support must be defined, by service, and provided the proper access and rights to perform the troubleshooting task. This role will: • Escalate the incident to a Vendor (Global Vendor) or next functional level • Take care of the Incident Status and documentation during troubleshooting • For P1 Incidents, this role will raise a RCA (Root Cause Analysis) to be reviewed and attached to the incident.

Validation Group	The Validation Group is responsible for: • Setting the Resolved state on the incident, usually IT-Operations Center or IT-Service Desk. • Performing the validation of the incident resolution by contacting the End User/IT Staff. • Engaging the resolving group in case the incident was not resolved • Documenting the validation approval in the ticket. • Incident resolution tracking.

Major Incident Management

Role	Ownership
Major Incident Manager	The Major Incident Manager (MIM) Manages all Major (P1) and High-Priority (P2) Incidents to successful resolution and is accountable for: • Delivering accurate communication via defined applications (ServiceNow & xMatters) during the incident lifecycle • Management of stakeholders until recovery and resolution are achieved.
Resolver Group	Group responsible for resolving or restoring the services related to a failure in a time defined (SLA/OLA). All groups are defined as L1, L2 or L3 teams.
First Responder Team	Manages all Priority 3 (medium) and Priority 4 (low) Incidents to successful resolution, accountable for: • Delivering clear and accurate communication and resolution during the Incident lifecycle. • Escalation to the Major Incident Management Team if a P2 or a P1 Incident is identified.
Business Continuity Process Team	Group responsible for: • Determining customer impact • Relaying information to impacted businesses during a major incident.

4. References

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

4.2. Related:
Major Incident Management Process Document in Service Now Knowledge Base
Major Incident Management Procedures document
Incident Management Process document

4.3. A full list of controls can be found on the Brink's Resource Library.
Applicable SOX Control #:
Applicable Brink's Common Control #: 24

5. Definitions

a. Not Applicable

6. Appendices

a. 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

Additional Stakeholders: Lisa Marshall & Guillaume Nonain (Legal Ethics and Compliance)

8. Change History

Revision	Date	Author	Revision History / Purpose of Change
1.0	10/12/2018	Miguel Araya	Creation
1.1	12/26/2018	Guillaume Nonain	Added Language related to personal data breaches
1.2	1/25/2019	Mustapha Kebbeh	Final Version
1.3	11/14/2019	Angel Mosley, GIS	Creation, Combination of IT Incident Management policy (GITP-000) and proposed Major Incident Policy.
1.4	10/12/2021	Ana Cotes	Updated Incident Management Prioritization, Incident Management Escalation, Metrics, Major Incident Management, Policy, and Roles and Responsibilities Added Incident Management policy and Incident Management roles/ownership table
1.4	11/29/2021	Carrie Rogers	GRC Review
1.4	December 2021	Stakeholders	Review
1.4	03/12/2022	Mark Armour	Review
1.4	03/25/2022	Charles Finklea & Ana Cotes	Review and update
1.4	04/15/2022	Greg Osgood	Review
1.4	08/25/2022	Carrie Rogers	Updates to template

1.4	11/29/2022	Kristina Keller	Review