Executive Summary
Brink’s US Business Continuity Plan

*This document has been reviewed since the emergence of COVID-19 (3/12/20).

Contents

1.0 OVERVIEW ................................................................................................................................. 2
2.0 INTRODUCTION ............................................................................................................................. 2
3.0 PURPOSE .......................................................................................................................................... 2
4.0 ACTIVATION ...................................................................................................................................... 2
5.0 ROLES ............................................................................................................................................. 3
6.0 ALL HAZARDS PLANNING ........................................................................................................... 3
7.0 PROCEDURES ............................................................................................................................... 4
Appendix .................................................................................................................................................. 5

Brink’s US Business Continuity Policy (edited)..................................................................................... 5

REVISION HISTORY: .......................................................................................................................... 8
1.0 OVERVIEW
The Brink’s US Business Continuity Plan Executive Summary provides general information about Brink’s Business Continuity Program and high-level details around its Recovery Plan contents. Included in the Appendix of this document is an edited version of Brink’s Business Continuity Policy.

2.0 INTRODUCTION
Brinks recognizes the potential risks associated with service and business interruptions and the importance of maintaining operations and the continued delivery of services following an adverse event. Brink’s Business Continuity Program provides the policies, procedures and framework needed to minimize the potential for disruption and to recover services should an interruption occur.

3.0 PURPOSE
Brink’s maintains several plans for the recovery of Business Functions / Services and critical technology systems. At a minimum, each plan includes defined roles and responsibilities for the execution of response and recovery activities. Each plan also includes clear, actionable procedures for the execution of the recovery process.

4.0 ACTIVATION
The Brink’s Incident Response Team has authority to activate business recovery plan procedures and to initiate technology troubleshooting and remediation activities. In the event of an activation, the Plan Owner and designated Alternate(s) will be contacted and informed of the decision to activate. Brink’s Incident Response Team is tasked with escalating to the Brink’s Crisis Management Team when conditions warrant.
5.0 ROLES

Activities and procedures within each plan are assigned to Roles defined within the plan. The below are required roles and optional / suggested Roles for specific plan types (business vs. technology recovery).

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan Owner [Required Role]</td>
<td>• Plan Review, Approval and Ownership</td>
</tr>
<tr>
<td></td>
<td>• Overall management of Plan Execution, including the mobilization of resources</td>
</tr>
<tr>
<td></td>
<td>• Communication with team members and the Brink’s Incident Response Team</td>
</tr>
<tr>
<td>Plan Lead [Recommended Role]</td>
<td>• Direct oversight or execution of Plan Procedures</td>
</tr>
<tr>
<td></td>
<td>• Coordination with the Plan Owner and team members</td>
</tr>
<tr>
<td>Internal Communications Lead</td>
<td>• Management of outbound communications to internal team members</td>
</tr>
<tr>
<td>[Alternate Business Role]</td>
<td>• Management of incoming Brink’s communications</td>
</tr>
<tr>
<td>External Communications Lead</td>
<td>• Management of communications to external customers and / or support partners</td>
</tr>
<tr>
<td>[Alternate Business Role]</td>
<td>• Management of incoming external communications</td>
</tr>
<tr>
<td></td>
<td>• Coordination of messaging with internal corporate communications designate</td>
</tr>
<tr>
<td>Global Operations [Required</td>
<td>• Systems monitoring and initial troubleshooting</td>
</tr>
<tr>
<td>Technology Role]</td>
<td>• Emergency / Incident Communications</td>
</tr>
<tr>
<td>Network Engineering [Alternate Technology Role]</td>
<td>• Configuration and validation of supporting network systems (incl. hardware, software and circuits)</td>
</tr>
<tr>
<td>Systems Engineering [Alternate Technology Role]</td>
<td>• Systems support architecture (DNS, AD, TMG Authentication, etc.)</td>
</tr>
<tr>
<td>DBAs (SQL, Oracle) [Alternate Technology Role]</td>
<td>• Back-end data for specified system</td>
</tr>
<tr>
<td>Business Support [Alternate Technology Role]</td>
<td>• Transaction and Line-of-Site testing / validation</td>
</tr>
</tbody>
</table>

6.0 ALL HAZARDS PLANNING

Brink’s takes an all hazards approach to Business Continuity and Disaster Recovery. This means Brink’s does not manage separate response procedures for every potential threat (i.e. fire, flooding, earthquake, etc.). Instead, the company develops procedures for the recovery of services based on the impact from a wide variety of disruptive events. Impacts include:
- Loss of facilities / workspace (including on-site physical resources)
- Loss of computing technology (including network and internet capability)
- Loss or significant reduction of workforce (including pandemic events)
- Loss of critical third-party services

Brink’s does take event-specific steps in cases where preparatory actions are appropriate. This includes regions that are prone to hurricanes or other tropical systems in which the threat is known and can be prepared for ahead of time (i.e. pre-deploying resources or moving equipment out of the immediate threat zone). This also includes evolving events such as pandemics in which actions can be taken to mitigate the threat while it is ongoing (i.e. awareness campaigns and policies to promote social distancing).

7.0 PROCEDURES

Procedures are detailed steps for recovering defined resources or resource capabilities necessary to deliver critical Business Services. Procedures will vary greatly depending on the plan type (Business vs. Technology), defined strategy and overall priority of the service or dependency.

Procedures generally include actionable steps to be taken and the role responsible for carrying out the activity. Actions may also be broken out by phases, such as ‘readying of recovery environment / workspace’; ‘recovery steps’; and validation or testing needed for the recovery of technology systems. In some cases, procedures are also defined for resumption to normal operations or restoring technology systems to their production environment. Technology Recovery Plans will also include estimates of the time needed to execute the defined step.

<table>
<thead>
<tr>
<th>Action</th>
<th>Time needed to perform</th>
<th>Role Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Plan Owner</td>
<td>5 Minutes</td>
<td>Incident Response Team</td>
</tr>
<tr>
<td>Mobilize Team</td>
<td>20 Minutes</td>
<td>Plan Owner</td>
</tr>
<tr>
<td>Initiate Failover / Recovery</td>
<td>1 Hour</td>
<td>Plan Lead(s)</td>
</tr>
<tr>
<td>Other</td>
<td>10 Minutes</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Appendix

Brink’s US Business Continuity Policy (edited)

Purpose

The purpose of Brink’s Business Continuity policy is to establish:

- The individuals and teams with responsibility for preparing the organization and minimizing the potential loss of revenue or negative impact to reputation resulting from a significant disruption.
- The minimum requirements for departments, divisions and countries to be adequately prepared to respond and recover from a significant disruption to their operations.
- Steps departments, divisions and countries can take to improve their level of preparedness, in order to minimize impact to customers and any subsequent negative impact to the organization’s reputation.
- Support and resources that are available to assist departments, divisions and countries in improving their overall level of preparedness.

ORGANIZATION

Business Continuity at Brink’s is led by the Global Director of Business Continuity and is responsible for enterprise level Business Continuity (BC), Technology Recovery (TR), and Emergency / Crisis Management (EM/CM). This includes:

- Developing and maintaining the policies and procedures necessary to support and execute BC, TR and EM/CM activities.
- Developing and maintaining tools, resources and templates to facilitate BC, TR and EM/CM activities.
- Providing guidance and support to departments, divisions and countries in the execution of their BC, TR and EM/CM programs and activities.

APPROACH

Brink’s takes a LEAN based approach to Business Continuity (BC), Technology Recovery (TR), and Response Management (RM, aka Emergency or Crisis Management). The focus of all activities should be to improve the organization’s ability to effectively respond and recover from any disruptive event or significant threat. This starts with measuring the current state and identifying where improvements can be made to shorten response and recovery timeframes or to increase capacity and functionality of recovery strategies and resources.
CAPABILITIES ASSESSMENT

The Capabilities Assessment replaces the traditional Business Impact Analysis and Risk Assessments. This document defines:

- Workspace, technology systems, third party and physical assets needed to conduct business and deliver products and services to customers.
- For each dependency (workspace, technology, vendors and assets) current capabilities are identified that serve to minimize loss / impact or to facilitate restoration / recovery of the resource(s) in the event of a loss or disruption.
- Service-level recoverability is based on three factors needed to effectively respond and recover from a disruption. These are:
  - Resources: these are tools, equipment and systems
  - Procedures: the processes and steps followed
  - Competencies: the skills, training and awareness needed by individuals to properly utilize defined resources or execute procedures effectively.

REMEDIATION AND IMPROVEMENT

The results of the Capabilities Assessment are used to identify opportunities for improvement and determine ownership of remediation activities. Improvements can be made in any one or combination of multiple factors (Resources, Procedures and Competencies). Prioritization of improvement activities is the responsibility of leadership with input and guidance from the Business Continuity Team. Factors that drive the prioritization of efforts include:

- Operational or service recovery capabilities at risk due to existing gaps.
- Cost and effort of remediation
- Anticipated improvements in recovery time and / or capability or functionality.

Upon review and approval of defined improvement initiatives, the assigned owner is responsible for managing to completion. The Global Business Continuity Team tracks and reports progress to leadership, while providing support and assistance to responsible teams.
EXERCISING

Periodic exercises shall be conducted to:

- Improve the skills and competencies among individuals with roles in the Response and Recovery Processes.
- Measure / validate the time needed to execute response and / or recovery activities.
- Measure / validate the capacity of the recovery environment to handle normal production volumes.
- Measure the functionality of the recovery environment, including identification of any lost capabilities.
- Measure / validate the effort of executing recovery strategies (personnel needed, man-hours, support services, etc.).

At a minimum, all exercises must include all staff and resources necessary to fully execute the defined recovery strategy. Where possible, exercises must provide opportunities to involve affected audiences in validation routines. At a minimum, all exercises must include:

- A high-level Plan, which lists the exercise objectives, participants and plans / resources / activities within scope.
- A measurement of the recovery timeframe and the capacity / functionality of the recovery environment as compared to production.
- Identification of issues encountered and any opportunities to further improve by shortening the time to respond and recover or increase capacity / functionality of recovery strategies and recovered resources.
- All issues and opportunities must be assigned an owner and remediation tracked to completion by Business Continuity.
- An executive summary report, which lists the results of all exercise objectives, issues encountered and follow-up actions.

EVENTS

Events that necessitate assembly of the Incident Response Team AND execution of at least one defined recovery strategy may be substituted for a scheduled Exercise as evidence of recovery capability. In all such cases, the response and recovery must be documented and a report completed that addresses exercise requirements, including:

- Participants and plans / resources / activities executed or engaged as part of the event response and recovery effort.
- A measurement of recovery timeframes and capacity / functionality restored as well as any service, operations or customer impact form the event.
- A list of any issues encountered, opportunities for improvement and follow-up actions.
## Executive Summary

Brink’s US Business Continuity Plan

### REVISION HISTORY:

<table>
<thead>
<tr>
<th>Version</th>
<th>Change(s) made</th>
<th>Date</th>
<th>Updated By</th>
<th>Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Document Developed</td>
<td>2/24/2014</td>
<td>Mark Armour</td>
<td>2/27/2014</td>
</tr>
<tr>
<td>1.1</td>
<td>Addition of version control and Strategies (#7) Section</td>
<td>10/9/2014</td>
<td>Mark Armour</td>
<td>10/17/2014</td>
</tr>
<tr>
<td>1.2</td>
<td>Minor modifications to verbiage and update of current policy statement</td>
<td>3/1/2016</td>
<td>Mark Armour</td>
<td>5/2/2016</td>
</tr>
<tr>
<td>1.3</td>
<td>Updated to reflect revised Policy</td>
<td>7/20/2017</td>
<td>Mark Armour</td>
<td>7/28/2017</td>
</tr>
<tr>
<td>1.4</td>
<td>Updated to reflect revised Policy</td>
<td>11/27/2017</td>
<td>Mark Armour</td>
<td>9/28/2018</td>
</tr>
<tr>
<td>1.5</td>
<td>Reviewed, no changes necessary</td>
<td>10/15/19</td>
<td>Mary Hamre</td>
<td>10/1</td>
</tr>
<tr>
<td>1.5</td>
<td>Reviewed, no changes necessary</td>
<td>3/12/20</td>
<td>Mary Hamre</td>
<td>3/13/20</td>
</tr>
</tbody>
</table>