BRINKS LEGAL

POLICY FOR RESPONDING TO THIRD PARTY DOCUMENT DESTRUCTION REQUESTS

REVISED: MAY 2021

PURPOSE

The purpose of the Policy for Responding to Third Party Document Destruction Requests (the "Policy") is to set forth the expectations and provide guidance when Brink's is requested to destroy documents and confidential information as a result of a contractual obligation, usually contained in a Non-Disclosure Agreement. Often, this situation arises in the context of a Merger and Acquisition (M&A) transaction, where, following negotiations with a potential target, Brink's is asked to destroy documentation and confidential information and certify the destruction. Therefore, we have developed this Policy to ensure that all Brink's employees asked to perform this activity have clear expectations and guidance to do so. The procedures detailed in this Policy will be carried out by, or in consultation with, the Legal Department. This Policy supersedes any corporate Document/Records Retention policies in place with the exception of documentation provided to the Board of Directors, which much be retained indefinitely. Strict adherence to this Policy is expected. Failure to follow this Policy or other Brink's policies may result in disciplinary action, including possible termination.

STEPS FOR INTERNAL CERTIFICATION

If you receive a letter (usually delivered via DocuSign) to destroy documents and confidential information related to a contractual obligation, please follow these steps to complete the internal certification of destruction:

1. Read the details of the Destruction Letter carefully to ensure you understand the request. In certain situations, you may be asked to retain information based on the exceptions below. If there are any questions about what is expected, reach out to the contact name on the letter for clarification.
2. Review all of your documentation (in any format) related to the transaction in question.
3. Review the Destruction Definition in this Policy and then delete the records accordingly. Be sure to completely delete the files from any electronic recycle bins (if applicable). When destroying paper documents, be sure to shred and dispose of the documents in a safe, confidential manner.
4. Return to the Destruction Letter and Certification (usually delivered via DocuSign) and sign the certification that you have completed the destruction.

DESTRUCTION DEFINITION

Destruction of documents and confidential information should include any electronic repositories or data rooms, whether or not hosted by Brink's and all documents in any format.

As an exception to the general requirements to destroy all documents and confidential information, the Legal Department:

- will retain indefinitely any materials submitted to the Board of Directors per company policy;
- will retain one copy of material related to the negotiation and execution of any agreement in connection with the transaction in question; and/or
- may retain additional information needed to respond to pending or potential regulatory inquiries.

Examples of "documents and confidential information" include, but is not limited to:

1. any type of document or information (e-mails, including attachments to e-mails, memos, letters, faxes, correspondence, presentations, contracts, papers, books, accounts, ledgers, spreadsheets, drafts, versions, attachments, studies, reports, logs, notes, calendars and calendar entries, day-planners, diaries, agendas, minutes, transcripts, statements, rolodexes, notebooks, drawings, graphics, images, diagrams, maps, charts, graphs, films, animations, photographs, photocopies, voice mails, telephone messages, invoices, statements, instant messages, text messages, communications, microfilm, recordings (electronic, videotape, and sound), forms, templates, outlines, word-processing documents, files, and any other records, writings, data and data compilations, and tangible things and objects, including both originals and non-identical copies or duplicates (such as with any notes or markings), and both active and archived documents and information);
2. electronically stored information in any format, metadata, any type of computer or electronic storage device such as laptops/personal computers, personal digital assistants ("PDAs"), any type of drive or electronic storage device (e.g., network drive, hard drive, shared drive, flash drive/USB drive, memory card, any type of tape or disk (backup tapes, backup disks, compact disks ("CDs"), digital video disks ("DVDs"), zip disks),

any type of system (accounting systems, voice mail systems, instant messaging systems, text messaging systems, backup systems), any type of file or folder (office files, desk files, active files, archive files, working files, personal files; pst files, jpeg files, pdf files, wav files, etc.), any type of application or program, hardware or software, documents and information on the Internet/World Wide Web and any Company intranets, weblogs/blogs, bulletin boards, any type of server (file server, database server, e-mail server, web servers), and any other storage method or device of any kind), video and audio recordings from company vehicles however stored;

3. in any location including office, home, company or personal vehicle, third party location such as cloud based storage or stored by a Company vendor; and/or
4. within your or the Company's possession, custody, or control (including personal and home computers, laptops, cell phones, and e-mail accounts, to the extent they contain documents and information that are connected or related to, or that may affect or impact, the matter(s) identified above).