BRINKS LEGAL

POLICY FOR RESPONDING TO THIRD PARTY DOCUMENT DESTRUCTION REQUESTS - WORK INSTRUCTIONS

REVISED: MAY 2021

TABLE OF CONTENTS

PURPOSE

The purpose of this work instruction is to outline the steps the Legal Department, or Corporate Development in conjunction with the Legal Department, must take to destroy (and certify the destruction, if applicable) information as a result of a contractual obligation, usually contained in a Non-Disclosure Agreement, which aligns with the Brink's Policy for Responding to Third Party Document Destruction Requests.

STEPS FOR INTERNAL CERTIFICATION

The following are the typical steps to internally certify the proper documentation has been destroyed:

1. Compile a list of Brink's employees (name and email address) who must destroy information.
2. Determine whether an electronic repository (or data room) was used to store information or documentation that is subject to the destruction/certification request and, if so, determine the contact person and owner of that repository.
3. Update the Sample Destruction Letter with the pertinent details.
4. Gain approval of the Destruction Letter from the General Counsel or VP & Associate General Counsel – Corporate Legal.
5. Send the Destruction Letter and Certification (and a copy of the Policy for Responding to Third Party Document Destruction Requests) to all employees identified in Steps 1 and 2 (usually delivered via DocuSign) with a due date and reminders.
6. Store all internally signed Destruction Certifications.
7. Once all internal Destruction Certifications are received, Brink's may sign any external documents certifying destruction to another party.

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).

SAMPLE DESTRUCTION LETTER AND CERTIFICATION

This is a sample destruction letter and certification. This should be altered by the Legal Department, or in consultation with the Legal Department, based on the exact situation.

Destruction Certification TEMPLA