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 use of Brink's information technology assets ("IT Assets") in compliance with hardware and software license agreements.

2. Policy Statement

2.1. IT Assets must be sourced or installed with the defined approvals.
2.2. Addition of IT Assets should be requested using the established local and/or country procurement processes.
2.3. IT Assets must be purchased in compliance with Brink's sourcing policy, using approved sourcing processes and engagement tools.
2.4. IT Assets must be deployed and installed by authorized personnel only. Please follow GITP-039 Global Connectivity and Field Device Policy.
2.5. IT Asset inventory must to be maintained within the Global asset management platform to properly manage its utilization, in compliance with manufacturer's/software provider's regulations.
2.6. IT Assets no longer required for business use must be decommissioned and installations removed. Copies and packages will be archived or destroyed in compliance with Brink's requirements. Support and maintenance may be canceled or contracts terminated as appropriate.
2.7. Where monitoring identifies software is not being used, this may be uninstalled and redeployed elsewhere in the organization, once the investigation has confirmed that it is no longer required. Harvesting will be carried out in compliance with vendor terms and conditions relating to redeployment and license transfer between users and devices.
2.8. IT Assets must be disposed in controlled and secure manner, in compliance with IT Security policies & procedures and Data Security obligations with Brink's customers. A certificate of destruction or data eraser is required.

2.8.1. All retired technology assets will be inventoried by the IT Department until disposal of the asset is approved.
2.8.2. All equipment containing storage media, (e.g. hard disks) must be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal or re-use.
2.8.3. Damaged storage devices containing sensitive data must be destroyed according to Brink's standards.
2.8.4. Destruction of information captured on computer storage media (such as CD-ROMs, DVD's, USB drives) must only be performed with approved destruction methods.
2.8.5. Destruction methods should correspond to the sensitivity of the data.

2.8.6. Destruction of media should be conducted only by trained and authorized personnel. Safety, hazmat, and special disposition needs should be identified and addressed prior to conducting any media destruction.

2.8.7. Verification (Restricted and Confidential Information): Verifying the selected information sanitization and disposal process is an essential step in maintaining confidentiality. A representative sampling of media should be tested for proper sanitization to assure the organization that proper protection is maintained. Verification of the process should be conducted by personnel without a stake in any part of the process.

2.8.8. Documentation (Restricted and Confidential Information): Record of sanitization should include what media were sanitized, when, how they were sanitized, and the final disposition of the media.

2.8.9. Controls: The destruction or secure overwriting of restricted and confidential information must be logged. Management is responsible for reviewing the destruction logs and performing spot checks to ensure proper disposal of all sensitive information.

2.9. Personal devices may be used to access Brink's only with specific authorization, and in compliance with Brink's bring your own device (BYOD) policy. Brink's processes for personal devices must be followed to ensure that all software accessed is correctly licensed.

2.10. The ability to download and install software is limited to authorized personnel only. Those individuals who have been given download rights must ensure that any software downloaded is appropriately licensed and managed in compliance with standard processes.

2.11. IT Assets, Hardware (Desktop, Laptop & Servers) and Software (which includes software and SaaS) used within Brink's must be approved by Enterprise Architecture, IT Infrastructure & Operations and IT Security. Also, the license terms and conditions must be approved by IT and Procurement to ensure the agreement will permit its use.

2.12. Software purchased from third parties is licensed, not owned. Brinks will use such software in compliance with the contractual terms and conditions, or end-user license agreement (EULA). This includes business systems provided by third parties that are accessed via the internet (e.g., SaaS, PaaS, IaaS).

2.13. IT Assets, Hardware and software, must be in an external (manufacturer) and internal lifecycle state. All exceptions will need to go through the risk assessment process for approval.

2.14. Development licenses may have terms and conditions different from those of standard product software licenses. Developers are expected to ensure that they understand these terms and conditions and comply with them. Development software must be used only within designated development environments.

2.15. When Brink's owns the rights to internally developed software, it may still be bound by terms and conditions relating to elements owned by third parties (including open source). It is therefore important that these are documented, and internally developed software is used in compliance with these terms and conditions.

2.16. Brink's will keep records in the Global asset management platform of entitlement data, including contracts, EULAs, purchase records and any other data that may be used to prove software and subscription use rights. As applicable, copies of license documentation to substantiate any preapproved purchases must be sent to the software asset management team or designated personnel within 30 days from the effective date of the agreement.

2.17. Brink's IT Asset Management will conduct periodic audits of hardware and software in the environment against our entitlements, including but not limited to, Software License terms and conditions, and IT Asset Management Policy

2.18. Breach of third parties copyright will be considered gross misconduct. Any suspected incidence of breach of software copyright will be dealt with in accordance with Brink's disciplinary procedures.
2.19. Upon employee separation from Brinks, all compute assets MUST be returned to their local IT Department within seven (7) business days.
2.20. Compute assets must not be redeployed or placed in storage by department. Redeployment of the compute assets will be managed by Desktop Services.
2.21. Returned equipment will be wiped from a security standpoint and physically cleaned. This process ensures proper security of the retained information and licensing of each device.
2.22. If information residing on a returned compute asset is required to be retained, a request can be submitted through the Local IT Department to retain the data for an undetermined period of time. The data retention request is to be approved by HR and Legal.
2.23. Viable compute inventory storage devices will be wiped and repurposed to fulfill new requests, and to ensure cost effective use of the assets.
2.24. All print devices within Brink's facilities will be networked on the Brinks network.
2.25. No stand alone or personal printers are permitted.
2.26. All print devices will have a standard configuration ensuring appropriate security and cost effectiveness of print environment.

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. The IT asset manager or responsible party, will ensure compliance with this policy. If necessary, the IT asset manager will be supported by local representatives, who are responsible on the IT asset manager's behalf for ensuring compliance in the respective Brink's entities.
3.3. In their duties under this policy, the IT asset manager or responsible of this role and local representatives are independent of directions by the local management. The respective management within Brink's will support the IT asset manager and the local representatives in carrying out their duties.

4. References

4.1. Principles: see GITP-001 Global Technology Policy Manual Principles document.
4.2. Related: see
GITP-039 Global Connectivity and Field Device Policy
GITP-004 Global IT Hardware Lifecycle Policy
GITP-003 Global IT Software Lifecycle Policy

4.3. A full list of controls can be found on the Brink's Resource Library.
Applicable SOX Control #:
Applicable Brink's Common Control #: 30, 23, 16, 34

5. Definitions

5.1. Types of Media:

5.1.1. Hard Copy: Hard copy media is physical representations of information. Paper printouts, printer, and facsimile ribbons, drums, and platens are all examples of hard copy media. These types of media are often the most uncontrolled. Information thrown into recycle bins and trash containers exposes a significant vulnerability to “dumpster divers”, and overcurious employees, risking accidental disclosures.

5.1.2. Electronic (or soft copy): Electronic media are the bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, and networking equipment.

5.2. Disposal Methods:

5.2.1. Disposal: Disposal exists where media are thrown out with no special disposition given to them. Disposal is a valid method for handling media containing non-confidential information.

5.2.2. Clearing: Clearing (or wiping) information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Simple deletion of items would not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. For example, overwriting is an acceptable method for clearing media. There are overwriting software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not writeable. The media type and size may also influence whether overwriting is a suitable sanitization method. Studies have shown that most of today’s media can be effectively cleared by one overwrite.

5.2.3. Purging: Purging information is a media sanitization process that protects the confidentiality of information against a laboratory attack. For some media, clearing media would not suffice for purging. However, for disk drives manufactured after 2001 (over 15 GB) the terms clearing and purging have converged. A laboratory attack would involve a threat with the resources and knowledge to use nonstandard systems to conduct data recovery attempts on media outside their normal operating environment. This type of attack involves using signal processing equipment and specially trained personnel. Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

5.2.4. Destruction: Destruction of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting. If destruction is decided upon due to the high security categorization of the information or due to environmental factors, any residual medium should be able to withstand a laboratory attack.

5.2.4.1. Disintegration, Incineration, Pulverization, and Melting: These sanitization methods are designed to completely destroy the media. They are typically carried out

at an outsourced metal destruction or incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.

5.2.4.2. Shredding: Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality level that the information cannot be reconstructed.

6. Appendices

6.1. Not Applicable

7. Authorization

This policy is authorized by:

Greg Osgood
Vice President Global IT & Shared Services

Policy Owner: Jeff Gibson, Sr. Director Global IT

Additional Stakeholders: Charles Finklea, IT Director- Global IT Service Management

Tom Weir, Sr. Director- IT Infrastructure and Operations

8. Change History

Original Issue Date: 05/26/2020

Revision	Date	Author	Revision History
1.0	05/10/2019	Ricardo Sanchez-Cortes	Initial draft
1.1	05/26/2020	Jeff Gibson	Updated to reflect existing processes
1.1	03/08/2021	Carrie Rogers	Updated Template and GRC review
1.2	10/18/21	Jeff Gibson	Review
1.2	12/21/2021	Tom Weir	Review and updates
1.2	03/03/2022	IT Service Management Team	Review and updates
1.2	03/18/2022	Mark Armour/GRC	Review and updates
1.2	03/23/2022	Jeff Gibson	Review and updates
1.2	04/18/2022	Greg Osgood	Review
1.2	04/21/2022	Charles Finklea	Review
1.2	04/25/2022	Jeff Gibson	Final review
1.2	05/04/2022	Lisa Marshall	Legal review
1.3	08/25/2022	Carrie Rogers	Updates to template