Global Information Security Procurement Policy

Document Classification: Internal Use Only

Policy No: GITP-007

Version: 1.0

Last Publish Date:
09/12/2023

1. Purpose and Scope

The Global Information Security (GIS) Department provides advice and counsel to support Brink's business and enable execution of the Company's overall Information Security strategy. This policy provides guidelines for engaging internal Brink's Global Information Security. If you have any doubt about whether a decision or activity may have information security or risk implications or warrants information security advice, please contact the Global Information Security (GIS) Department.

This policy is owned by the Global Chief Information Security Officer (CISO) of The Brink's Company ("Brink's"), who is responsible for the information security of Brink's and its subsidiaries (companies in which Brink's has a majority interest or otherwise controls). As used in this policy, the term "Company" refers to Brink's and its subsidiaries, unless otherwise specified. If you are unsure who to contact for "Global Information Security (GIS) Department approval," you should contact Global Information Security (GIS) Department. As used in this policy, the term "Security Services" refers to any information security products or services or those related to information security.

2. Policy Statement

2.1. External Information Security Usage

2.1.1. ***Engaging Outside Security Services.*** The Global Chief Information Security Officer (CISO) or their designee must approve the engagement of, and fees paid for external Information Security Services. Internal Brink's GIS, in consultation with the function or business needing external Security Services, will agree on scope and strategy of any engagement.

2.1.2. ***Consulting with Outside Security Services.*** The Global CISO or their designee shall direct and manage outside Security Services.

2.1.3. ***Review of Outside Security Services.*** The GIS Department may periodically review outside Security Services' performance and cost with reference to a particular matter or scope of work, its complexity and the level of specialty expertise required. The business or functional area for which the Security Services were performed may also be asked to review performance and cost.

2.1.4. ***Outside Security Services Guidelines.*** All engagements of outside Security Services are subject to the Company's Outside Security Services Guidelines.

2.2. Contracts

Except as provided, below, all written contracts/agreements (including amendments, supplements, or modifications of existing contracts/agreements) containing information security provisions to be executed by or on behalf of the Company or any subsidiary must be reviewed by a member of the Global Information Security (GIS) Department prior to execution. As necessary, the Global Information Security (GIS) Department should also be involved in drafting and negotiation of the information security provisions within such written agreements. The table below provides examples of written contracts/agreements that may contain information security provisions, regularly entered into by the Company and its subsidiaries.

Sample Contract/Agreement Types	
Asset Management Agreements	Letters of Intent/Indications of Interest/Memoranda of Understanding
Assignments and Novations	License/Subscription agreements
Consulting Agreements and Engagement Letter	Participation/Sponsorship Agreements
Credit Agreements	Pre-contract documents (e.g., customer bids, term sheets)
Customer Agreement Templates	Services/Sales Agreements
Indemnification Agreements	Statements of Work
Vendor/Supplier Agreements	Product Pilot/Proof of Concept Agreements

Previously Approved Form Contracts. GIS Department review is not required where the agreement is an unmodified, standard Company or industry form contract/agreement previously approved by GIS for current use after January 1st, 2023.

In certain cases, the GIS Department provides authorization to individuals to modify or amend form contracts according to pre-established guidelines and/or pre-approved amendments. You should consult with the Global Information Security (GIS) Department if you have any question as to whether this authorization is available in your country or business unit.

2.3. New Products and Services

Consistent with the Company's Stage Gate process, GIS Department approval is required before any new products or services may be marketed, offered or sold by any Brink's business unit, and before any existing products or services may be materially changed. The GIS Department must also approve the offering of any existing or new service to a new country or territory. You may consult with the GIS Department to obtain approval.

2.4. Cyber Incident Notifications

The GIS Department must be notified immediately of any known or suspected cyber security incidents in accordance with Cyber Security Incident Response Plan (CSIRP). The GIS Department is responsible for coordinating related communications to management and others so as to maintain privilege and confidentiality, where applicable.

2.5. Acquisitions and Divestitures

The GIS Department must be notified of any proposed business acquisition or divestiture and must be provided with the results of relevant due diligence for review. Any acquisition that includes information security or technology requires separate GIS Department review.

2.6. Public Disclosures and External Communications

Any proposed public disclosure or public discussion of information security matters, including cybersecurity alerts/incidents, the information security program, assessments, or controls must be approved in advance by the GIS Department.

3. Roles and Responsibilities

All employees, contractors and consultants are required to comply with this Policy. 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 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.

4. References

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

4.2. Related Referenced Document Links: Please note that you must be on the Brink's Network in the office or through VPN to access the Brink's Network Link.

- European Data Protection Policy (Brink's Network Link / Google Workspace)
- Global Data Protection Policy (Brink's Network Link / Google Workspace)
- Global Information Security (GIS) Department Organizational Chart
- Cyber Security Incident Response Plan (CSIRP) – *links coming soon*

5. Authorization

This policy is authorized by:

Kurt McMaken
Executive Vice President and Chief Financial Officer

Policy Owner: Patrick Benoit, Chief Information Security Officer

Additional Stakeholders:
Chris Parks, EVP and President, Europe, Middle East, Africa & Asia
Jamal Powell, EVP, Brink's Business System
Danny Castillo, EVP and President, North America
Dominik Bossart, EVP and President, Latin America and BGS
David Dove, EVP and President, ATM Managed Services
Lindsay Blackwood, EVP and General Counsel
Keith Barthelmeus, VP, Strategic Sourcing & CFO Product & IT
Laurent Borne, EVP and Chief Experience Officer
Neelu Sethi, SVP and Global Chief Information Officer
Ricardo Sanchez Cortes, Sr. Director, Strategic Sourcing

6. Change History

Original Publish Date: 09/12/2023

Revision	Date	Author	Revision History
1.0	02/28/2023	Patrick Benoit	Draft
1.0	03/20/2023	Carrie Rogers	Placed in current policy template
1.0	05/02/2023	Carrie Rogers	Review and minor updates
1.0	05/12/2023	Carrie Rogers	Updates to Section 6
1.0	05/16/2023	Patrick Benoit	Review and Updates
1.0	June – Aug 2023	Stakeholders	Reviews and Updates
1.0	9/11/2023	Carrie Rogers	Clean up and final copy