Global Technology Wireless LAN Configuration Policy
Document Classification: **Internal Use Only**

Policy No: GITP-015
Version: 3.3

Last Publish Date:
01/11/2023

1. Purpose and Scope

The purpose of this policy is to document the basic principles and policies that are fundamental to Brink's Global Technology in accordance with industry best practices. The policy assists in the following:

- Assuring a secure and stable technology environment,
- Managing and decreasing the risk of exposure and compromise
- Protecting and maintaining the confidentiality, integrity, and availability of digital information and related infrastructure assets.

Additionally, the policies provide the basic boundaries for more detailed procedures and standards. In the event of a conflict between these policies and applicable law, 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 Wi-Fi (Wireless LAN) access to corporate facilities.

2. Policy Statement

2.1. General Requirements:

2.1.1. Devices must be authorized to access the Brink's network domains.

2.1.2. Devices must be Brink's-managed and use approved virus protection, security patches, and personal firewalls.

2.1.3. Users must authenticate through Active Directory (AD) credentials.

2.1.4. Devices / clients must mutually authenticate via remote authentication dial-in user service (RADIUS) server through Brink's internal Certification Authority (CA) machine certificates.

2.2. Hardware:

2.2.1. All wireless devices connecting to the Brink's network must be company approved and purchased. This includes laptop computers, handheld devices, wireless access points, and any other type of equipment.

2.2.2. Wireless applications must be capable of "mutual" device and user authentication (i.e., the device, the user, and the network must recognize each to be who they say they are).

2.3. Administration: All Access Points are a point of entry into the network and must be controlled just like firewalls.

2.3.1. Wireless and wired networks must be developed and maintained separately and distinctly.

2.3.2. A firewall is required between the wired and wireless network segments if Brink's certificates are not used to authenticate the devices to the network.

2.4. Authentication: All authentication requests must be handled by an approved method such as RADIUS.

2.4.1. There must be a secure link between a device and an access point (AP).

2.4.2. Software updates and product enhancements must be downloaded to Access Points, as required, to improve performance and enhance security.

2.4.3. Access point management must include ongoing operating assessments / monitoring of the device. Malfunctions and / or loss of effectiveness must generate alerts for resolution.

2.5. Encryption: All wireless data must be encrypted per Brink's encryption standard.

2.6. Use of any unauthorized wireless equipment to access Brink's internal network, systems or data is prohibited

2.6.1. Approval must be obtained according to GIS Policy and regional IT procedures.

2.6.2. Non-approved wireless technology must be removed from the Brink's computing environment.

2.7. Compliance and Monitoring Requirements: Security assessments and audits are essential tools for checking the security posture of a wireless technology and for determining corrective action to ensure the network remains secure.

2.7.1. Regular audits must be performed using wireless diagnostic hardware and software. Administrators should periodically check for rogue access points and other unauthorized access.

2.8. Disconnect Authorization: Any wireless segment on the Brink's Network which poses a security threat, must be disconnected from the backbone network.

2.8.1. Every reasonable attempt will be made to reach the registered "Point of Contact" to resolve security problems. Authorized Regional Leadership has the authority to disconnect any wireless network from the enterprise network backbone whose traffic violates practices set forth in this policy.

2.8.2. If a serious security breach is in process, the telecommunications department and Information Security will disconnect the LAN immediately.

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. Information Technology management is responsible for reviewing and understanding the policies and ensuring that compliance is monitored and enforced within their areas of responsibility.

3.3. The policy owners must gather and communicate to the Chief Information Security Officer (CISO) information regarding major changes in policy, standards and process. The threat landscape of the company may require changes in this Policy and recommendations for changes.

4. References

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

4.2. Related: GITP-008 Global Information Security Management 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 #: 43, 23, 25

5. Definitions

5.1. Not Applicable

6. Appendices

6.1. Not Applicable

7. Authorization

This policy is authorized by:

Greg Osgood
Vice President Global IT & Shared Services

Policy Owner: Chris Foley, Sr. IT Manager

Additional Stakeholders: Ron Banks, Director, Information Security

8. Change History

Original Issue Date: 11/17/2016

Revision	Date	Author	Revision History / Purpose of Change
2.1	11/17/2016	David Armato	No changes.
2.2	05/17/2018	Huan Do	No changes.
3.0	11/26/2019	Angel Mosley	Changes to reflect new compliance requirements

3.1	05/26/2020	Chris Foley;
		IT Compliance;
		Legal
			Review and update policy

3.1	03/04/2021	Carrie Rogers	GRC review and update to current template
3.2	04/13/2021	Angel Mosley	Updated Wireless Data Encryption Standard
3.3	08/08/2022	Carrie Rogers	Review
3.3	08/25/2022	Carrie Rogers	Update of template

3.3	09/08/2022	Chris Foley	Review; No Changes
3.3	10/27/2022	Ron Banks & Angel Mosley	Review
3.3	12/06/2022	Mark Armour	GRC Review
3.3	12/19/2022	Greg Osgood	Review
3.3	01/10/2023	Lisa Marshall	Global Ethics and Compliance Review and Approval