Table of Contents

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:

- Foster 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 legal entities, employees, contractors, and vendors doing business on behalf of Brink's.

The scope of this policy is to establish an organization-wide standardized framework of information security policies to ensure the monitoring, detection, prevention, response to, and investigation of cybersecurity issues and misuse, cybersecurity misconfiguration, vulnerability, or threat to Brink's information technology assets. Additionally, this policy is meant to facilitate Brinks' overall cybersecurity posture and to provide a baseline for measurement across all the entities within the company.

Adherence to information security policies will safeguard the integrity, confidentiality, and availability of Brink's information and protect the interests of its personnel and business partners. The implementation of the requirements set forth in this policy aims to reduce the risk that information assets, either accidentally or intentionally, are disclosed, modified, destroyed, or used in an unauthorized manner. Any deviations from this policy must have an approved policy exception.

2. Policy Statement

2.1. Acceptable Use

Brink's information system resources must be used in an approved and lawful manner, in accordance with Brinks Code of Ethics.

- Brink's-owned systems and office equipment are to be used for business purposes.
- Personal use of Brink's technology equipment is permitted on a limited or incidental basis and consistent with this policy. Personal use must not interfere with work.
- Use of Brink's information system resources constitutes permission for Brink's to monitor those resources for compliance and proper usage.
- Data created on corporate systems remains the property of Brink's. Except where required by law and regulation, management cannot guarantee the personal privacy of information stored on any network device belonging to Brink's.
- Only software that has been specifically licensed and authorized for business use may be installed on Brink's-owned computer equipment.
- All media provided by third parties must be checked for viruses before being introduced to Brink's computers or servers.
- Users should never connect public Wi-Fi networks to their corporate networks.

2.2. Prohibited Use

Users are prohibited from using Brink's information system resources (including servers, laptops, and mobile devices) for purposes other than those specifically authorized by their respective organization and in accordance with job responsibility. Brink's-owned systems and office equipment must not be used for prohibited activities, including but not limited to, the following:

- Any unauthorized purpose, including, but not limited to, gaining unauthorized access to other systems; disseminating any discriminatory or hate-based materials or speech; or reproducing or distributing copyrighted, trademarked, proprietary, or export-controlled data, software, pictures, music, and video.
- Exporting or importing software, technical information, unauthorized encryption software, or technology in violation of international or regional export control laws.
- To perform activities intended to circumvent security or access controls of any organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, and decrypt encrypted files, or compromise information security by any other means. Such activities include, but are not limited to, the use of private VPNs and TOR Peer-to-Peer Networks and Proxy Avoidance.
- Unsafe/uncertified data handling practices which may result in a security compromise to either Brink's or other Data Owners, including, but not limited to, unauthorized data access, servers, or privileged accounts; circumventing user authentication on any device; or interception of network traffic.
- Causing a disruption of service to either Brink's or other network resources.
- Intentionally or unintentionally introducing malicious code, including, but not limited to, scripts, viruses, worms, Trojan horses, email bombs, spyware, adware, and key loggers.
- Port scanning or security scanning on a production network unless authorized in advance by Global Information Security (GIS).
- Attachment of non-approved network devices, thereby violating the Network Resource Administrative Access Policy.
- Activity in violation of Brinks' Code of Ethics.
- The disclosure of any Brink's information that is not otherwise public.
- Personal profit through private commercial transactions.
- Conduct activity in violation of intellectual property rights; using peer-to-peer software or services to engage in file-sharing, media downloading, etc., of unlicensed material is strictly prohibited.
- Store or transmit Restricted and Confidential data (including personally identifiable and customer data), critical or commercially sensitive information without prior authorization.
- Store Brink's data on a Brink's device that is not controlled by IT and protected by strong encryption.
- Store Brink's data on personal devices including, but not limited to, USB drives, external hard drives, CDs/DVDs, mobile phones, etc.
- Disclose Brink's data onto the Internet via any method including file transfers, email, social media posting, etc. without prior authorization.
- Make misrepresentations or express personal opinions on behalf of the company.
- Distribute information that can negatively affect the reputation of any users or of the company or its relations with its customers.
- Intentionally participate in activity that could introduce any type of vulnerability to Brink's systems, network, or equipment.

- Create, send, or forward chain letters or joke emails. Users who receive any emails with this content from any Brink's user must report the matter to their supervisor immediately.
- Perform unofficial activities that may degrade the performance of or access to information system resources, such as playing unapproved or personal electronic games.
- Store, transmit or process any material that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, Brink's, the recipient, the sender, or any other person.
- Download or distribute unauthorized software (music, video, applications, etc.) from the Internet.
- Use hardware or software tools whose functionality allows the exploitation of vulnerabilities, or the compromise of security, or the systems of other users. Incidents that involve the unauthorized use of these tools or the unauthorized attempt to compromise the security measures of information system resources will be considered serious violations of Brink's policies.
- Use of Brink's office equipment in violation or excess of the limited personal use permitted by this policy may result in limitations on future use, administrative action, criminal penalty, and personal financial liability. Users are responsible for exercising good judgment regarding the reasonableness of personal use.
- Auto-forwarding rules in Outlook will be prohibited. For valid business cases, auto forwarding can be requested through a service request.

2.3. Access, Authentication and Authorization Controls

Access controls prevent persons entitled to use a data processing system from accessing data beyond their authorizations. Access controls typically consist of login accounts and passwords set up directly on the resource to be accessed but may include tokens or other authentication mechanism incorporated in their local identity andaccess management system.

Access to Information System Resources

- Access to information system resources requires proper authorization from the manager of the respective area.
- Unauthorized access, use, destruction, disclosure, displacement, manipulation, or concealment of Brink's data is prohibited and can result in termination.
- The establishment of connections to third-parties for the purpose of sharing Brink's information and/or connection to external communications systems must have prior approval from Global Information Security (GIS).
- The transfers of Restricted Data to third parties shall be subject to written agreements in accordance with Brink's standard third party terms and conditions.
- Access to the Internet or Brink's resources is made on a case-by-case basis and made available only to authorized personnel.

Revoking Access / Departing Personnel

- **Voluntary Termination** - When personnel leave under no adverse circumstances, the individual's manager, supervisor, or company official (for contractors/suppliers) must ensure thefollowing:
    - All accountable items and other computer-related equipment are returned.

The individual's computer log-on ID, building and information system access permissions are terminated upon departure, unless needed in the new assignment.
- All Restricted, Confidential, and Internal information be returned, destroyed, or transferred to the custody of another authorized individual.

- **Involuntary or Immediate Termination** - When personnel leave under adverse circumstances, the individual's manager, supervisor, or company official (for contractors/suppliers) must ensure the following:
  - The individual's computer log-on ID, building and information system access permissions are removed immediately.
  - That the individual is always supervised while in any locationthat provides access to Brink's information system resources, property, or personnel.
  - That all computer passwords, access codes, badge readerprogramming, and physical locks used by the individual are changed or disabled prior to release of the individual.
  - Recover accountable items and all Restricted, Confidential, and Internal UseOnly information in the custody of the individual being terminated.
  - Attempt to securely disable and/or lock any accountable item that cannot be recovered.
  - Destroy or transfer Restricted, Confidential, and Internal Use Only information to anauthorized individual.

- **Privileged Access User Departure** - Any departure of a system, network, or database administrator, or developer requires immediate account revocation. Information system resources used by the departing individual must be monitored for improper use or access. The manager,supervisor, or company official (for contractors/suppliers) of the departing individual must:
  - Follow the requirements documented above for routine separation or for adverse termination.
  - Reconfigure access and distribution lists to remove the departed individual's accounts.
  - Disable access or change passwords and remove secondary authentication factors registered to the user for all shared devices, shared services, applications, and privileged accounts.
  - Disable physical access to buildings, systems, and information associated with the departed administrator's former access.
  - Monitor all privileged accounts for usage and access to the systems, applications, and databases formerly under the administrator's control to ensure all access has been removed.
  - Review records for Brink's information approved for removal offsite and make appropriate efforts to recover information and/or equipment as applicable. Notify GIS of any information identified as removed but not recovered.
  - Break glass account passwords associated to the individual need to be rotated.

- **Employee Transfers / Role Change**
  When individuals change roles, access rights to Brink's Information system resources must be modified or revoked in accordance with the new role as of the effective date of the change. When an employee switches roles, their new manager needs to notify them if previous access needs to be kept or removed within 10

business days.

Account Access Controls

Access to information system resources is managed using multiple types of accounts:

- **User Accounts** provide a minimum level of information systemresources and application functionality needed to perform the user's business function. This includes limited access accounts that exist for a specific purpose (e.g., an auditor account).
  - Application accounts must not include system or administrator privileges, unless required for business reasons.
  - Platform user accounts (i.e., database and operating system) are used to accessplatform-level resources and are limited to non-privileged access rights.
  - Accounts must use multi-factor authentication when remotely accessing applications or systems.
  - New user accounts must be approved by the employee's or resource's manager.

- **Service Accounts** are assigned to an information system resource (e.g., server, application) or automated service to process data and/or perform actions/ requests. Service Accounts:
  - Must not use the same service account name and password in bothproduction and non-production environments.
  - Must be placed under management control.
  - Must be created with the minimum access rights and privilegesrequired to perform the necessary business function.
  - Must not be allowed root or administrative privileges.
  - Must be managed by the Brink's entity responsible for the life cycle of the account from creation, deployment, usage, and retirement.
  - Passwords must be changed annually.
  - Must be non-interactive.
  - Must be approved by Global IT Engineering.
  - Service Accounts associated to the Brink's Forest must be vaulted (Domain and Local).

- **Shared Accounts have a single log-on ID and password used by more than one individual (not an automated process/service).** Shared accounts are discouraged and require the approval of management and GIS. Shared IDs must be granted read-only or minimal privileges commensurate with a least-privilege user account.
  - The use of shared accounts must be tracked (e.g., logged) to manage individual accountability through a PAM solution.
  - The requesting manager is responsible for undocumented usage of shared accounts.
  - System operators must not share identification or authentication materials of any kind, nor allow any other person to operate any information system resources by employing that user's identity. Shared accounts must not be used to administer production system components except for an emergency.

- **Privileged Accounts** (e.g., administrator or maintenance accounts) enable users to

change data, alter configuration settings, run programs, or permit unrestricted access to view data. Assignment must be restricted to a unique individual whose duties require these privileges (e.g., system, network, database administrators)

- Privileged accounts include, but are not limited to, Enterprise Admins, Schema Admins, Domain Admins, Administrators, Account Operators, Server Operators, Print Operators,and Backup Operators.
- Absent of technical limitation preventing it, administrative accounts must be managed by our Privileged Access Management (PAM) solution.
- Permission inheritance must be disabled for all privileged accounts.
- Access to privileged accounts must be secured with Multi-factor Authentication.
- An audit trail must bemaintained for all privileged account usage.
- Privileged accounts must be labeled using the following schema to identify access type:

  - –A – Administrator elevated account
  - –B – Elevated Support Desk account (no Domain Admin privileges)
  - –D – Application Support for Production Support (i.e., KTLO)
  - –E – Firecall ID for Application Development and Level 3 processes; ID mustremain disabled except while in use. See Firecall Policy for additional information.
  - –F – DTS (Desktop Services) elevated account (no domain admin)
  - –P – Privileged accounts not dedicated to administrators, support, or Firecall

- Sudo (super-user do) access has higher levels of rights, such as account creation/update/deletion,full application/platform functionality, or a subset of rights that have been designated as privileged. Sudo Access:
  - Must be restricted to a unique individual whose duties require these additional privileges.
  - Use is restricted to performing those job functions required by the privileged access - individuals must use regular user accounts to perform non-privileged functions.

- Test Accounts are accounts used for testing purposes only and assigned to an individual (not an automated process/service). Test accounts:
  - Must be set with an expiration of 30 days upon creation. Extensionsmust be documented and approved by GIS.
  - May not remain active for more than one (1) year.
  - Must be approved by GIS prior to account creation.

Identification

Identification is the process of associating a person or information system resource with a unique enterprise-wide identifier (e.g., a user log-on ID). The log-on ID is used in conjunction with other security services, such as authentication. Log-on IDs must be protected in accordance with the following:

- Personnel must not share their log-on IDs or permit others to use them.
- Log-on IDs must not be embedded in application code, batch files or stored in application files or tables.
- Log-on IDs must be used as the primary means of identification.
- A log-on ID must not exist without associated authentication information.

- Log-on IDs must be suspended for a period of at least thirty (30) minutes after five (5) unsuccessful login attempts. If the log-on ID or account does not unsuspend itself after the suspension period, the user must use Password Reset procedures or follow defined local procedures for resolution.
- Log-on IDs not used for a period of 90 days or more must be disabled.
- Failed log-on attempts must be recorded.
- The reason for the failed log-on attempts and information previously entered must not be disclosed to the user.

Authentication

Authentication is the process of verifying the claimed identity of an individual, workstation, or originator. Identification is accomplished through a log-on ID while authentication is achieved when auser provides the correct password, personal identification number (PIN), or other authenticator(s) associated with that identifier.

Personnel must be required to identify and authenticate themselves to the information system resourcebefore being allowed to perform any actions. Means of authentication include the following:

- Passwords
- Personal identification numbers
- Shared secrets
- Digital certificates and signatures
- Smart cards and tokens
- Biometrics

Authorization

Brink's information system resources must comply with authorization requirements, including:

- Use of a centralized authorization system to control access.
- Access to resources is not allowed without invoking the authorization process and checking the assigned rights and privileges of the authenticated user.
- The use of features to assign user privileges (i.e., access permissions) to log-on IDs, roles, groups, and other information system resources.
- Privileges (e.g., computing devices, consoles, terminals, and subsidiary networks) must not allow the user to bypass or upgrade his or her privileges established in centralized access control lists or databases.
- The capability to restrict session establishment based on the time of day, day of the week, calendar date of the login, and source of the connection. Information system resources running on operating systems that do not have these capabilities must implement compensating controls (e.g., monitoring devices).
- The administrator-configurable capability to limit the number of concurrent log-on sessions for a given user.
- Mechanisms to bypass authorization restrictions must not be allowed.
- Access must be accurately reflected in the system of record and must not extend beyond the pre-established role definitions.
- Access by computing devices from remote, non-Brink's locations must authenticate before access is granted.

Non-Repudiation

Authentication and non-repudiation together are the process of associating any action on the information system resource with one and only one user, process, or other information system resource and is essential for maintaining minimum levels of information security.

Each user or information system resource (e.g., a workstation or terminal) is associated with any action on an information system resource. Individual non-repudiation is established byissuing a unique user or log-on identifier (i.e., user ID or log-on ID). Machine non-repudiation may be established for a specific information system resource through its workstation certificate. All information system resources must be capable of individual accountability and do the following:

- Identify information system resources each time an attempt is made to log-on to the system.
- Verify that information system resources are authorized to use the system.
- Associate all actions taken by an information system resource with that resource's unique identifier (i.e., resource ID or log-on ID).

Account Management

Restricted and Confidential information system resource access must be limited by Role Based Access Controls (RBAC) in a manner that is sufficient to support approved business functions.

All accounts must be established in a manner that ensures access is granted based on role-based access controls, separation of duties, and least privilege basis. Accounts unused for 90 days must be disabled. Accounts unused for one (1) year must be deleted.

Separation of Duties

Personnel must not be assigned duties that could cause a conflict of interest or present an undetectable opportunity for wrongdoing, fraud, or collusion. Separation of duties and responsibilities are considered when defining roles. For special situations where additional control is required, dual authorization can be implemented.

Only authorized personnel are approved for access to Brink's information system resources. This approval must be specific to an individual's roles and responsibilities in the performance of his or her duties and must specify the type of access (e.g., read, write, delete, and execute); specific resources and information; and time periods for which the approval is valid.

Least Privilege

Information system resource access is based on providing personnel with the minimum level of information system resources and system functionality needed to perform their duties. Systems and applications must define as many levels of access as necessary to prevent misuse of system resources and protect the integrity, availability, and confidentiality of Brink's information. Brink's information system resources must be capable of imposing access controls based on specific functions (e.g., create, read, update, delete, and execute).

Periodic Review of Access Authorization

Managers must review access granted to personnel under their supervision to ensure that access is still required for personnel to perform their duties. Refer to Access Review Procedure document for frequency and processes.

2.4. Password

Passwords are unique strings of characters that personnel or information system resources provide in conjunction with a log-on ID to gain access to an information system resource. All passwords must follow the security standards outlined below for Brink's internal users:

- All default system passwords must be changed immediately upon implementation into any production environment.

- For Active Directory accounts:
  - All user account passwords for Active Directory and those applications integrated with Active Directory must consist of at least fifteen (15) characters.
  - User accounts not used for at least 90 days should be disabled.
  - User password history must be stored, and the system configured to prevent the reuse of the previous eight (8) passwords.
  - Accounts must be disabled for a minimum of 30 minutes following five (5) failed log-in attempts.
  - Active sessions must expire after 15 minutes of inactivity.
  - Passwords must not contain any part of the user's full name.
  - Passwords cannot match the Login ID / username.
  - The password must not contain more than two (2) consecutive repeat characters.
  - Initial passwords for users must be sent via protected electronic delivery system or personal delivery to the user (First Class Mail is also acceptable). For all accounts, the initial password must be set to a temporary password, and the user must be required to change the password at log-on and upon subsequent password resets.
    - Note: Caution must be taken not to standardize on generic or global passwords when issuing new accounts or when resetting forgotten passwords.
    - New hire passwords must be sent by email to the hiring manager and separate from the User Network ID Information.

- For those systems not integrated with Active Directory, including applications, databases and operating systems:
  - All user account passwords must consist of at least eight (8) characters.
  - Passwords must be changed at least every 90 days or less.
  - User accounts not used for at least 90 days should be disabled.
  - Password history must be stored, and the system configured to prevent the reuse of the previous eight (8) passwords.
  - Accounts must be disabled for a minimum of 30 minutes following five (5) incorrect log-in attempts. and locked for 10 seconds for each failed attempt.
  - Active sessions must expire after 15 minutes of inactivity.
  - Passwords must not contain any part of the user's full name.
  - Passwords cannot match the Login ID / username.
  - The password must not contain more than two (2) consecutive repeat characters.
  - Initial passwords for users must be sent via protected electronic delivery system or personal delivery to the user (First Class Mail is also acceptable). For all accounts, the initial password must be set to a temporary password, and the user must be required to change the password at log-on and upon subsequent password resets.

- Note: Caution must be taken not to standardize on generic or global passwords when issuing new accounts or when resetting forgotten passwords.
- New hire passwords must be sent by email to the hiring manager and separate from the User Network ID Information.

- All passwords must contain characters from at least 3 of the 4 main character sets:
  - Uppercase alphabetical. English uppercase letters (A–Z)
  - Lowercase alphabetical. English lowercase letters (a–z)
  - Numerical. Westernized Arabic numerals (0–9)
  - Special Characters (non-alphanumeric) character (i.e., &,#, and $)

- Password reset:
  - Requests for password changes require verification of user's identity prior to providing atemporary or replacement password.
  - User passwords must change following a data breach or known fraudulent activity.

Protection of Passwords

Passwords must be treated as sensitive information and never disclosed. In addition:

- Passwords must be encrypted in transmission.
- Passwords must be masked as part of the authentication process.
- Passwords must not be inserted into email messages or other forms of electronic communication, nor should they be written down.
- Unencrypted passwords may not be stored on ANY computer system.
- Brink's passwords must never be shared with anyone.
- If someone demands a password, refer them to this policy, a local IT Manager, or GIS

Personal Identification Numbers

PINs are a specialized type of authenticator that are used in conjunction with unique identifiers to verify the identity of users before allowing them access to information system resources. To ensure that PINs retain integrity and confidentiality, PINs must be protected during generation and dissemination. All personnel are encouraged to change their PIN from the initial assignment. PINs must:

- Be a minimum of four characters in length, two of which are unique.
- Not be obvious combinations or sequences.
- Not be well-known or easily guessed combinations (e.g., social security number, telephone number, and house address).

Password Storage

Passwords must be stored in one-way encrypted format where possible. Passwords stored in batch files,automatic log-in scripts, software macros, keyboard function keys, or computers without access control systems must be encrypted using the Brink's encryption standard.

For Non-Privileged External Users (i.e. Customer facing applications), passwords must adhere to the following:

- User passwords must consist of at least seven (7) characters.
- All passwords must contain characters from at least 3 of the 4 main character sets:
    - Uppercase alphabetical. English uppercase letters (A–Z)
    - Lowercase alphabetical. English lowercase letters (a–z)
    - Numerical. Westernized Arabic numerals (0–9)
    - Special Characters (non-alphanumeric) character (i.e., &,#, and $)
- User password history must be stored and the system configured to prevent the reuse of the previous eight (8) passwords.
- Accounts must be disabled for a minimum of 30 minutes following five (5) failed log-inattempts.
- Active sessions must expire after 15 minutes of inactivity.
- Passwords must not contain the user's name or any part of the user's full name.
- Passwords cannot match the Login ID / username.
- The password must not contain more than two (2) consecutive repeat characters.
- Initial passwords for users must be sent via protected electronic delivery system or personal delivery to the user (First Class Mail is also acceptable).
- For all accounts, the initial password must be set to a temporary password, and the user must be required to change the password at log-on and upon subsequent password resets.
    - Note: Caution must be taken not to standardize on generic or global passwords when issuing new passwords or when resetting forgotten passwords.
- Password reset:
    - Requests for password changes require verification of user's identity prior to providing a temporary or replacement password.
    - User passwords must change following a data breach or known fraudulent activity.
- **Protection of Passwords**:

  Passwords must be treated as sensitive information and never disclosed. In addition:
    - Passwords must be encrypted in transmissions.
    - Passwords must be masked as part of the authentication process.
    - Passwords must not be inserted into email messages or other forms of electronic communication, nor should they be written down.
    - Unencrypted passwords may not be stored on ANY computer system
    - Passwords must never be stored in clear text
    - Brink's passwords must never be shared with anyone
    - If someone demands a password, refer them to this policy, a local IT Manager, or GIS

- Password Storage: Passwords must be stored in one-way encrypted format where possible. Passwords stored in batch files, automatic log-in scripts, software macros, keyboard function keys, or computers without access control systems must be encrypted using the Brink's encryption standard.

2.5. Encryption and Key Management

The following sections cover the standard cryptographic algorithms for protecting information assets from unauthorized disclosure and tampering during various forms of connectivity, communication, access, and storage. Various categories with underlying scenarios are detailed where application of cryptography is necessary to safeguard information assets. The encryption algorithms and cryptographic modules outlined in this standard are aligned with FIPS 140-2 suite and FIPS 197. The methods listed below should be adhered to where technically feasible.

Classes of Cryptographic Algorithms – There are basic classes of cryptographic algorithms. These algorithms and their acceptable key sizes are outlined below. Where applicable, preferred algorithms are specified.

- Symmetric Encryption Algorithms: used in secret key cryptography. A single secret key is used for the encryption and decryption of messages. Used mostly for message payload encryption.

Algorithm	Acceptable Key Sizes (bits)
AES – Advanced Encryption Standards	128,192, or 256
CAST-128	128
RC4 (prior approval required)	128 or higher
RC5	128 or higher
RC6	128 or higher
IDEA (prior approval required)	128

  - RC4 may not be used without compensating controls.

- Asymmetric Encryption Algorithms: require the use of public and private key pairs. The private key is secret and the public key is known. This type of encryption is primarily used for key protection and management.

Algorithm	Acceptable Key Sizes (bits)
RSA (Required)	2048
DSA (prior approval required)	2048

  - DSA use may cause issues in OpenSSH v7.0 and higher. Upgrading openSSH from older versions cause users to be locked out.

- Cryptographic Hash Algorithms: take an input of arbitrary length and output of a fixed value. Hash algorithms are ideally suited for protecting passwords in storage. All passwords must be stored in Salted Hashed form.

Algorithm	Output Digest (bits)
SHA-1 **(prior approval required)**	160
SHA-2 (Strongly Preferred)	224, 256, 384, 512, respectively
SHA-3	224, 256, 384, 512, respectively

- SHA-2 (SHA256) or SHA-3 must be utilized whenever technically feasible.
- Applications must not use the MD-5 Hash algorithm. The SHA-1 algorithm may not be used without compensating controls or documented approval.

- **Data at Rest**: Confidential and Restricted information stored in data systems, databases andnetwork storage must be protected from unauthorized disclosure. The following sections outline the standard practice in these areas:
  - Application Development Platform: FIPS certified cryptographic frameworks and modulesmust be used where available. These are normally a component of the operating system or Middleware. Use of open-source cryptographic providers is not permitted, unless approved by GIS. The following frameworks shown employ these modules.

Development/Platform	Security Framework
Java/All	JCE (approved providers only)
C,C++/Solaris	Solaris Crypto Framework
C,C++/AIX	Aix Crypto Framework
.Net/Windows	.Net Security Framework

- Electronic Transportable Media Encryption: Confidential and Restricted information must be encrypted prior to being copied to Electronic Transportable Media devices such as CD, DVD, USB storage, etc. Software products utilizing one of the algorithms identified above orother approved FIPS compliant encryption methods are acceptable. Encryption of any transportable media containing Confidential or propriety information must conform to the NIST Special Publication 800-111 for data at rest on portable devices.

- Database Encryption is required when technically feasible for Confidential and Restricted information. The encryption for any database containing ePHI must conform to the specifications of the NIST Special Publication 800-111 for data at rest. The following database platforms and encryption shown are acceptable.

Database Platform	Encryption
Oracle	Advance Security Options
MS SQL Server	EFS Encryption Algorithms indicated above
Other Databases	Advance Security Options

- The use of vendor specific encryption algorithms is strictly forbidden. Legacy environments using vendor specific algorithms must be reviewed by IRM obtain necessary approval.

- **Data in Transit**: Confidential and Restricted information traversing any network link must be protected. Protected Health Information (PHI) transmitted outside of Brink's network must conform to the specifications of FIPS 140-2 and must support a path to FIPS 140-3 compliance.

  The following outlines the various scenarios and acceptable encryption techniques:
  - Server to Server communication: Brink's requires all communication of Confidential and Restricted information over public networks (e.g., the Internet) be encrypted using an approved algorithm during transmission. The followingtable outlines acceptable encryption technologies, standards, and APIs:

Application Platform	Encryption
Windows	TLSv1.2 or TLSv1.3
Unix	TLSv1.2 or TLSv1.3
Web Services	SODBC, JDBC over SSL, LDAP over SSL, WS-Security, JSSE
Cloud	All cloud data must be encrypted according to Brink's standards.

  - User desktops: must access applications using the encryption methodsshown below:

User Environment	Encryption
Windows	TLSv1.2 or TLSv1.3
Unix	TLSv1.2 or TLSv1.3, SSHv2

  - File Transfer: the following encryptionmethods must be used when transmitting Confidential and Restricted information:

Platforms	Encryption
All	FTPS, SFTP, SSHv2, FTP over IPSec

  - Secure Email Communication: The below approved encryption solutions must be used when sending emails:

Platforms	Secure E-Mail Solutions
Exchange	PGP, Ironport, Zip with 12-digit password

  - TLS technology used to encrypt transmission links must adhere to the following guidelines:
    - TLSv2 must be enabled at minimum.
    - Weak ciphers suites (key sizes of less than 256 bits) must be disabled

on all communication endpoints.
- SSL endpoints must use x.509 certificates issued by approved CertificateAuthorities.
- Client authentication (i.e SSL mutual authentication) must be utilized for applications that transmit Confidential and Restricted information over the public internet.
- For applications that hold customer data, the client and server should perform certificate path validation to ensure that the other party's certificate has be issuedby a trusted CA and CRL checking to determine the revocation status of the other party's certificate.
- The client should perform Hostname Verification to ensure that the domain name ofthe server (as contained in the URL) matches the subject of the server's X.509 certificate.

- **Encryption Certificates**: Use of self-signed X.509 server certificates is not acceptable. An approvedCertificate Authority must be used to generate all server certificates. All certificates must pass certificate path validation tests and CRL revocation checking.

- **Encryption Key Management:** The following must be adhered to for proper key management.

  - Generation
    - The mechanism employed for key generation must employ dual controls such thatcreation and validation are conducted by two separate individuals.
    - Complete key must not be maintained by a single entity or department and distributedbetween two groups with separate and distinct reporting structures.
    - The keys generated must employ an encryption algorithm indicated above and ensure atleast 128 bits to establish strong encryption.
    - Separate keys must be used for each environment, such as development, test, andproduction.
    - GIS must be engaged for all key managementsolution implementations.
  - Distribution
    - A secure, encrypted key distribution method must be used to distribute keys.
    - Email distribution should only be used internally out of necessity and not indicated within the subject line.
    - Access must be restricted to the fewest number of custodians necessary. Logical (systemic) and physical access to keys must be minimized.
    - Key custodians are required to sign a form stating that they understand and accept their key-custodian responsibilities.
  - Storage
    - Key stores must protect against compromise and tampering and provide integrity and access controls.
    - Encrypted storage must be used and may not be open or publicly accessible or in easily readable format (e.g., simply browsing a file).
    - Access to key storage must employ the principle of least privilege.
    - Store keys in the fewest possible locations.
    - Key documentation must be shared with GIS for storage at a separate facility for disaster recovery purposes.
    - Key Encrypting Keys must be stored separately from Data Encrypting Keys.
    - The keys must not be stored within application business logic.

- Renewal and Recovery
  - A key renewal process is required and define lifetime based onthe criticality of information and risk.
  - Keys which undergo processes that require Key Access by any user or custodian must have a shorter lifespan than Non-Accessed keys, with the maximum lifetime ofa given key not to exceed a year.
  - In cases where a technology or process requires a “key recovery” mechanism, the key recovery decisions must be carefully assessed regarding the need for renewal; the criticality of the protected data; the ownership of the keys, and; keyring access rights.
- Revocation and disposal
  - Processes must be in place which enable the easy invalidation of keys in the event ofa suspected compromise or as part of routine key management.
  - In the event of an unscheduled revocation of a key, appropriate notification identifying the keying material, the date and time of revocation, and the reason forrevocation must be communicated.
  - Key Supersession routines must incorporate an inventory or log identifying each keyand their supersession rate.
  - The disposal of old keys must ensure destruction of the keys in the manner that alltraces of keying information are irrecoverable.
  - Disposal of old keys stored on portable media must follow the electronic mediadisposal policy.
  - Printed keys must be disposed of by following company practice for disposing Confidential and Restricted information. Data which has been encrypted by an expiring key must be deciphered and then re-encrypted withcurrent encryption methods prior to disposal of old key(s).

2.6. Network Security

The networking components of Brink’s infrastructure must be protected at a level commensurate to its value to Brink’s. Protection must include the implementation of physical, administrative, and technical security controls and processes.

Network Security Requirements

- Networking asset components must be inventoried at regular intervals and labeled for asset management and physical protection.
- Information system resources supported by networking must be hardened to meet or exceed security requirements specific to each platform.
- Network information including such as configurations, addresses, subnet masks, secure enclave locations, and firewalls must be protected and treated as Internal Use Only.
- Access to network configuration information must be based upon the security principles of need to know and least privilege.
- Access to networking components must be done from a fully auditable centralized bastion host.
- All administration must be performed over an encrypted connection.
- The network must be compartmentalized and segmented, so servers and users do not occupy the same segment.

- Security measures for lower environments are subject to a similar level of control as the production environment.
- Networking components must be maintained with the appropriate security patches or upgrades.
- Networking components must be monitored at all times to ensure proper configuration and security.
- If network operations are contracted to a third party, Brink's must have the ability to monitor networking components.
- Only required network services will be enabled. Network services not needed will be disabled.
- Use of VPN is required for connectivity from public Wi-Fi networks.
- Connectivity to corporate IT resources must be secured with two-factor authentication for remote access into corporate networks.
- Remote access to the network must be authorized and approved by Network Management and Information Security and implemented according to stated standards.
- Connections between the Brink's network and any other network must traverse a Brink's firewall.
- A DMZ (Demilitarized Zone) must be used for any Brink's equipment exposed to non-Brink's networks.
- Adequate audit procedures must be employed to monitor and analyze network integrity.
- Administrative access to the network must be auditable based on to defined Brink's standards.
- Externally accessible web services must be protected through the following requirements:
    - Hardening standards
    - Vulnerability scans, penetration testing, and vulnerability assessments
    - Audit logs
    - Web application firewall (WAF)
    - Automation/bot defense solution
    - (Distributed) Denial of service protection ((D)DOS

2.7. Cloud Computing

This policy statement provides guidelines for use and evaluation of any cloud computing service such as cloud-based email, application, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

Cloud Computing Policy Statements:

- Use of cloud computing services for work purposes must be formally authorized by the Global Chief Information Security Officer (CISO). All security, privacy, and IT management requirements must be adequately addressed by the cloud computing vendor.
- Cloud services agreements that require users to agree to terms of service must be approved by the CISO and Compliance attorney/counsel.
- Services must comply with the existing Acceptable Use, Computer Usage, Internet Usage and Mobile Device Management.
- Employees must not share log-in credentials.
- GIS will decide what data may or may not be stored in the Cloud.
- Personal cloud service accounts may not be used for the storage of company-related communications.

2.8. Viruses and Malware Control (Anti-Virus)

All Brink's information system resources must be protected against the introduction of viruses and other types of malicious code.

- Computers attached to the Brink's network must run Brink's provided standard and supported anti-virus software. Software must be active and configured to perform scheduled virus checks at preset regular intervals.
- Users must not deactivate anti-virus software or manipulate the configuration of their equipment.
- The anti-virus / endpoint detection and response software requires internet connectivity. In the event an internet connection is unavailable, a local database must be utilized.
- Anti-virus software must be kept as current as possible. Versions must be reviewed at least annually to ensure it is current and supported by the vendor.
- IT must monitor for new updates and ensure virus definitions are applied as soon as they become available.
- If an employee receives what they believe to be a virus, or suspects that a computer is infected with a virus, they must report such incident to their local IT representative immediately. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.
- Employees must not destroy or remove a virus, or any evidence of the virus, without direction from local or regional IT Management.
- Infected computers will be removed from the network until it is verified as virus-free.
- If an update cannot be applied immediately, other means must be enlisted to prevent system compromise. This may include monitoring system logs, applying tighter security, disconnecting devices from network, or shutting down the system.
- No Change Control is required for anti-virus definition updates.

2.9. Physical and Environmental Security

Brink's protects its information system resources through sound physical, environmental, and administrative security controls. Physical and Environmental Security is a shared responsibility between Brink's GIS and Brink's Physical and Branch Security.

Where possible, all information system resources (including portable information system resources) must reside in a protected environment. Physical and administrative security controls must be implemented at each facility to protect against unauthorized personnel access and to protect the physical integrity of Brink's information system resources located at the facility.

Additional physical access security mechanisms (e.g., locked cabinet or desk, portable device cable lock, and biometric workstation lock) must be implemented for information system resources processing Restricted, Confidential, or Internal information.

Restricted, Confidential, and Internal information stored on removable devices or media must be stored in a controlled area or in a locked cabinet.

2.10. Clear Desk and Workstation Security

Clear Desk policy standards are part of industry best practices for confidentiality and privacy controls. The following is applicable to remote/home offices, corporate and branch offices.

- Employees and contractors are required to ensure that Confidential information in hardcopy or electronic form be secured.
- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut down at the end of each workday.
- Cabinets containing Restricted or Confidential information must be locked when unattended.
- Keys used for access to Restricted or Confidential Information must not be left at an unattended desk.
- Laptops and tablets must be secured by a security cable, locked in a secure location or kept with the employee.
- Passwords must not be written down in an accessible location.
- Printouts containing Restricted or Confidential information must be removed from printers.
- Restricted or Confidential documents must be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted or Confidential information must be erased.

2.11. Mobile Device Management

Mobile devices supplied by Brink's shall beused for business purposes. Personal use of Brink's technology equipment is permitted on a limited or incidental basis and consistent with our acceptable use policy. Personnel are responsible for the safekeeping and the protection of any information stored on a mobile device.

Laptops with SIM card capability are considered mobile devices and must implement hard diskencryption and adhere to the MDM policy.

All mobile computing devices must be managed by a Mobile Device Management (MDM) solution. Anyselection of alternative solution for MDM software must be approved by the CISO.

Assigning Mobile Devices:

- Mobile devices are issued for business purposes and remain the property of Brink's.
- Users must acknowledge that theyhave read this policy and the user agreement, or electronically accept the user agreement during registration of the device.
- Where Brink's has enterprise accounts with operators or stores, users must obtain their devices from these sources.

User Responsibilities:

- Brink's-owned devices are subject to monitoring.
- Users are not permitted to authorize purchases or services for their mobile devices.
- Upon termination of employment, users must confirm the removal of any enterprise data and any backups thereof, before any paymentof severance, pension or other compensation can be dispensed.
- Users are responsible for delivering the mobile device to the IT security department if and when the device is selected for a physical security audit or is needed for e-

discovery purposes.

- Brink's has the right to secure enterprise data by wiping the device if compromised, lost, or stolen.
- Device functionality must not be modified, unless required or recommended by Brink's.

Applications and Downloads Restrictions on Corporate Devices

- Users must take all reasonable steps to protect against the installation of unlicensed ormalicious applications.
- All software on the device must either be provided and installed by Brink's or approved by Brink's for installation by the user.
- Users are not permitted to make copies of licensed software.
- Users must ensure that they comply with data copyright requirements.
- Brink's-owned devices are not to be connected to non-owned PCs for accessing iTunes or equivalent software.

Backup and File Sharing or Synchronization:

- Users are required to use approved software for backing up device data.
- The use of a cloud-based file synchronization services, such as Box.com or Dropbox.com is not permitted for Brink's information.

Mobile Device Management

- Mobile Device Management (MDM) solutions must include the ability to maintain a logical separation of Brink's owndata and personal data.

- MDM is responsible for the lockdown for the Brink's apps and maintains the ability to wipe Brink's information on the device.
- Personally owned devices may not be connected to enterprise-owned PCs to utilize consumer media technology such as iTunes.
- MDM solutions must meet the following standards:
    - Encryption of data on the device.
    - Remote Wipe capability enabled.
    - Passcode to access the physical device with timeout enabled.
    - Password to access Brink's data residing on the device.
    - Remote lock capability enabled.

Security Requirements when traveling:

- Users are responsiblefor familiarizing themselves with local and international mobile device laws when traveling to other regions.
- Exercise caution to avoid incurring excessive charges and roaming fees when using the mobiledevice.
- Choose trusted Wi-Fi hot spots while traveling abroad (for example, hotel Wi-Fi or airport Wi-Fi, avoiding unknown open Wi-Fi networks).
- Avoid using mobile phones where alternate, cost-effective communications options exist.
- Disable automatic updates and backup processes when connected to roaming mobile data

networks.

Loss or Theft:

- It is the user's responsibility to take appropriate precautions to prevent damage or loss/theftof the device.
- If the device is lost, stolen, or suspected to be compromised in any way, the user must notify ITManagement as soon as feasibly possible. Notification must take place prior to any cancellation of mobile services.

2.12. Security, Development and Operations

All development, acquisition, or integration projects for information system resources, whether performed in house or by a business partner, must follow an approved systems development life-cycle methodology inclusive of security activities. Security must be addressed throughout the information system resource life-cycle process, from requirements, design, build, system testing, acceptance testing, release (and production) and retirement. All systems development must follow secure coding best practices. All legally protected data must be masked/obfuscated or cleansed prior to utilizing the data in the testing or non-production environments for all systems and/or applications. Each information system resource (i.e., application or infrastructure component) must receive Brink's certification and accreditation.

All new system implementations are required to have IT General Controls (ITGCs) in place and confirmed by Global IT Compliance prior to being made available in production (e.g. SOX, SOC, NIST-CSF, ISO).

2.13. Global Vulnerability Management Program (GVMP)

The Global Vulnerability Management Program is designed to protect Brink's external and internal networks and critical assets.

Vulnerability Scanning

Vulnerability Management plans must cover the following:

- Internal and External network vulnerability scans must be executed every **week**.
- Web Applications must be scanned at least every **quarter**.
- Penetration Testing must be performed at least **annually** and cover globally managed Regional Data Center environments.
- Penetration Testing, including logical and physical testing must be coordinated with and approved by GIS Leadership, including during vendor selection, contract/SOW negotiation, and test scoping.
- Penetration Tests and Vulnerability scans require Change Advisory Board (CAB) approval before being conducted. Full scope and details of the planned test activity must be attached to the change record for review.
- Full results of Penetration Tests and Vulnerability Scans must be made available to GIS Leadership for review.
- Vulnerabilities identified must be remediated according to defined timelines.
- IP address ranges must be reviewed and updated **prior** to scheduling a network vulnerability scan. Asset groups not reviewed must be approved.
- Only the Brink's network is in scope for vulnerability scans. The IP addresses of vendors,

third-parties or service providers, or any other non-Brink's entity should not be included in Brink'svulnerability scans, unless authorized by the third party.

- All systems are subject to scans at anytime without prior notice or approval.
- Internal Vulnerability scans may require that an appliance be installed. GIS must approve such appliances prior to installation.

Vulnerability Remediation:
Vulnerability scans are performed inside and outside of the network and used to test potential exposure over the internet:

- Vulnerabilities detected during network scans shall be prioritized by risk and addressed accordingly.
- Vulnerability remediation must be documented, tracked, and monitored.
- Vulnerabilities associated with assets located within Data Centers will be documented in one ticket opened by GIS and assigned to the technology team responsible for remediation. After each new scan, any open asset group ticket will be updated withthe new scan report as needed.
- Infrastructure, Cloud, and Application Managers are responsible for assigning open vulnerabilities and monitoring to ensure they are remediated in a timely manner.
- Tickets may be closed only after verification that the vulnerability no longer exists through a re-scan.
- Vulnerability severity levels are classified as: Critical, High, Medium, and Low.
- Severity levels are assigned by the Vulnerability Scanner service and determined by the security risk associatedwith its exploitation.
- Countries can request technical assistance from GIS to remediate vulnerabilities.

Remediation Schedule

Severity	Description	Remediation Timeframe
5 - Critical	Intruders **can easily** gain control of the host, which can lead to the compromise of the entire network security. For example, vulnerabilities at this level may include zero-day vulnerabilities, root compromise (or equivalent), full read andwrite access to files, remote execution of commands, and the presence of backdoors.	7 days
4 - High	Intruders **can possibly gain control** of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may be exploitable and result in elevated privileges, could result in significant data loss or downtime, may allow attackers to access sensitive data	10 days
3 - Medium	*Intruders **may be able to gain access** to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.*	*30 days*

2 –Low	*Intruders can collect information about the host (open ports, services, etc.) and **may be able** to use this information to find other vulnerabilities.*	*60 – 90 days*

Remediation Exceptions
Systems may be exempted from the vulnerability management remediation schedule due to possible technical dependencies or third-party contractual obligations. Any such exceptions must be documented and approved.

When remediation is dependent on technology or resources not currently available, an action plan for remediation must be documented and presented to Senior IT Leadership within the timeframe below:

Finding Rating	Action Plan Submission
High	10 business days
Medium	20 business days
Low	30 business days

Reporting of Vulnerabilities:
Vulnerability Management reports are considered Confidential and must not be shared with external contractors, third-parties, or distributed outside of the Brink's organization. If a network device within a Country is managed by a third-party, only those observations pertaining to that particular device may be shared with the vendor.

2.14. Patch Management

Brink's Patch Management Program defines a unified approach to system patching. Information system resources installed in Brink's computing environment must conform to the following Patch Management Requirements:

- Notification of vulnerabilities and patches from third parties must be reviewed.
- Ongoing Analysis of all operating systems and applications must be performed to identify all possible security vulnerabilities.
- Results of vulnerability scans must be remediated to secure information system resources (e.g., installing service packs and hotfixes).
- Scanning of the entire Brink's network for the purpose of identifying systems that are not up to date with current internal patching standards.
- Patches shall be tested in a test/staging environment prior to production deployment.
- Verification of successful deployment on each machine.
- Exceptions to the Patch Management process must be documented and approved according to the Risk Acceptance and Policy Exception process.
- All server patching must follow the Global IT Change Management process.

Patching Prioritization
The Patch Management and GIS Vulnerability Management teams are responsible for assigning patch priority. Patches are prioritized according to the severity assigned by the vendor, vulnerability exposure, and impact to Brink's environment.

Severity	Schedule
Critical (out of Band/Zero-Day)	• Desktop/Laptops – Immediately • OS Servers – Next patching cycle • Application- On demand pending nonproduction testing as soon as possible
Critical (CVSS 9.0 - 10.0)	• Desktop/Laptops - 7 days • OS Servers - Next patching cycle • Application- 30 Days
High (CVSS 7.0 - 8.9)	• Desktop/Laptops - 10 days • OS Servers- Next patching cycle • Application – 60 days or regular maintenance schedule
Medium (CVSS(4.0 - 6.9)	• Desktop/Laptops - 30 days • OS Servers – Next patching cycle • Application- 90 days or regular maintenance schedule
Low (CVSS 0.1 - 3.9)	Desktop/Laptop and Servers - 120 days or regular maintenance schedule

2.15. System Logging and Monitoring

Brinks Log Management is comprised of foundational event logging and monitoring as well as modern security monitoring, investigation, and forensics. This is achieved by:

- Log Aggregation: the process of collecting logs from multiple computing systems, collecting them in a central source, extracting structured data, and putting together in a format that is easily searchable by modern data tools.
- Log processing: taking raw system logs from multiple sources, identifying their structure or schema, extracting fields, and turning them into a consistent, standardized data source.
- Log Normalization: merging events containing different data into a reduced format which contains common event attributes.
- Log Categorization: identifying log data related to system events, authentication, local/remote operations, network, application, database, etc.

Logging and Monitoring controls apply to all managed hardware and software using the Brink's network via a physical or wireless connection, regardless of the ownership of the computing device connected to the network.

Logging and Monitoring controls also apply to off-site computing devices that connect remotely to the network.

Access to, and usage of, Brink's network, systems and communications shall be logged and monitored to identify unauthorized or potential misuse of systems or information.

Logging should be enabled and tuned to ensure events of interest are recorded for operating systems, network devices, services, and applications that store, process, and transmit information. Every critical component in the system architecture should be configured to generate audit events.

To ensure that appropriate safeguards are in place and effective, Brinks shall audit, log, and monitor events to detect, report, and support response for:

- Network activities, vulnerabilities, and intrusions

- Performance problems (system, network, or application)
- Application configuration issues and flaws
- Security violations
- Data loss or unauthorized access, modification, or destruction
- Unauthorized access and processing of restricted or confidential data
- Loss of confidentiality and security of restricted or confidential data.

UNDERLYING REQUIREMENTS

Brinks shall implement a suitable logging infrastructure and configure all devices, systems, and applications with logged audit trails.

Brinks IT & application owners shall establish a baseline of “normal” activity to determine what constitutes standard behavioral activities and identify anomalous, abnormal, or malicious activity and alert appropriately.

A SIEM shall be used for continuous monitoring. The SIEM shall have engineering support across the product and use case/detection lifecycle.

Security logs may be subject to regulatory or compliance requirements.

Server and networking equipment must perform security log generation for components (e.g., OS, service, application). Server SIEM and systems capable of generating alerts (e.g., intrusion detection systems, etc.) shall issue alerts on security log processing failures, such as software/hardware errors, failures in the log capturing mechanisms, and log storage capacity being reached or exceeded. All alerts must be as close to real time as possible.

Systems and applications that handle restricted or confidential information shall record and retain audit logging information to:

- Determine the activity that was performed
- Who or what performed the activity, including where or on what system the activity was performed (subject)
- Identification of the source of event such as location, IP addresses terminal ID or other means of identification
- Systems and objects involved
- When the activity was performed
- Status (such as success vs. failure), outcome, and/or result of the activity

LOGGING ACTIVITIES

Security Operations shall be assigned to review alerts generated by the SIEM and security tools deployed on Brinks systems and networks.

Auditable Events:

Logs shall be used to reconstruct the following events to support cybersecurity investigations:

- Successful and unsuccessful login events
- Account management activities (e.g., account creation, modification, deletion)
- Successful and unsuccessful resource access events
- Successful and unsuccessful access to log files
- Changes in authorization
- Changed of passwords

- Access, modification, and deletion of critical data sets
- Individual user accesses to systems and information
- Access to audit trails
- Invalid logical access attempts and failures
- Initialization, stopping, or pausing of services
- Creation and deletion of system level objects
- Successful and unsuccessful privileged operations including:
    - All actions taken by any individual with administrative privileges
    - Use of privileged commands on the operating system and for applications
    - Use of and changes to identification and authentication mechanisms including all changes, additions, or deletions to accounts with administrative privileges
    - Use of system privileged accounts
    - System starts and stops
    - Hardware attachments and detachments
    - System and network management alerts and error messages
    - Account/group management and policy changes.

SYSTEM LOG ELEMENTS

System events and activities that shall be monitored and logged are as follows:

- System administrator and system operator activities
- System start-ups and shutdowns
- Logging start-ups and shutdowns
- Backups and restorations/rollbacks
- Alerts, exceptions, and security events
- Database commits and transactions
- Modifications to data characteristics including permissions, location, file type
- Authentication successes and failures (e.g., log in, log out, failed logins).

APPLICATION LOG ELEMENTS

Application events and activities that shall be monitored and logged include:

- Application authentication (e.g., successes, failures, logouts)
- Data audit trails (e.g., access to sensitive data, adding data, modifying data, deleting data, exporting, and importing data)
- Input validation failures (e.g., protocol violations, unacceptable encodings, invalid parameter names and values)
- Output validation failures (e.g., database record mismatch, invalid data encoding)
- Suspicious behavior (e.g., multiple records deleted in a short period of time, invalid access attempts)
- Session management failures (e.g., cookie session identification value modifications)
- Application errors and events (e.g., syntax and runtime errors, connectivity problems, third party service error messages, file system errors, sequencing failure)
- Higher-risk functionality (e.g., adding and deleting users, changes to access privileges, use of administrative privileges, access by application administrators, and access to sensitive data)
- Legal compliance services (e.g., permissions to transfer information, and terms of use).

LOGGING ELEMENTS

Generally, automated audit trails shall include the following information:

- User initiating action (e.g., user ID)
- Host name, system component, or resource

- Date/Time Stamp (including time zone or UTC)
- Application ID (e.g., name and version)
- Initiating Parent Process ID or event origination (e.g., entry point URL, page, form, and path)
- Code location (e.g., module, subroutine, directory)
- Event type
- Result status (e.g., success, failure, defer)
- Resource (e.g., identity or name of affected data, component)
- Location (e.g., IP address or location)
- Severity of event (e.g., emergency, alert, fatal error, warning, information only)
- An indication of success or failure of event
- Other (e.g., parameters, debug information, system error message).

INFORMATION SECURITY ISSUES

Detailed procedures that support this policy shall be developed to protect against and limit log security risks such as:

- Controls that limit the ability of administrators and those with operating system command line access to disable, damage, or circumvent access control and audit log mechanisms
- Protecting the contents of system logs from unauthorized access, modification, and/or deletion
- Limiting outside access to logging systems to extreme or emergency circumstances.
- Authorized emergency access roles and tools used to bypass security controls should be documented
- Changes to auditing policies that stop logging of unauthorized activity should be limited
- Log settings should be set to track and record user policy changes

ADMINISTRATIVE RESPONSIBILITIES

The Office of the Chief Information Security Officer (CISO) shall be responsible for:

- Separating duties between operations and security monitoring
- Ensuring a regular review of activity audit logs, access reports, and security incidents
- Approving the types of logs and reports to be generated, review activities to be performed, and procedures that describe the specifics of the reviews
- Procedures that specify monitoring log-in attempts, reporting discrepancies, and processes used to monitor log-in attempts
- Procedures that specify audit controls, hardware, software, and/or procedural mechanisms
- Procedures that ensure the audit controls meet security requirements
- Securing audit trails by limiting viewing to those with a job-related need
- Protecting audit trail files from unauthorized modifications
- Ensuring audit trail files are promptly backed up to a centralized log server or media.

Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of Brinks procedures. At a minimum, auditable controls shall include:

- On demand and historical log reviews of areas described in this policy
- Documented communications surrounding logging activities
- Incident response procedures

Formatting and Storage

- The system shall support the formatting and storage of audit logs to ensure enterprise-level

analysis and reporting.
- Systems that collect logs, whether local or consolidated, must maintain sufficient storage space to meet the minimum requirements for both readily available and retained logs.
- Storage planning must account for log bursts or increases in storage requirements that could reasonably be expected to result from system issues.
- Storing logs in a documented format and sent via reliable network protocols to a centralized log management system.
- Storing log entries in a SQL database that generates audit logs in compliance with the requirements of this policy.

Log Retention and Disposal
Information System audit logs must be retained for an appropriate period, based on the Business Records Retention Schedule and business requirements. Audit logs that have exceeded this retention period must be securely disposed of in compliance with Brinks document destruction guidelines.

IT system logs must be retained based on:
- Brinks Data Retention Schedule
- Information owner
- Contractual obligations

A process must be put in place to provide for log preservation requests, such as a legal requirement to prevent the alteration and destruction of log records (e.g., how the impacted logs must be marked, stored, and protected).
Log integrity for consolidated log infrastructure needs to be preserved, such as storing logs on write-once media or generating message digests for each log file.

2.16. Monitoring, Detection, Response

A dedicated Global Security Operations Center (GSOC) Team is responsible for monitoring and investigating systems, cloud, application, infrastructure, networking, and other logs. Suspicious cyber activity must be reported to GIS and the GSOC team according to the Cybersecurity Incident Response Plan (CSIRP).

The following controls must be implemented by both the Intrusion Detection Team and local IT resources:

- Actively search for signs of unauthorized access.
- Increase security by detecting weaknesses in systems and network design early.
- Prevent unauthorized access to organizational systems.
- All systems accessing the internet must operate IT approved active monitoring and detection software.
- Network and monitoring capabilities shall be implemented.
- Identity monitoring, including authorization, authentication and access shall be implemented.
- Additional controls in DMZ environment shall be added.
- All host based and network-based intrusion detection systems must be checked on a daily basis and their logs reviewed.
- All intrusion detection logs must be kept in compliance with Brinks' Record Retention Policy.

2.17. Data Compromise

A material data incident is one that threatens confidentiality, integrity, or availability of Brink's information assets. The Data Breach Response Plan defines the roles and responsibilities for critical incident response team members, defines critical incident severity levels, outlines a process flow for critical incident management, and includes methodologies for conducting response activities. This includes:

- The individuals and teams with responsibility for responding to the impact from any materialcompromise of Brink's data.
- Support and resources that are available to assist in responding to a compromise of private Brink'sdata.

Data Compromise Definitions

- **Breach:** the exposure, compromise, or loss of Brink's private data.
- **Brink's Private Data:** any information under Brink's control that is not considered public. Thisincludes:
    - **Personally Identifiable Information (PII):** this includes any information relating to an identified or identifiable natural person employed by Brink's, i.e., non-public employee personal data such asdate of birth, address, cell phone number, social security, bank account, and even benefits and health-related information
    - **Customer Data:** any non-public information used by Brink's, its customers, suppliers, other businesspartners and contacts and subsidiaries in the execution of services. This includes internal technical details such as IP addresses, account information and details needed in the execution of specific services, such as ATM maintenance and any personal data related to the natural persons mentionedabove.
    - **Non-Public Information (NPI):** any proprietary or confidential information.

Global Information Security: This team is led by the Chief Information Security Officer (CISO) and isresponsible for enterprise level technology and data security. This includes:

- Developing and maintaining the policies and procedures necessary to support and executeinformation and data security activities.
- Developing and maintaining tools, resources, and templates to facilitate information and datasecurity activities.
- Providing guidance and support to departments / divisions and countries in the execution oftheir information and data security programs and activities.
- Providing regular information and updates to the Data Protection Officer as to the above andinforming them immediately in case of breaches involving Personal Private Information or Customer Data.

Country Level Leadership: This includes both the country General Manager and the country IT Director.

Employees: Any employee who suspects that a theft, incident, or exposure of Brink's Private data has occurred must immediately provide a description of what occurred via e-mail to GIS@Brinksinc.com orby calling 469-549-6733, or through the Service Now reporting web page.

Data Compromise Statements:

- Compromise, theft, or exposure of Brink's Private data is communicated to the InformationSecurity Team through a variety of channels. This includes:
  - Engagement by Brink's Physical Security Team following a theft or suspected compromise.
  - Escalation by Brink's Level 1 or 2 Support Teams such as Brink's Technical Assistance Desk(BTAC) or Brink's Global Operations Team.
  - From outside third partiesor law enforcement agencies should they encounter stolen or compromised data.
- As soon as a compromise or exposure of Brink's Private data is identified, Brink's Information Security Team will take the following actions:
  - Affected systems on Brink's network will be immediately isolated from Brink's network.
  - Inform the Data Protection Officer (DPO) as soon as it is determined that PersonalPrivate Information or Customer Data has been breached.
    - When the Personal Private Information or Customer Data breach is likely to result in *a high risk* to the rights and freedoms of the relevant persons, the DPOwill help assess whether it shall be communicated to the relevant persons without undue delay.
    - When the Personal Private Information or Customer Data breach is likely to result in *a risk* to the rights and freedoms of the relevant persons, the DPO willhelp assess whether it shall be communicated the relevant data protection agency without undue delay and no later than 72 hours after the breach has been discovered.
  - Forensic investigators and experts will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.
  - Initiate the Crisis Management Process following the steps outlined in Brink's GlobalCrisis Management Team Procedures*.
  - Brink's Crisis Management Team Procedures also trigger Brink's Crisis Communications*plan which establishes procedures for the communication of the breach to employees, customers, and investors.

**These procedures outline the roles and responsibilities of Crisis Management Team Member, DPO and their procedures responding to such events.*

2.18. Education and Security Awareness Training

Brink's GIS, in cooperation with local management, shall ensure that Security Awareness Training is routinely conducted for all Brink's users who have access to Brink's data systems, specifically, email and networks. Information Security Awareness training will be created and issued by GIS.

- Brink's employees with privileged access to Restricted and Confidential information will be required to complete additional annual role base training for their specific role.
- Employees with access to Brink's data systems, specifically email and networks, must be trained to report information security events and incidents.
- Employees in a developer role must complete formal training in general secure coding techniques and in developing secure code in the programming language(s) they use.

- Annual OWASP training must be completed by developers to create awareness on the latest threat vectors in web applications.
- Failure to complete Brink's Annual Security Awareness Training can result in deactivation of access until training is completed. Exceptions may be granted by the CISO.

All personnel with access to Brink's data systems. e.g., specifically, email and, applications, networks must receive Information Security Awareness training within 90 days of hire. Contractors must provide evidence of Information Security Awareness training through contracting agency in accordance with contractual requirements. All employees and contractors with access to Brink's data systems. e.g., specifically, email and, applications, networks are required to take annual Information Security Awareness Training, which is tracked and audited using the Global IT Security Learning Management System (LMS)

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 security is the individual and collective responsibility of all Brink's personnel, business partners, contractors, and other authorized users. Access to information system resources is based on an individual's roles and responsibilities. Only authorized personnel are approved to access Brink's information system resources.

3.3. All officers, business and line managers, and supervisors, are responsible for implementing and enforcing information security standards and policies. All officers and managers must ensure compliance with information security policies by organizations and information system resources under their direction and provide the personnel, financial, and physical resources required to appropriately protect information system resources. Managers at all levels are responsible for identifying sensitive positions within their organizations and notifying GIS. Sensitive positions include those in which personnel could, in the normal performance of their duties, cause material adverse effects to Brink's information system resources. Such duties include: making changes in the operating system, configuration parameters, system controls, and audit trails, modifying security authorizations, and making revisions to sensitive programs and data that could be undetected. Any individual with responsibility for management of IT General Controls (ITGCs), including the delivery of evidence demonstrating compliance with required controls, is a Control Owner. Control Owners are required to review control requirements (attributes) for each applicable control and system for which the Control Owners is responsible. In addition, the Control Owner must confirm, through a quarterly attestation process, that they are aware of their responsibilities and that the applicable control(s) and system(s) they manage will remain compliant.

4. References

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

4.2. Related: Standard number or other references, when applicable.
- GITP-015 - Wireless LAN Configuration Policy
- GITP-018 - Global IT Incident Management Policy
- GITP-035 - Global IT Change Management Policy
- Access Review Procedure
- Brink's Code of Ethics
- Brink's Cloud Security Strategy

4.3. A full list of controls can be found on the Brink's Resource Library.

5. Authorization

This policy is authorized by:

James Holley
Vice President
Global Chief Information Security Officer (CISO)

Policy Owner: Ron Banks, Deputy Chief Information Security Officer

Additional Stakeholders: Chris Foley, Global IT Senior Director
Gangadhar Polavarapu, Global IT Director
Garrett Hamlin, Security Engineering Manager
Bill Morrison, Sr. Director, Cyber Security Operations & Incident Response

6. Change History

Original Publish Date:

Revision	Date	Author	Revision History
1.0 - Draft	05/12/2020	Brink's GIS Angel Mosley James Pak Ron Banks Mustapha Kebbeh	Combined 15 GIS Policies into 1 Comprehensive Global Information Security Management Policy
1.1	05/27/2020	Governance, Risk and Compliance	Review / alignment with policy standards
1.2	June 2021	Carrie Rogers	Review; updates to section 8

1.2	09/17/2021	Carrie Rogers	Verbiage update section 7
1.2	10/28/2021	Mustapha Kebbeh & Carrie Rogers	Verbiage update – Section 8
1.2	11/26/2021	Carrie Rogers & Mark Armour	Verbiage update – Section 8
1.3	April / May 2023	Owner, Stakeholders and GRC	Review and Updates
1.3	05/26/2023	Carrie Rogers	Update to current policy template; clean-up of all edits/updates
1.3	05/30 – 06/02/2023	Patrick Benoit and Hal Snedden	Authorizer and Global Ethics & Compliance Review and Approval
1.4	02/01/24 – 03/28/24	Owner, Stakeholders, and GRC	Minor updates to language
1.5	9/24/2024	James Holley, Ron Banks, and Carrie Rogers	Updated language in Password section (2.4)
1.5	11/05/2024	James Holley, Ron Banks, Tina Cavitt, and Carrie Rogers	Additional updated language in Password section (2.4)
1.5	11/07/2024	Ron Banks	Review of updated language and approval
1.5	11/12/2024	James Holley	Review of updated language and approval