Brink's Incorporated North America

Information Security Overview
2014

Summary:

Brink's, Incorporated, a subsidiary of The Brink's Company, is a global leader in business and security services serving banks, retailers, governments, mints, diamantaires and jewelers through more than 800 facilities and 9100 vehicles in 50 countries on 6 continents – an unrivaled footprint that delivers incomparable security, efficiency and visibility across the logistics lifecycle.

Brink's North American IT Security program follows the same legacy of trust and is designed to provide the same level of protection to customer data that Brink's is known for providing to all customer assets. The following information is provided as a detailed overview of the IT Security safeguards Brink's currently has in place.

A portion of this data is derived from the Level 2 Standardized Information Gathering (SIG) questionnaire published by the Financial Institution Shared Assessments Program (FISAP), a widely recognized and accepted standard for Information Security exchange.

As with all information related to a dynamic, evolving, computer-based environment, this information is a point-in-time depiction and is subject to change without notice. Brink's North America makes every reasonable effort to maintain the currency of this information but cannot guarantee absolute accuracy at all times. *This information is Brink's Incorporated confidential and is made available only under a signed non-disclosure agreement; distribution without prior authorization from Brink's is prohibited.*

Please direct any questions or concerns about this document to your Account Executive.

Contents

Section 1: Information Security Policies

Brink's North America maintains a comprehensive set of Information Security policies covering all aspects of data protection. Policies are available to all Brink's employees through the company Intranet. The following list provides a summary of these policies.

- Acceptable Use and Electronic Asset Protection
- Computer Systems User Account Management
- Computer Systems Third Party Account Management
- Computer Systems User Password Management
- Computer Systems User Account Termination
- Computer Systems Privileged or High Risk Account Management
- Computer Systems Patch Management
- Computer Systems Internet Access Restrictions
- Computer Systems Software Installation and Usage
- Antivirus & Malware Protection
- Data Encryption Standards
- System Backups
- Offsite Storage
- Electronic Mail Backup
- Electronic Mail Retention Requirements
- Production System Changes
- Production Systems Change Management Guidelines
- Testing, Quality Assurance and User Acceptance
- Application Configuration Management
- Application Development Requirements
- Application Deployment
- Application Security Requirements
- Third Party Network Access
- Remote User Access
- Physical Security – General
- Physical Security – Data Center Access
- Physical Security – Branch Offices
- Physical Security – Portable Devices
- Physical Security – Loss or Damage Reporting
- Physical Security – Equipment Disposal & Re-use
- Physical Security – Power Management
- Physical Security – Environmental Controls
- Information Security Policy Management

Section 2: Employee Awareness & Training

Brink's enforces its commitment to protection of customer data through regular communications and notifications to employees. Employees, Vendors and Contractors receive notification of important changes to:

- Regulatory requirements
- Policy updates
- New policy requirements
- Potential dangers from cyber activity

In addition to regular communications, employees, vendors and contractors are required to read and acknowledge Brink's General Information Security Policy. This policy highlights major areas that employees, vendors and contractors are expected to be aware of at all times and reinforces Brink's commitment to protecting sensitive internal and customer data.

The General Information Security policy provides employees with an overview of:

- Proper handling of confidential or sensitive consumer information
- Handling of information incidents
- Protection of Information Systems
- Employee obligations
- Protection of hardware & software assets
- Appropriate use of removal media (USB drives, CD's, etc)
- Appropriate protection of system passwords
- Email security
- Approved use of computer software
- Document handling and confidential information protection
- Legal obligations of all employees

Section 3: Network Security & Monitoring

- All external network connection terminated at a firewall
- Are network devices are configured to prevent communications from unapproved networks
- Routing protocols are configured to require authentication
- Network devices are configure to deny access by default
- A process to request, approve, log, and review network access is in place
- Network traffic events are logged to support investigations and incident response
- Security patches are regularly reviewed and applied production devices
- Communication through network devices is controlled at both the port and IP address level
- Critical network segments are isolated
- All internal devices are configured to pass through a content filtering proxy prior to access the Internet
- Network Intrusion Detection/Prevention System are in place
- Proxy Server is in place
- Event Monitoring is in place
- Quarterly vulnerability assessments are performed on both internal and external network.
- A current and approved risk assessment program is in place

Section 4: Change Management

- A Change Management Policy is in place
- CAB meetings are held weekly to approve incoming changes
- All changes require documentation inducing
    - ✓ Requester
    - ✓ Type of Change
    - ✓ Risk of Change
    - ✓ Approved Testing of proposed change
    - ✓ Back-out plan in the event the change fails
- All changes require management approval

Section 5: Accountability of Assets

- A Corporate Asset Policy is in place
- All assets are identified with a Control Asset Tag/Label
- A physical count of assets is executed at least annually
- Asset counts are recorded by the Finance Department
- An automated process is in place to query assets to ensure compliance with licensing requirements.

Section 6: Systems Security and Backups

- Anti-virus/Malware protection is in place and deployed
- Anti-virus updates are scheduled daily
- Users cannot disable anti-virus software
- Approved patches are approved and applied quarterly
- Backup policies are in place
- System Backups are performed on all production systems.
    - ✓ Daily incremental
    - ✓ Weekly Full
- Backup media is store offsite
- Backup media is not currently encrypted
- A Secure Hardening process is in place
- Secure Hardening standards and procedures are in place.

Section 7: Incident Management & Response

- An Incident Management policy and Plan is in place
- Incident Response Plan is tested annually
- Incident Response procedures is tested annually
- Security incident response team is define and roles and responsibilities assigned
- Documentations for all incidents (issues, outcomes, and remediation) are documented

Section 8: Incident Management & Response

- An Incident Management policy and Plan is in place
- Incident Response Plan is tested annually
- Incident Response procedures is tested annually
- Security incident response team is define and roles and responsibilities assigned
- Documentations for all incidents (issues, outcomes, and remediation) are documented

Section 9: Physical and Environmental Security

- A Physical Security Policy is in place
- Access to the building and sensitive areas are controlled via
  - ✓ Security Guards
  - ✓ CCTV
  - ✓ Alarm Systems
  - ✓ Badge Access
- The loading dock area is monitored by CCTV camera and Security guard patrols the area.
- Battery/UPS devices are in place
- Generators providing emergency power is in place
- Access to IDF closets is control via Badge Access
- Mailroom does not stores or processes target data
- Brinks data center hold all target data
- Telecom equipment is house in the data center or IDF rooms.
- Access to Brinks Data Center is controlled and limited to authorized personnel?
- Brinks Data Center is located in a Colo-Site and restricted by cage environment (High Metal Walls and Badge Access systems)

Section 10: Access Control

Access control policy is in place

- Access control policy covers applications, operating systems, databases, and network devices ensuring least privilege access
- Unique user IDs are issued to all users with access
- The following are not allowed as part of the user ID
  - ✓ SSN
  - ✓ DOB
  - ✓ Proper names
  - ✓ Access level description
- Stale accounts are disabled after 90 days
- Sharing of User IDs or Passwords is prohibited
- A process to grant and approve access to systems holding, processing, or transporting target data is in place and require management approval
- Approved requests for granting access are archived and tested in an annual basis
- Business Owner approval is required to grant access to applications and systems
- Passwords are required to access all systems and must meet the following criteria:
  - ✓ Must be a minimum of eight characters
  - ✓ Must contain a minimum of three of the following four attributes:
  - ✓ Upper-case alphabetic
  - ✓ Lower-case alphabetic
  - ✓ Number
  - ✓ Non-alphanumeric character
  - ✓ Must be changed at least every 60 days
  - ✓ Cannot reuse previous eight passwords
- All new users are issue random initial passwords, which require the user to change the password on first login.
- Clean Desk Policy is in place
- Default passwords are remove, disabled or changed prior to placing devices or systems into production
- Remote access policy is in place
- All Policies are reviewed and approved by management annually

Section 11: Human Resource Security

- Background screenings of applicants is performed to include criminal, credit, professional, academic, references and drug screening
- Pre-screening policy and procedures are in place
- When allowed by law, new hires are required to sign any agreements that pertain to non-disclosure, confidentiality, acceptable use or code of ethics upon hire
- New users are required to participate and pass a Security Awareness Program. All users must recertified annually
- The security awareness training include security policies
- Associates responsible for information security undergo additional training
- A disciplinarily process for non-compliance with information security policy is in place and includes termination when appropriate.

Section 12: Organizational Security

- A formal Information Security Team is in place
- Information security responsibilities are allocated to the group and specific individuals
- Information Security Group maintains contact with special interest groups, specialist security forums, or professional associations to obtain current and relevant information
- No independent 3rd party responsible for the regular review of the information security program is in place
- An independent group responsible for ensuring compliance with security policies is in place
- Key Information Technology constituents are identified
- Management require the use of confidentiality or non-disclosure agreements when allowed by law
- Information Security Policies are in place
- Information Security Policies have been published
- Information Security Policies must be acknowledged by all users with access to sensitive data
- Information Security Policies are reviewed and approved at least annually
- An Acceptable Use Policy is in place