# COLE GROUP

## Corporate Security Policy/Training Booklet

## Managers

# Corporate Security policy/Training booklet for Managers
# Revision History

| Revision # | Date | Revision Summary | Author |
|---|---|---|---|
| 1 | Mar 31/09 | Initial release | K DeFoe |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Security Policy Statement

The Cole Group is committed to creating and maintaining the securest possible work environment for our employees, customers and general public. The company believes that our employees are our most valuable asset and are critical to our overall results and the success of the organization. We define security as the prevention of harm or damage to people, property and the environment. We will achieve this goal by implementing, training and reinforcing the security standards, values and objectives we have developed.

# Document Security

It is the responsibility of all Cole Group employees to ensure that sensitive documents are not left out in the open. Documents that are necessary to the performance of daily duties may be left out, but employees must ensure that sensitive information is not visible when visitors are present. Meetings with visitors should be conducted away from areas where sensitive information is visible. If the office has a boardroom or meeting room, these rooms must be utilized.

Although they may not be perceived to be sensitive, articles such as company letterhead, envelopes bearing company information or transaction bar codes must not be left out under any circumstances. Any documents bearing freight rates, brokerage schedules or customers' financial information must not be left out. If you must leave your desk for an extended period of time, please ensure that all such documents are filed away.

Proper disposal procedures of unwanted, expired, sensitive documents must be followed. Shredding is preferred, but any other secure disposal method is acceptable.

# Computer and Information Technology Security

Electronic files play a key role in the functioning of our organization. Securing data from intentional or accidental damage is vital in an increasingly paperless world. Our electronic files need to be protected.

Some general common sense rules are:

- Passwords must be controlled. Never write down or share your password(s).
- Do not leave computers logged on when unattended for extended periods.
- Follow proper Email policy.
- Follow proper Internet policy.
- Regularly backup your information to avoid loss of data.
- Lap top users must ensure that anti-virus software and any critical updates are applied in a timely manner.
- Securely store laptops during non business hours.
- Out of the office, laptops or any other removable storage media, should never be left unattended (in vehicles etc).
- Immediately notify management and our IT department if sensitive information is lost or suspected of being lost, unauthorized use of our information system is suspected or taken place, or actual or suspected access mechanisms are lost, stolen or disclosed.

Please refer to the ‘The Cole Group Information Technology Security’ document for complete details.

# Hiring Policy

Personnel selections of the company are very important. The company is committed to hiring only the best, safest and most qualified employees. To achieve this objective, the company has implemented the following employee hiring standards and procedures.

All management personnel who either solicit or receive information regarding a potential employee must obtain and verify the following during the application and hiring process.

Potential Employee Requirements:

- At least three personal references with complete contact information.
- Accurate information regarding home address and telephone number.
- Information regarding their level of education, including copies of any degrees or certificates.
- Employment history for at least 5 years, or if they have not been in the labour market for 5 years, information from the point of leaving school will be acceptable.
- Any professional references as they see fit.

Management requirements:

- All personal references **must** be verified.
- Education must be verified.
- Professional references must be verified.
- The potential candidate must be advised that a security background check must be performed if they will be handling any exports on passenger aircraft. This is a requirement of the Transport Canada, Air Cargo Security Program. Background checks may also be performed on prospective employees hired for a security-sensitive position.

Once all the references have been verified and the background check documentation is in place (if required), an Employment Offer must be completed and presented to the potential employee for their agreement. Once this document is completed, you will be responsible to provide them with a “New Employee Package” specific to their location. This package can be located on the Cole intranet under Human Resources, Hiring Process, Step 2. All forms must be completed and returned. Please ensure that you print the checklist and all items are completed and checked. Any forms noted on the checklist that are not included in the new employee package can be found on the intranet.

For identification purposes, all new employees must be taken through the facility and introduced and made familiar to other staff.

# Key and Access Device Control

Management at each branch must control the issuance and retrieval of all access devices such as keys, swipe cards and access codes. It's recommended that staff sign for these devices upon receipt. Management must securely maintain this information on file. Staff must be instructed not to share, copy or loan these devices.

Access to any secure areas within the facility must be restricted to employees whose job function is required in these areas. After hours access must also be restricted to authorized staff. Only they should be issued keys, swipe cards or access codes allowing for non-business hour access.

# Termination Procedures

The following steps must be adhered to when an employee is terminated.

1. If the termination is voluntary, the employee must provide written notice. If the employee is in a sensitive position, it may be required to dismiss him/her immediately and make arrangements to pay them for the period of their notice.

2. In the event of an involuntary termination, or voluntary termination of an employee with access to sensitive information, the employee must be supervised at all times while collecting personal items from their workspace. Only personal items may be allowed to leave the premises. An inspection of articles prior to them leaving, is required.

3. If the employee was in possession of any company property such as portable electronic devices, cell phones, blackberries, laptop computers, keys, swipe cards etc, all of these must be surrendered prior to their leaving. For control purposes, these items should have been signed for when initially issued.

4. For any offices with push-button locks, all codes must be changed immediately and the new codes provided to all affected staff members. If all access devices are not returned, swipe cards must be deactivated, locks changed and new keys issued to all affected personnel.

5. IT must be informed to immediately deactivate any user ID or access information. A delete request form can be obtained on the Cole intranet. Delete requests are given a high priority by our IT department.

6. Remind all terminated employees of their obligations regarding confidentiality. If required, provide them with a copy of the agreement they signed at time of employment.

7. Immediately inform HR of the termination. This ensures that their payroll is terminated at the end of their notice, or immediately, as required.

# Visitors and Vendors

## Visitors

In most cases, the main point of entry is via the front door that may lead to a reception desk, counter or reception area. The receptionist or person stationed at or closest to this entry point, will be the first line of defense in dealing with any visitors. They will be responsible for visitor controls.

In order for visitors to gain access into the office:

1. Receptionist must ask appropriate questions as to the nature of the visit.

2. Visitors must register in the visitor log, completing the various fields (name, company name, type of photo ID presented, person being visited and arrival/departure times)

3. Visitors must present photo ID.

4. Visitors must be issued a temporary visitor identification badge, which must visibly be worn throughout the visit.

5. Visitors must be escorted beyond the reception area and not be allowed to wander off alone.

Meetings are to be held in boardrooms or conference rooms and not at employee desks. When the visit is over, the visitor is to be escorted back to the reception area. Upon departure, they must return their visitor identification badge to the receptionist and indicate their departure time in the visitors log.

## Vendors

All vendors entering the premises must present photo and/or company ID prior to acceptance or surrender of packages. All should have a drivers licence, but company ID is preferred. If the vendor does not have appropriate ID, they should be refused entry and asked to return with proper identification.

If the vendor must enter the premises, past the reception area, then they must sign into the logbook and visibly wear temporary visitor ID at all times. Vendors must be escorted beyond the reception area and not be allowed to wander off alone. Upon departure, they must return their visitor ID badge and indicate their departure time in the log.

# Challenging and Removing Unauthorized Persons

## Manager Guidelines

All Cole Group managers are responsible to ensure that unauthorized persons are identified and removed from the premises as necessary. Management is to encourage employees to report any unauthorized person to their supervisor immediately, and failing that, the department manager. Employees should never confront an intruder on their own. Another employee must be present when an unauthorized party is confronted. As corporate policy dictates that all visitors and vendors must wear temporary issued ID while on the premises, the identification of unauthorized parties should be relatively simple. If it is discovered that the visitor/vendor has passed reception without signing in and obtaining a visitor badge, they must be immediately escorted back to the point of entry for proper check in (sign in, show ID and receive a visitor badge). If the unwanted party is not a bonafide visitor or vendor, then extreme caution should be used while attempting to have them escorted from the building. If further intervention is required, then building security is asked to assist if available, otherwise appropriate local authorities are to be contacted. Do not make any effort to apprehend or detain anyone, as such action may place you or other staff members at risk.

**Please note: In addition to contacting local authorities, all managers must immediately report all security breaches to the corporate director of their business group and to our Security Manager. This must be followed up in writing with an explanation of the circumstances, including statements from all affected Cole Group employees. Any police reports must also be forwarded.**

## Employee Guidelines

All Cole Group employees have a responsibility to report unauthorized persons. Any unidentified parties on the premises must be immediately brought to the attention of your supervisor or manager. DO NOT confront any unidentified person or persons on the premises. As corporate policy dictates that all visitors and vendors must wear temporary identification (visitor badge) while on the premises, the identification of unauthorized parties should be relatively simple. Again, DO NOT confront any unidentified person or persons on the premises. Go directly to your immediate supervisor or manager and they will handle the situation.

# Packages and Mail

Any courier/driver delivering or picking up packages must be asked for photo and/or company ID prior to acceptance or release of packages. Employees of parcel service companies and Canada Post often wear uniforms and carry ID that clearly identify them as employees of that company.

A possible exception to requesting ID, may be for the courier or postal employee that has a regularly scheduled pickup or drop off at our location and we know them by sight. If your staff has historically dealt with the same individual, then photo or company ID does not need to be requested each time.

**Incoming Packages and Mail**

It is not acceptable to accept packages/mail that are not specifically addressed to our office. Staff must also instruct the shipper to indicate the name of the individual to whom the package is destined, or the package could be refused at time of delivery. Packages that are mis-delivered must be refused and if possible, directed to the appropriate party. We sometimes see freight for one of our own customers that has been incorrectly addressed to our location. If this occurs you must contact our customer so they may make arrangements with the transportation company for delivery to their location. In order to prevent future similar occurrences, you must ensure that your customer relays specific instructions to the shipper.

In addition, packages should be visually inspected for any external damage or other exception, such as piece count, prior to acceptance and signed for accordingly. Packages and mail must also be periodically screened before being disseminated. Any packages that seem unusual should be further inspected utilizing the attached “Mail Bomb Information” and “Suspicious Letter” sheets.

For offices of the Cole Group, which are specifically set up to receive international goods, please apply all of the foregoing principles with one exception. For these locations, it may be that the freight must be consigned to the customer c/o our location for either convenience or distribution. In these cases, it is acceptable to receive the freight.

**Outgoing Packages and Mail**

It is the responsibility of each employee to ensure that all outgoing packages do not contain any unwanted “materials” prior to closing. Once the package or envelope has been stuffed, it should be sealed and delivered directly to the mailroom. For those offices that do not have a mailroom, please ensure that all packages and mail are protected from the introduction of any unwanted materials prior to pickup. Just as you are responsible for the packing of your airport luggage, you must ensure the security of the package/envelope until such time as it is picked up.

For offices of the Cole Group that are specifically set up to ship international goods, please apply all of the foregoing principles with regard to shipping crates, cartons, pallets etc. International destined freight should be segregated, prior to shipping, to prevent the introduction of unwanted materials.

# Threat Awareness

It is the responsibility of all Cole Group employees to be able to identify and report threats to our person, business or premises.

Although this seems like a difficult subject, there are simple procedures that can be followed to reduce or remove threats to employees, company property and the supply chain. These are detailed below:

1. **Know who you are dealing with**- Always obtain proper ID from drivers, visitors or vendors. Anyone refusing to provide ID should be considered a threat and turned away. If the situation warrants it, contact your immediate supervisor so they may handle the situation. You must always be polite and defer the situation as it becomes necessary. Do not place yourself in a confrontational situation. If there is a perceived threat to your well being or the security of the premises, your manager will take the appropriate measures with the local enforcement authorities.

2. **Report intruders**-Anyone within Cole Group premises must visibly display appropriate visitor ID. If you encounter any unidentified parties, DO NOT confront them. Immediately advise your supervisor or manager. They must handle the situation and contact local law enforcement if warranted.

3. **Know your clients**-Prospective clients must be checked for validity, financial soundness and their ability to meet contractual and security requirements. Be suspicious if an unknown client wants to immediately transact business with us without providing many details or offers to pay large invoices by cash.

4. **Know your service providers**-Service providers must be carefully selected in order to avoid dealing with unscrupulous companies that could pose a risk to ourselves and to the supply chain. A supply chain security questionnaire is being mailed to our vendors.

5. **Telephone security**- Employees receiving telephone calls which are perceived as threats to themselves or to the company must remain calm and try to obtain as much information as possible from the caller. There is a form available to document this. The form entitled “Telephone Security Checklist” is available through your manager. There is also a “Bomb Threat Record Sheet” available. Immediately advise your manager of any perceived or actual threats.

## Threat Awareness, Continued

6. **Verify all documents**- Always ensure that the documents you are given match the goods being transported, cleared and delivered. If the number of pieces exceed those shown on the documents, DO NOT sign for the goods. It's acceptable to contact the parties involved in the transaction for verification on the discrepancy, but this must be prior to receipt of the goods. If the discrepancy cannot be resolved, the goods must be refused. Unless you can properly account for overages, they must be considered a threat.

7. **Package and mail verification**-Perform a quick inspection of any packages or mail upon receipt. Anything that looks suspicious should not be opened. Leave the package alone and notify your supervisor. Some of the suspicious tell tale signs are; oily stains, leakage marks, small holes present, wires sticking out, ticking or buzzing sounds emitted, an unusual odor present etc. Further details are provided in the Security Manual, or refer to the "Mail Bomb Information" and "Suspicious Letter" documentation.

8. **Conveyance inspection**-This applies if your facility handles international freight and you are involved in the loading or unloading of conveyances such as at our Cancon locations. Procedures must be in place to verify the physical integrity of the container, trailer, or railcar prior to loading or unloading. This is to identify any potential deficiencies that could allow the loading of un-manifested, contraband goods. The following seven point inspection process is recommended.

    - Front wall
    - Left side
    - Right side
    - Floor
    - Ceiling/roof
    - Inside/outside doors
    - Outside/undercarriage

    Prior to unloading, it is imperative that the seal integrity is verified. If there is no proper seal affixed, or it shows signs of tampering or its' number does not match what is documented, then there's the potential that the security of the load has been compromised. This must be immediately reported to your supervisor. If any unusual packages or anything out of the ordinary is discovered during the unloading process, then stop and immediately advise your supervisor or manager. Ultimately any discrepancies should initiate an investigation and management must contact the appropriate parties. This may include the CBSA or local enforcement authorities.

## Threat Awareness, Continued

If Cole is loading outbound containers or trailers destined to the USA or other foreign country, then a proper high security ISO/PAS 17712 seal must be affixed upon completion of loading. Again, this is to prevent un-manifested cargo being illegally added.

For additional information for procedures on loading, unloading, seal use and control, please refer the document “The Cole Group Security Seal Policies”.

**Please note: In addition to contacting the appropriate parties and enforcement agencies, all managers must immediately report all security breaches to the corporate Security Manager. This must be followed up in writing with an explanation of the circumstances, including statements from all affected Cole Group employees. Any police reports must also be forwarded.**

# Security Training Confirmation

By signing this document, I confirm that I have read and understand all of the information contained in the Corporate Policy/Training Booklet.

Branch Location (Please Print): _____

Branch Division (Please Print): _____

Name (Please Print): _____

Signature: _____

Date:_____

**IMPORTANT**

**Please ensure that this page is signed and returned to the corporate Security Manager. Make sure a copy is retained at your branch.**