| SUBJECT: | ORIGINATING DEPT: | SECTION: |
|---|---|---|
| INFORMATION SECURITY INCIDENT RESPONSE | SYSTEMS & TECHNOLOGY GROUP | PRIVACY |

| DATE ISSUED: 01-15-09 | SUPERSEDES: New | PAGE: 1 OF 3 |
|---|---|---|
| INITIATED BY: Systems Technology Group ("STG") | APPROVED BY: Legal | |

## I. POLICY/PURPOSE

The purpose of this Policy is to outline how Compass Group (the "Company") provides a coordinated, effective and cohesive approach to privacy and information security incidents ranging from unauthorized intrusions into systems to the mishandling of data in such a way that the privacy, integrity, or availability of confidential information is at risk.

## II. ASSOCIATES COVERED BY THE POLICY

This Policy applies to all the Company associates, temporary service personnel, and consultant/contractor personnel engaged by the Company, or external sources authorized by the Company who have been identified and requested to participate in an incident response situation.

The Incident Response Responsibility Matrix and work flows, supporting documents to this Policy, identifies the process, departments and key stakeholders. Information Systems Security ("IS Security"), Human Resources ("HR") or Legal will be the overall process owner, to be determined on a case by case basis depending upon the underlying security incident.

## III. RESPONSIBILITY FOR ADMINISTRATION

The Systems and Technology Group ("STG") and all levels of management.

## IV. ENFORCEMENT

Non-compliance with this Policy is a security violation and will be reported to management. Depending on the severity of the infraction, a user could lose short term or permanent access to the system, and/or be sent to counseling, suspended or terminated.

## V. PROCEDURES

### A. Identification

**Incident Reporting**
Report all security incidents to **Compass Group Crisis Management Hotline** (1.877.710.6291), which will escalate the incident to the relevant department to obtain clear and documented details of what information will be captured.

## B. Assessment

### 1. Preliminary Investigation

A preliminary investigation will be undertaken involving the appropriate departments, confirming incident details and gathering all critical information. For example, what systems and data have been compromised, financial loss, business disruption, etc.

Depending upon the nature of the data compromise, IS Security will determine the appropriate departments to become involved. Incidents typically involve IS Security, Legal, HR, Corporate Communications, Treasury, Operations, and client representation. As supporting documentation to this Policy, the *Incident Response Responsibility Matrix,* defines specific protocol for departmental involvement.

### 2. Primary Investigation

Once the preliminary investigation is complete, the IS Security team, in coordination with other appropriate departments/parties, will determine if a primary investigation will be required. IS Security will then contact the appropriate parties (client's IT departments, field operations, etc) and perform an incident validation and assessment. This may also involve an approved third party IT incident assessment and response provider, depending on the findings thus far.

As part of the primary investigation, the IS Security team, in coordination with appropriate departments/parties, will make the following determinations:

- **Response Tactics** – how best to address the incident and what parties should be involved in the response.
- **Senior Management Approval** – approval in coordination with the following departments (dependant upon incident) but in general. STG, Legal, HR, Corporate Communications, Treasury, Senior Operators.
- **Fully Define Scope of incident** – establish and identify source of compromise, determine timeframe and what specifically is at risk.

As part of the supporting documentation to this Policy, the *Incident Response Process* defines the primary investigation in greater detail.

## C. Containment

### 1. Isolate Problems

IS Security will immediately identify all areas of intrusion, working in coordination with an approved third party IT incident assessment and response provider.

### 2. Reporting the Incident

Depending upon the nature of the data compromise IS Security will determine reporting requirements in consultation with relevant departments, such as Legal, Corporate Communications, Treasury, etc.

## D. Remediation

### 1. Resolution

IS Security will facilitate agreement to the remediation plan among all relevant departments/parties, coordinate all agreed-upon remediation steps to the incident, and ensure all appropriate parties are engaged.

### 2. Lessons Learned

Following the incident, all involved departments will engage in a lessons learned session in an attempt to identify and improve any part of the incident response process.