

PERSONNEL SECURITY

Section: Security	Effective Date: <Effective Date>	FIRST RELEASE
Policy Number: POLICY IS013	Date Last Approved by Board: <Approved Date>	Prior Policy Number: N/A
Department: Management	Initial Policy Date: <Initial Policy Date>	Prior Effective Date: FIRST RELEASE

POLICY STATEMENT

<Company Name> is dependent on the reliable support it receives from its staff and contractors. To ensure a safe work environment and foster staff participation in the protection of confidential information, <Company Name> has adopted the following policies for personnel security.

HIRING PRACTICES:

<Company Name> Human Resources Department (HR) in conjunction with Management will deploy and enforce the following personnel policies.

- Each new hire granted access to client information and other confidential <Company Name> data will undergo a background check. Any past activity that would subject sensitive systems and data to risk due to an employee's past behavior will be cause to terminate the employment relationship with <Company Name>.
- Prior to granting access to sensitive systems and data, all new hires will receive orientation and training that include responsibilities for protecting confidential information. (Currently this process is done by the manager and not the employees. A new employee does not know what to request).
- The new employee's supervisor must approve access to systems on a "business need to know" basis and submit the **Systems Access Request Form** to both IT and HR for processing.
- The new employee must sign a **Statement of Understanding Form** and the **Systems Access Request Form** acknowledging acceptance of responsibilities contained in the <Company Name> security policies.
- The IT Department will enable access to only those systems approved on the Systems Access Request Form and submit a copy of the completed form to HR for filing.
- All new hires must execute a Confidentiality Agreement to protect <Company Name> sensitive and confidential information.
- Temporaries and independent contractors will be given access to only that data necessary to complete their identified tasks, provided that such Temporaries and independent contractors first sign a Confidentiality Agreement, the Systems Access Request Form and the Statement of Understanding Form.

TRAINING

Department managers, with IT Department oversight, are responsible for instructing new and existing end-users regarding their department's utilization of <Company Name>'s Information Technology. The **IT Department** is responsible for informing end-users of pending operational changes and assists them once the changes are in place.

New Hire Orientation: Each new-hire will complete an orientation session where <Company Name> policies and procedures are reviewed. Moreover, these employees will receive network training as well as training for the use of the systems and applications required to perform their job functions.

In-House Instruction: All staff will be trained on the security, compliance, and proper procedures to effectively use <Company Name>'s information systems and applications required to perform their duties. Our staff will also receive periodic security awareness training including the importance of protecting sensitive information. This training is performed as new systems or enhancements are introduced or may be periodically performed in order to ensure that the staff is following the established policies, procedures and guidelines.