**Screening**

The screening is the process of verifying a candidate’s credentials and suitability for the job prior to offering a position in HiQuSystems.  Most often this is in the form of a background check.  The general idea is to make sure that former criminals are not hired or placed in positions of trust within the organization.  But employee screening can take on many different levels, depending on the nature of the organization and the position being screened. The best approach is to check the reference from one or more previous employers. This should provide good information to make determination to hire or leave the candidate.

**Contracts**

This is important to have non disclosure clause in the contract and employee is fully aware of the consequence incase of violation of any clause of the contract and to take action against employees who violate security policies.  Controls related to contracts include employment agreements, non-compete agreements, non-disclosure agreements and intellectual property agreements.  Contracts are designed to protection intellectual properly from being stolen or lost.

**Security Policy Acknowledgement**

Every employee or contractor with access to information must be made aware of the information security policies that apply to them.  In most organizations, this includes a high-level “Code of Conduct” as well as acceptable use policies such as Internet Acceptable Use.

The acknowledgement section must make certain that employees formerly acknowledge that they have read and understood the written policies.

**Security Education**

The employees must be trained and educated on the basic security information and common threats for breach of data. This is recursive and must be performed periodically.

**Monitoring**

Although employees are by definition trusted by the organization, their behavior still must be monitored at some level.  The type and level of monitoring depends on many factors, including the sensitivity of the data being used, the overall security posture of the organization, or even government requirements.  At a minimum, the organization should monitor all security-related user activity on systems.  Many organizations choose to monitor internet and web traffic.

**Termination Procedures**

The final essential component of personnel security is having proper termination procedures in place and enforced.  Once an employee is no longer employed (or has indicated that they are going to leave), both logical and physical access must be terminated.  In addition, the exit process usually involves the return of organizational property such as laptops or access badges.