Information Security Plans are to be developed and documented for IT applications, as per the Company's Information Security Policies. This template is to be used as a guide in developing individual security plans for application and infrastructure systems.

A security plan should include at minimum a description of the various security processes for the system, procedural and technical requirements and organizational structure to support the security processes. The Security Plan should describe the security needs and processes for the 'Life Cycle Support' of the system.

A risk assessment should be performed first. Identifying risks provides guidance on where to focus the security requirements. Security requirements and controls should reflect the business value of the information assets involved and the consequence from failure of security. Security mechanisms should be 'cost beneficial', i.e., not exceed the costs of risk.

**Process:**

This Security Plan Template is to be incorporated into the Project Management Methodology. Security Plans will be developed, using this template, as part of new systems development projects and major upgrade projects. A Security Plan for the application will be a deliverable for each new system or major upgrade.

The Security Plan will be initiated in the early phases (business analysis and requirements) of a project, and completed before the system is migrated to production.

This template can also be used to document security plans for current systems, where such documentation does not exist and management directs that security plans be documented for certain applications.

**Information Security References:**

When developing and documenting the Security Plan for a system, keep the following in mind for each section.

1. Information Security is made up of a number of technical, operational and management components, in various layers, all working in coordinated and integrated processes.

> *Management Controls* address security topics that can be characterized as managerial. They are techniques and concerns that are normally addressed by management in the organization's computer security program.
>
> *Operational Controls* address security controls that focus on controls that are primarily implemented and executed by people (as opposed to systems).
>
> *Technical Controls* focus on security controls that the computer system executes. These controls are dependent upon the proper functioning of the system for their effectiveness.

2. Information security is defined as the assurance and protection of:
   a) Confidentiality: ensuring that information is accessible only to those authorized to have access;
   b) Integrity: safeguarding the accuracy and completeness of information and processing methods;
   c) Availability: ensuring that authorized users have access to information and associated assets when required.
   d) Reliability: increasing the reliability of systems and information.

3. Refer to the Information Security policies and architecture.

***System Security Plans are COMPANY Confidential. Handle accordingly and limit distribution per COMPANY's Data Classification policies and guidelines.***

| **Information System Security Plan**<br>System Name: | |
|---|---|
| **Application Name** | |
| **Brief Description**<br>Brief description of business function, purpose | |
| **Application Data Owner(s)**<br>Use position titles, departments, business area names – don't use people's names | |
| **Business Area/ Department**<br>Use departments, business area names and location names | |
| **Summary of Hardware / Software**<br>Microsoft Windows O/S, SQL, C++, Compaq, Dell, HP, etc.; how many, locations | |
| **For each of the following, please provide description and sufficient details of the processes, procedures and requirements for providing and maintaining security over the application system and its related data. Please review the various Information Security policies for further guidance on requirements. This Plan is not a procedures document; as needed, refer to specific procedures documents.** | |
| **Overview of Security Requirements and Processes**<br>One or two paragraphs describing overview of security requirements, processes | |
| **Legal / Regulatory Requirements for Security / Privacy**<br>SOX, GLBA, HIPPA, FDIC, SEC, privacy laws, etc. – indicate what laws or regulations affect this system and data, how they affect it | |
| **Confidentiality Requirements / Data Classification**<br>Describe confidentiality issues and requirements; Classify the data as confidential, internal, public – refer to Company Data Classification and Information Security policies. | |
| **Administration, Roles & Responsibilities for Security Functions**<br>What position administers the userids - is it centralized? Business area or IT Security Administration? Who (position title) approves access requests? What positions are responsible for the various security functions; indicate positions by job title, and indicate responsibilities by role and or position? | |

| Information System Security Plan<br>System Name: | |
|---|---|
| **Access Requirements and Restrictions**<br>Describe access rules and requirements; what types of employees can access which data elements. Will access be by 'roles', groups? What access restrictions are there? What 'external' users need access? What requirements for external access into the Company's network/systems?<br><br>Access permissions - how are these done, authorization process, overview security administration procedures?<br><br>Also, consider these questions:<br><br>What are the data security access levels? Are there varying levels of security access for different types of transactions:<br>• inquiry only<br>• update non-monetary transactions<br>• update financial transactions<br>• add/delete records<br>How do the roles and accesses permissions provide proper segregation of duties? | |
| **Security Logging and Monitoring**<br>Describe the security and access logging processes, transaction logging, review of security exceptions, monitoring of security events, log review processes. Logging can be at O/S, database and application levels. | |
| **Security Training**<br>Security awareness and security administrative process training, initial training, new user and ongoing security training plans. | |
| **Security Testing**<br>Initial implementation and periodic testing to ensure ongoing compliance to security requirements – should link to QA testing and Change Management processes, also periodic security assessment reviews. | |
| **Infrastructure, Telecommunications and Environment Security Components**<br>Dependencies, interaction with firewalls, router configuration or ACL's, intrusion detection, anti-virus, system logging, operating system security settings/configurations, network segregation, Web application based security requirements, configurations for web application/DMZ, secure telecommunications, SSH, HTTPS, etc. | |

| Information System Security Plan<br>System Name: | |
|---|---|
| **Backup and Disaster Recovery Requirements**<br>Availability requirements for system, backup requirements/frequency, DR requirements – brief description here, refer to the specific DR Plan for details. Data retention requirements. Restart requirements | |
| **Remote Access Requirements**<br>What restrictions/allowances for remote access by users; any modem requirements for vendor or technical support; how should any remote access by controlled, logged, monitored? | |
| **Physical Security**<br>Where are the physical components for the system, what physical security requirements are needed; What secure room/computer facility to be used; controls, logging and monitoring of physical access to computer hardware, data backups, etc | |

| Document Control Section | |
|---|---|
| Version Number | 1 |
| Prepared By | |
| Issued By | |
| Approved Date | 9/25/2018 8:16:00 AM |
| | |

***Application Security Plans are COMPANY Confidential.***