SAMPLE SECURITY PLAN

1.0 Introduction

1.1 Purpose

The purpose of this document is to describe the Company's Security Management System. The Company is committed to the safety and security of our employees, the customers we serve, and the general public. We urge all employees to help us implement this plan and to continuously improve our security efforts.

1.2 Background

The management principles presented in this document are derived from the Company's philosophy and commitment to the Quality process. It creates the framework that all Company employees should follow in their operations with regard to Security.

1.3 Revision

Revisions to this document may be made only through Company management and according to the Company's document control procedures.

2.0 Overview of System

2.1 Five components in the Security Management System

The Company's Security Management System is based on a quality management system that contains the following five components:

- POLICY
- ORGANIZATION
- PLANNING AND IMPLEMENTATION
- MEASURING PERFORMANCE
- AUDITING AND REVIEW

Within each of these components, the Company has incorporated the following twelve aspects, which are essential to the success of the framework objectives.

2.2 Twelve essential aspects of a successful Security Management System

A. STRONG MANAGEMENT COMMITMENT

- A Security policy must be given to all new employees.
- Senior management committees must review all security incident reports.
- Top management must allocate resources for security support and training initiatives.

B. WORKING SAFETY POLICY

The Company has developed security policies and procedures according to industry, regulatory, and internal standards.

C. EMPLOYEE INVOLVEMENT

The Company has designed a Security Management System that involves all levels of employees and subcontractors. Lines of communication are established to ensure every person is able to participate.

D. SECURITY - LINE ORGANIZATION RESPONSIBILITY

- It is the Company's philosophy that every employee is responsible for security and has the authority to ensure security as appropriate.
- All job descriptions will include specific security performance responsibilities. How well these responsibilities have been fulfilled will be a basis for evaluating individual performance.
- Supervisors and managers are given the responsibility and authority to actively manage and ensure the Security System's implementation and effectiveness.

E. SECURITY GOALS AND OBJECTIVES

The Company's management establishes security objectives annually. Based on these, action plans are defined by relevant line management to ensure correct implementation. Security meetings are structured to ensure that the implementation is monitored and adapted accordingly.

F. SUPPORTIVE SECURITY PERSONNEL

- The Security Manager has the responsibility to direct and support the efforts of the Security System.
- All employees are expected to support and work within the Security Management System by participating in management, review, and employee committees.

G. COMPREHENSIVE INCIDENT INVESTIGATION

All security incidents must be recorded. Identifying the root causes of these incidents is critical to preventing recurrence of unsecure conditions. Engineering and procedural controls will be examined and modified as necessary.

H. EFFECTIVE COMMUNICATION

The Company believes that communication is the most important component in the success of its Security Management System. Communication occurs in several different ways:

- security meetings and training.
- effective security assessments and audits.
- incident reporting and review processes.
- emergency and contingency plans.

I. COMPETENCE, SELECTION, AND TRAINING

- Management is responsible for selecting personnel and subcontractors based, in part, on their experience with and training on security issues. Every employee chosen must demonstrate the highest level of competency.
- The United States Department of Transportation regulations require employees of this Company (including senior management and independent contractors) who work with hazardous materials (HAZMAT) to be trained in security awareness. Employees must also receive in-depth training regarding our Company's Security Plan.

- Managers are responsible for ensuring that each employee's proficiency level is documented.

J. HIGH STANDARDS OF PERFORMANCE

- The security policy statement establishes a high standard of performance all employees must strive to reach.
- Meaningful participation is required of each employee. Participation will be evaluated using performance appraisal systems.

K. POSITIVE MOTIVATION

- Management and supervisors submit incidences of positive security performance to top management for appropriate recognition from top management.
- Employees who display leadership and exceptional performance in security functions will be rewarded.

L. EFFECTIVE SECURITY AUDITS

- Site-specific security inspections are performed by site managers, supervisors, and security representatives. The results are reported to management with ongoing updates regarding the completion of action items.
- The security department and third-party independent auditors perform periodic security audits and provide formalized audit recommendations. These recommendations are monitored for completion by both security and operations management.

3.0 Company Secuirty Policy Statement

The Company's commitment is communicated in the following policy statement, which is given to all employees and subcontractors. This document states the commitment of top management, empowers employees, and establishes a teamwork environment in which every employee is responsible for security. Copies of this policy can be found in each office and on each site.

SECURITY POLICY STATEMENT

The Company is dedicated in providing a safe and secure workplace for its employees through the active implementation of an effective Security Management System. At all times, security aspects of operations are an integral part of how we do business and will always be paramount in importance to other business objectives.

The company establishes security procedures that meet or, in some cases, exceed industry standards and governmental regulations in order to protect the interests of employees, customers, the public, and the environment. To accurately refine these as needed, the company actively participates with industry in developing standards and promoting security issues.

Communication, awareness, and participation in the security process are key ingredients to the success of a Security Management System. Therefore, all employees and, when applicable, customers, contractors, and visitors, are expected to attend security meetings, participate in internal auditing of their respective operations, attend security review meetings, and generate a level of heightened communications with regard to security practices. All employees are actively encouraged to achieve defined security objectives and standards. These standards are regularly reviewed and appraised.

Line management must ensure that employees and contractors are aware of and have access to copies of all regulatory requirements, company policies, and procedures. These employees must also have the appropriate training to comply with these requirements.

All employees are required to familiarize themselves with and adhere to company policies, procedures, and safe work practices. In addition, each individual will have the opportunity to provide input to operations by means of safety and security meetings and the Company's open door policy regarding all security issues. The Company acknowledges that it is only through the freedom to make comments, and through a flow of information, that risks may be identified and minimized.

Employees are also encouraged to reduce risk by identifying unusual or suspicious behavior and reporting these observations to their supervisors. Company management will ensure the proper action is taken and that reasonable attempts are made to reduce or eliminate hazards and security risks. Employees who bring such matters to the Company's attention will be rewarded.

_____

President

4.0 Company Security Organization

4.1 Organizational chart

The Company's security organizational chart coordinates all parties necessary for a successful Security Management System.

4.2 Defined authorities and responsibilities

The following list has been developed to provide defined authority and responsibilities for all levels of employees:

PRESIDENT

- Communicate to top management throughout the company that all security breaches are preventable and that all reasonable measures shall be taken to identify and reduce security risks.
- Ensure top management is actively participating in a security management committee that will provide direction to the security process.
- Establish an open door policy for all employees that ensures each employee recognizes his or her importance in security issues.
- Ensure that all managers use measurable security goals when they appraise their own performance as well as the performance of their employees.

VICE-PRESIDENT-OPERATIONS

- Provide consistent management commitment with the understanding that all security breaches are preventable.
- Support the open door policy.
- Ensure that sufficient human and financial resources are available to provide the necessary support for the Security Management System. This includes, but is not limited to, the selection and training of personnel, purchasing security resources, and implementing security procedures.
- Participate in the security management committee.
- Require security incidents to be reported in order to uncover root causes.
- Ensure that the loss control program assigns economic responsibility to the individual departments who directly control the activities that incur any loss.
- Require all managers to participate in appropriate performance appraisal systems.

SECURITY MANAGER

- Advise management on statutory, corporate, and industry standards and practices governing secure systems at work.
- Work with Human Resources to designate who is in charge of security for the company and at each facility.
- Design security systems and operating procedures that minimize loss. These should include threat vulnerability assessments as well as any adjustments to standard procedures that are necessary when the National Threat Level changes.
- Develop and review security policies and procedures that comply with corporate and local regulatory requirements.
- Work with the Security Review Committee to review security incidents and advise management on ways to reduce risk.

- Represent the Company's interests regarding security to industry associations.
- Perform contractor security audits to ensure compliance with security system requirements.
- Represent the established Security Management System to customers.

OPERATIONS MANAGEMENT

- Emphasize the belief that all security breaches are preventable and support the open door policy of top management.
- Ensure sufficient human and financial resources are available to support the Security Management System. This includes, but is not limited to, the selection and training of personnel, purchasing security resources, performing security risk assessments, and implementing security procedures.
- Ensure that compatible security policies and management systems are developed with contractor management and security requirements are contained in contractual agreements.
- Participate in security reviews or management committees.
- Ensure that mechanisms are in place to accurately report security incidents and that root causes are investigated and understood..
- Ensure that employees review the Company security procedures and follow the guidelines.
- Ensure that all employees develop action-based security goals.
- Be aware of all statutory and contractual security requirements.
- Ensure department security inspections are performed by departments and individual employees.
- Arrange required security meetings and drills and report the outcomes.
- Report all security incidents and take all the initial actions necessary to render the situation safe.
- Promote positive communication and teamwork among personnel and contractors with regard to security issues.
- Ensure that all employees and contractors have security training, as required to comply with governmental regulations and the Company's internal requirements, including procedures for authorized and unauthorized access, facility security, enroute security (where applicable), emergency response procedures, and incident reporting.
- Work with security management on all issues related to a safe and secure work environment.
- Provide minutes of all security meetings and follow-up on action points and audit findings on an ongoing basis.

HUMAN RESOURCES MANAGER

- The Human Resources Manager will perform employment background checks according to regulatory requirements. These checks must be performed in a confidential and secure manner and in compliance with all relevant Federal and state regulations.
- The Human Resources Manager will work with the Security Manager and Operations Managers to ensure all pre-employment and post-employment security measures are met.

CONTRACTORS

- Become familiar with and agree to follow the Company's security policies and procedures.
- Participate in pre-contract safety reviews with security management to ensure compatibility between the Company's secure working practices and the contractor's.
- Report all security incidents to Company management.
- Ensure that all employees are selected and trained according to recognized industry and regulatory standards.
- Participate in audits of company practices in safety and security issues.

EMPLOYEES

- Become familiar with secure work practice standards and comply with them.
- Be aware that security is every employee's responsibility.
- Report all security incidents, however minor, that resulted, or could have resulted in injury or physical damage.
- Participate in security meetings and drills.
- Work with management to develop security goals and performance indicators in their performance reviews.
- Follow appropriate security procedures according to the security alert level in effect.

5.0 Planning And implementation

5.1 Policies and procedures

The Company follows all the guidelines in our policies and procedures. Security meetings and bulletins will be used to update employees about changes in policies and procedures.

All policies and procedures will be made available to employees based on the recognition of hazards and or governmental requirements.

5.2 Competency arrangements

It is imperative that personnel and subcontractors who work for the Company have a level of competence that ensures the technical integrity of their operations, particularly in security matters. The Company's established competence assessment process provides management with a standardized method for choosing the right employees, orienting each employee in their job, and evaluating individual performance.

Selection of Personnel

Personnel who are selected to work for the Company are evaluated through a formal selection process. The requirements of prospective employees are determined by the responsibilities and accountabilities they will have while performing their job.

Management is responsible for proper selection based on an assessment of the applicant's technical knowledge and the skills required for the position.

Management works with internal human resources and external customers and contractors to ensure adequate needs assessments have been performed. All personnel decisions must be documented.

Orientation

Both job specific and general security orientations will help ensure all company employees and outside contractors are adequately informed about the environment in which they will be working. Orientation will also educate each individual about the Company's security system, policies and procedures, any hazards present in the workplace, and the process used to control those hazards.

Management is responsible for orientation.

Evaluation of Individual Performance
Management must evaluate individual employee performance based on the competency assessment developed for each position and the employee's performance objective goals. The evaluation should also include future goals and objectives.

The Company measures the employee's success in the Security Management System according to the employee's active participation in the security management process. Based on this evaluation, management arranges the necessary personnel training action plan to develop the employee's skills and knowledge.

Contractor competency profiles are periodically reviewed by the Security Manager to determine if any changes are necessary in order to stay current.

5.3 Contractor Security Management Systems

The importance of consistent Security Management Systems between the Company and its contractors is critical to the success of the professional relationship.

The Company evaluates contractors' security systems based on the same framework it uses to evaluate its own. Contractor security systems are periodically reviewed and compared to the Company's to ensure compatible systems are in place.

5.4 Security risk assessments

Managers are required to organize work teams to develop and maintain security risk assessments. These assessments will identify and prioritize security vulnerabilities. Steps to reduce these risks to the lowest possible levels are identified.

The Security Manager is responsible for providing consultation where necessary during the risk assessment.

5.5 Site-specific plans

Each site needs a specific security plan that addresses the unique factors present at its location. Therefore, each site must do the following:

1. **Form a security committee**
   Form a security committee that will define specific responsibilities for implementing site-specific security procedures and develop an action plan. The committee must be comprised of appropriate representatives from all partners and contractors involved.

2. **Meet with customers**
   Hold meetings with customers to do the following: review all applicable areas of the customer's security management system; determine what pre-contract safety training must be completed for each job position; analyze the customer contract to find any information that would affect the development of a site-specific security plan.

3. **Implement any necessary changes**
   Based on the customer meeting, the team must determine what changes will affect the Company's system. Appropriate revisions are made and implemented where necessary.

4. **Adjust criteria**
   Competency, selection, and training criteria are adjusted to align with identified requirements.

5. **Formalize a contingency plan**
   A contingency plan must be formalized. This plan must account for specific emergencies that may occur as well as the normal pieces of equipment, personnel, and substances introduced into the working environment.

6. **Have a pre-contract security meeting**
   Based upon the security team's review and planning described above, pre-contract security meetings are held with all employees and contractors expected to work throughout the duration of a contract. Site-specific action plan items and procedures developed to address specific security hazards must be covered.

7. **Review after every contract**
   After every contract is completed, the security committee will review the security performance of the contract and adjust the procedures to improve, where necessary, the action plans.

6.0 MEASURING PERFORMANCE

6.1 Goals and objectives

Management and Supervisors are responsible for developing appropriate goals and objectives for the organization and for employees.

Organizational goals

Organizational goals are established to meet the standards of the Company's Security Management System. Organizational goals provide the framework for implementing secure work systems, and they help managers delegate responsibility to other parties when necessary.

Employee goals

All employees have goals and objectives relating to security. Performance against these goals is measured and used in any assessment of the individual for promotion or other change in job function. These goals must include measurable actions that will help the employee recognize and prevent security breeches.

6.2 Performance reviews

Performance reviews have been implemented to measure the achievement of individuals from both a team and an individual perspective. Employees are reviewed throughout the year to ensure that performance targets are being met and that any necessary adjustments are being made.

7.0 AUDITING AND REVIEW

7.1 Company and contractor audits

The Company arranges for independent third party audits of its own Security Management System and that of contractor's once a year to ensure that the system is operating as established. Contractor personnel and management review these audits, prioritize audit items, and produce a plan to adjust the Security Management System. Line management both internally and within contractor companies should report results to the security department to ensure all items are complete.

7.2 Bridging document

The security manager must design a bridging document for each contractor. The bridging document helps the contractor identify compatible Security Management Systems. This enables the Company to identify congruencies with customers, industry, and the government. The bridging document is reviewed with relevant security personnel and the resulting information communicated to management and contractors.

7.3 Continuous improvement

The Company is committed to continuously improving the Security Management System.