1.0 Purpose:

1.1 To provide an organizational framework to establish and foster the development of a positive and robust Agency-wide safety culture.

1.2 To establish a structured management approach to identifying hazards, assessing their risk level, communicating to the appropriate department(s) regarding risks, monitoring corrective actions by department, and taking action to eliminate or mitigate and manage risks to the lowest practicable level.

Source documents used in the creation of this Hazard Management Plan are:

- Department of Defense: Standard Practice, System Safety MIL-STD-882E
- U.S. Department of Transportation, FTA Office of Safety and Security: Hazard Analysis Guidelines for Transit Projects.
- U.S. Department of Transportation, FTA Office of Safety and Security: Transit Safety Management and Performance Measurements.
- U.S. Department of Transportation, Research and Innovative Technology Administration: Transit System Safety.

2.0 Scope:

Applies to all Santa Clara Valley Transportation Authority (VTA) employees, consultants and contractors. Although this procedure is heavily weighted toward identifying, assessing, eliminating or reducing, and managing risks inherent in the maintenance and delivery of bus and rail transportation, the concepts and processes apply to all VTA activities.

3.0 Responsibilities:

3.1 The General Manager and all VTA Managers and Supervisors are responsible for:

3.1.1 Fostering an Agency-wide culture of safety.

3.1.2 Giving safety, security and risk management due consideration throughout all decision making processes.

3.1.3 Consulting with the Safety Department on new construction projects and/or projects involving configuration management.

3.1.4 Actively promoting safety and safe work practices in both written and verbal communications.

3.1.5 Establishing and maintaining the expectation of frequent safety and performance measurement checks to ensure all established rules and procedures are being

adhered to and to facilitate progress toward achieving established safety goals and objectives.

3.2 All VTA employees, consultants and contractors are responsible for:

3.2.1 Maintaining high standards of safety in the performance of daily job functions.

3.2.2 Maintaining high standards of safety and system assurance throughout the planning, design, construction, fabrication, installation, testing, pre-operational, and operational system phases of all VTA projects and activities.

3.2.3 Promptly reporting any known hazards and/or potential or perceived hazards to their direct supervisor and Transit System Safety and Environmental Health and Safety (Safety Unit) within the Safety and Security Department.

3.2.4 Promptly implementing corrective actions, once determined and agreed upon, to eliminate hazards or mitigate them to the lowest practicable/achievable level.

3.2.5 Managing risks (that cannot be completely eliminated) through the life cycle of the system and/or condition.

3.3 The Safety Unit is responsible for:

3.3.1 Identifying hazards through inspections, internal audits, accident/incident investigations, safety rule violation investigations, and hazard reports.

3.3.2 Documenting and investigating hazards reported by any VTA employee, VTA department, consultants and contractors and/or member of the general public.

3.3.3 Preparing hazard analyses to address hazardous conditions and recommending corrective actions to mitigate hazards.

3.3.4 Notifying California Public Utilities Commission when an identified hazard is categorized as high risk.

3.3.5 Reviewing accident/incident reports.

3.3.6 Providing technical support and oversight of VTA safety training and education programs.

3.3.7 Providing oversight and support of VTA's hazardous materials and environmental compliance program.

3.3.8 Providing administrative support and oversight for annual safety audits.

3.3.9 Performing environmental compliance audits as required.

3.3.10 Maintaining the Occupational Injury and Illness Prevention Program (IIPP).

3.3.11 Participating in the review of plans, specifications and drawings for buildings, facilities equipment, and vehicles to ensure compliance with established and accepted industrial and public safety standards and codes and to identify any potential hazards created by proposed designs and specifications.

3.3.12 Maintaining a master Hazard Tracking, Corrective Action and Resolution Matrix.

3.3.13 Maintaining liaison between VTA and external safety regulatory agencies and ensuring compliance with applicable local, state and federal codes and regulations.

4.0 Procedure:

Safety is of the utmost importance in all VTA activities. VTA is committed to developing, implementing, and improving strategies, management systems and processes to ensure that all of our administrative, construction, transportation and maintenance activities uphold the highest level of safety performance and meet or exceed national and industry standards.

4.1 Hazard Reporting Statement

To establish a systematic and proactive safety management system approach in recognizing and identifying real and/or potential hazards before they lead to accidents/incidents, the entire chain of events that if left unbroken could lead to a serious incident must be recognized, analyzed and understood. In order to implement preventative mitigations and safety measures to avoid the one (1) serious injury accident, the Safety Unit must continually gather as much hazard data and information as possible to build and maintain a comprehensive database, which can be used to establish baseline metrics, performance objectives, and to assess hazard trends based on specific activities, environments, and conditions. To achieve this goal, it is imperative that VTA employees have uninhibited reporting of all potential and/or real incidents and occurrences that may compromise the safety of VTA activities. To this end, VTA's Hazard Reporting Statement is as follows:

4.1.1 Every employee, regardless of classification, is responsible for communicating to their immediate superior any information that may affect the integrity of safety (near miss, unsafe behavior, unsafe conditions, rule violation, etc).

4.1.2 The immediate superior (supervisor, manager, director and/or chief) is responsible for communicating to the Safety Unit any safety information reported to them by their staff or which they've observed themselves.

4.1.3 VTA will not take disciplinary action against any employee who discloses a near miss incident or an occurrence involving safety or safety rules or procedures violations (This applies if the disclosure involves the first offense of a safety rule

or procedure violation self-reported by the employee involved. VTA may choose to take disciplinary action in response to subsequent incidents or occurrences of a like or similar nature. However, if subsequent incidents are again self-reported by the employee involved, the resolution will be mitigated or eliminated.) This policy shall not apply to information received from a source other than the employee involved, or which involves an illegal act, or a willful and deliberate disregard of established and promulgated rules, procedures, policies and regulations.

4.1.4 Whistleblowers shall be protected from any form of retaliation, consistent with State and Federal guidelines and regulations.

4.1.5 The Safety Department's program of collecting, recording, analyzing and disseminating information obtained from hazard reporting shall protect, to the extent permissible by law, the identity of any employee who provides information involving safety.

4.1.6 All VTA staff is urged to use the Hazard Reporting Program to assist VTA in becoming a leader in providing our patrons and employees with the highest level of safety.

4.2 Hazard Identification

4.2.1 There are four (4) basic elements of a System, each of which can contribute to the manifestation of a hazard:

- People (employees, consultants, contractors, patrons, the general public);
- Procedures (training, policies, rules, maintenance programs);
- Environment (weather, geography, landscape); and,
- Facilities (offices, maintenance shops, vehicles, bus stops/shelters, rail stations/elevators/escalators/shelters).

4.2.2 There are five (5) basic methods of Hazard Identification:

- Review of design data and drawings – this is the most preferred method, as the potential hazards and risks can be proactively identified and designed out of the system prior to the system being built;
- Formal hazard analysis techniques (*see Appendix 7.1, Hazard Analysis Schedule*):
  - Preliminary Hazard Analysis (PHA) – This is the first, most basic type of hazard analysis and is performed during the design phase of a project. This

phase begins with the decision to build and ends and at the onset of preliminary design.

- System Hazard Analysis (SHA) – This is a systematic study, performed during all phases of the life cycle of a system, to identify hazards and make recommendations for their elimination or control.
- Subsystem Hazard Analysis (SSHA) – This is a study of how safe a system is by looking at the sub-systems. An example might be doing a System Hazard Analysis on a bus by looking at the sub-systems, such as braking and propulsion. Sub-systems can be broken down further until you get down to the most basic level.
- Operating Hazard Analysis (OHA) – This is performed to identify hazards in an established system that may arise during operation of said system. The goal is to find causes of these hazards and recommend risk reduction alternatives.
- Software Safety Analysis (SSA) – This is performed to identify hazards created by software through undesired and unexpected outputs.
- Failure Modes and Effects Analysis (FMEA), also known as Fault Tree Analysis (FTA) – This is performed by analyzing a set of events arranged in systems to identify and prevent undesirable outcomes. This is a very formal analysis using "if/then" tests to organize events into a series of logical progressions in order to come up with an unwanted outcome.
- Security Analysis (SA) / Threat and Vulnerability Assessment (TVA) – This is performed to assess how different system components can be arranged to result in specific security incidents.

- Scenario development and judgment of knowledgeable personnel (example: table-top and live drills and exercises);
- Generic hazard checklists (example: monthly facility inspection forms); and,
- Data from previous accidents (case study) or operating experience – this is the least preferred method, as it is entirely reliant upon reactive processes; though in combination with proactive measures this method can be an effective means of hazard identification, mitigation, and risk management.

4.3 Hazard Analysis

A hazard, once identified, must be resolved by either eliminating or reducing the risks posed by the hazard. Decisions regarding the resolution of hazards are based on the assessment of the risks involved.

4.3.1 Hazard Severity:

This is a qualitative, if not somewhat subjective measure at times, of the worst credible accident/incident that might occur if the hazard is left unaddressed. Case study, data analysis, experience and institutional memory can make this assessment more objective, but there remains an element of "craft" in reaching the most appropriate severity assessment. Severity Categories are as follows (*see Appendix 7.2* for Severity and Probability Categories Charts):

- **1 –** Catastrophic: death, system loss, or severe environmental damage.
- **2 –** Critical: severe injury or occupational illness, or major system or environmental damage.
- **3 –** Marginal: minor injury or occupational illness, or minor system or environmental damage.
- **4 –** Negligible: less than minor injury or occupational illness, or less than minor system or environmental damage.

4.3.2 Hazard Probability:

This is a qualitative measure of the likelihood that a hazard will occur. Again, case study, data analysis, experience and institutional memory can assist in making the probability assessment more objective, but an element of subjectivity still exists. Probability Categories are as follows (*see Appendix 7.3* for Severity and Probability Categories Charts):

- **A** – Frequent: likely to occur frequently to a specific, individual item or likely to be continuously experienced by the system, fleet or inventory.
- **B** – Probable: will occur several times in the life of a specific, individual item or likely to be experienced frequently by the system, fleet or inventory.
- **C** – Occasional: likely to occur sometime in the life of a specific, individual item or likely to be experienced several times by the system, fleet or inventory.
- **D** – Remote: unlikely, but possible to occur in the life of a specific, individual item or unlikely, but can reasonably be expected to be experienced by the system, fleet or inventory.
- **E** – Improbable: so unlikely, it can be assumed occurrence may not be experienced by a specific, individual item or unlikely to occur, but may be experienced by the system, fleet or inventory.

4.3.3 Hazard Resolution Matrix (*see Appendix 7.3)*:

The assessed hazard severity and probability for any hazard are combined to determine whether the hazard is acceptable or unacceptable.

If a hazard has been assessed as posing a category 1 severity and a category A probability (1A), the hazard is an unacceptable condition that must receive immediate mitigation to protect against imminent death, system loss or severe environmental damage.

If a hazard has been assessed as posing a category 4 severity and a category E probability (4E), the hazard is acceptable and poses very little risk.

Hazards assessed as 1A, 1B, 1C, 2A, 2B, and 3A shall be reported to VTA's California Public Utilities Commission Representative.

4.4 Hazard Reduction:

There are four (4) basic methods of Hazard Reduction. Listed in order of precedence (although frequently they must be used in combination), the four (4) methods are:

4.4.1 Design for minimum risk – design, redesign or retrofit to eliminate the hazards from the system through design selection. If a hazard cannot be completely eliminated, utilize design selection to reduce the probability and severity of an occurrence to an acceptable level. This can be accomplished through the use of failsafe devices and design principles and standards.

4.4.2 Incorporate safety devices – hazards that cannot be completely eliminated or controlled through the design process can be controlled to an acceptable level through the use of fixed, automatic, or other protective safety features, such as machine guards, protective enclosures, safety pins, interlock features or pilot bars on light rail vehicles. It is important to note that care must be taken to ascertain that the implementation and/or operation of safety devices do not introduce any additional hazards. Provisions should be made to perform periodic functional checks or audits of safety devices.

4.4.3 Provide warning devices – when neither design nor safety devices can effectively eliminate or mitigate a hazard, warning devices can be utilized to detect the condition and generate an adequate warning signal, such as an audible alarm or a flashing light. Care should be taken to ensure the design and application of the warning device used minimizes the probability of an incorrect reaction by the personnel being warned. Care should also be taken to standardize the warning devices within like types of systems.

4.4.4 Develop rules, procedures and training programs – when it is not possible to eliminate or adequately control a hazard through the design process or use of safety and warning devices, Rules, Standard Operating Procedures, employee manuals, safety manuals, and training must be employed. This is the last resort as far as hazard reduction precedence. This must never be the sole hazard reduction method for Category 1 and 2 hazards.

NOTE: It must be understood that the farther down you go in the precedence list, the less safe the system. VTA employees, like all human beings, will occasionally err and violate training protocols or safety rules and procedures. The number one cause of the vast majority of accidents and incidents is the human element.

5.0 Definitions:

Accident: an event or occurrence that results in property damage, injury, or death.

Hazard: any real or potential situation or condition that could result in undesirable consequences if left unaddressed.

Incident: an event or occurrence that does not necessarily result in property damage, injury, or death.

Risk: the assessed likelihood, severity, and frequency of undesirable consequences resulting from a hazard.

Safety: the state in which the risk of injury to persons or damage to property is reduced to, and maintained, at or below an acceptable level through a continued process of hazard identification and risk management.

System: A composite of personnel, procedures, materials, tools, equipment, facilities, and software, at any level of complexity. The elements of this entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirement.

System Safety: the application of management and engineering principles, criteria, and techniques to the safety aspects of a system within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

VTA Manager: management staff including, but not necessarily limited to, the following positions - Chief, Director, Deputy Director, Manager, Superintendent, Assistant Superintendent and Supervisor.

6.0 Records:

6.1 All documents shall be retained according to the VTA Records Retention Schedule.

7.0 Appendices:

7.1 Hazard Analysis Types and Schedule.

7.2 Hazard Severity and Probability Category Charts.

7.3 Hazard Resolution Matrix.

8.0 Training Requirements:

None.

9.0 Summary of Changes:

Initial Release of this procedure.

10.0 Approval Information:

Prepared by	*Reviewed by*	*Approved by*
Garry Stanislaw Safety Projects Manager	Bill Lopez Chief Administrative Officer	Nuria I. Fernandez General Manager

APPENDIX 7.1 : HAZARD ANALYSIS SCHEDULE

HAZARD ANALYSIS	SYSTEM LIFECYCLE				
	Planning	Design	Construction	Operations	Disposition
Preliminary (PHA)					
System (SHA)					
Subsystem (SSHA)					
Operating (OHA)					
Software Safety (SSA)					
Failure Modes and Effects / Fault Tree (FMEA/FT)					
Security (SA) / Threat (TVA)					

ACTIVITY

FOLLOW-UP ACTIVITY

APPENDIX 7.2 : HAZARD SEVERITY AND PROBABILITY CATEGORIES CHARTS

Hazard Severity Categories

CATEGORY	SEVERITY	CHARACTERISTICS
1	Catastrophic	Death, severe property damage, or severe environmental damage
2	Critical	Severe injury, severe occupational illness, or major property or environmental damage
3	Marginal	Minor injury, minor occupational illness, or minor property or environmental damage
4	Negligible	Less than minor injury, occupational illness, or less than minor property or environmental damage

Hazard Probability Categories

DESCRIPTION	LEVEL	SPECIFIC INDIVIDUAL ITEM	FLEET OR INVENTORY
Frequent	A	Likely to occur frequently	Continuously experienced
Probable	B	Will occur several times in the life of an item	Will occur frequently
Occasional	C	Likely to occur sometime in the life of an item	Will occur several times
Remote	D	Unlikely, but possible to occur in life of an item	Unlikely, but can reasonably be expected to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to occur, but possible

APPENDIX 7.3 : HAZARD RESOLUTION MATRIX

Hazard Resolution Matrix

FREQUENCY	**SEVERITY**			
	Category **1**	Category **2**	Category **3**	Category **4**
A - Frequent	1A	2A	3A	4A
B - Probable	1B	2B	3B	4B
C - Occasional	1C	2C	3C	4C
D - Remote	1D	2D	3D	4D
E - Improbable	1E	2E	3E	4E

Unacceptable – high risk

Undesirable; management review and decision required – moderate risk

Acceptable with review by management – low risk

Acceptable without review – negligible or no risk