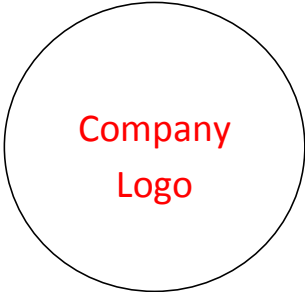




Your Bus & Truck Company - Security Plan

Security Sensitive Information



Security Plan

For

Your Bus & Truck Company

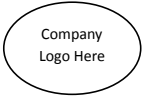
**Headquarters Location
222 Main Street
Anywhere City, Any State, 09090
(If Plan is Corporate-wide)**

OR

**ABC Bus & Truck Auxiliary Facility
1400 Freeway Blvd
Anothercity, Anotherstate, 44444
(If for local location only)**

[Date Created or Revised]

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

**Security Plan
Table of Contents**

- Section I: Background 3
 - Goals & Objectives 3
 - Purpose 4
 - Objectives..... 4
- Section II: Key Company Contacts 5
- Section III: Key Outside Contacts 6
- Section IV: Company Description..... 7
 - Organizational Structure 7
 - Area of Operations and Location of service contacts..... 7
- Section V: Security Action Item Operational Components..... 8
- Section VI: Security Plan Plan Adoption, Review & Revision Record 15
- Appendices 16
 - Appendix A - Vulnerability Assessment Summary/BASE Review 16
 - Appendix B - Continuity of Operations Plan (COOP) 16
 - Appendix C - Communications Plan 17
 - Appendix D - Background Check Guidance 20
 - Appendix E - Training Overview 23
 - Appendix E - Physical Security & Assess Control Guidance 27

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

I. Background

Our nation’s continuing war on terrorism has created a heightened threat environment for all transportation modes. The unexpected and vicious use of commercial airplanes under the control of terrorists raised a new realization of the ability of those who want to maim and kill Americans. This new threat has resulted in the need for organizations to develop security plans designed to protect their facilities, personnel, vehicles, and other assets. As time dims the memories of past events, there is an even greater need to stay focused and vigilant to protect our country’s assets, including its highways and infrastructure.

To establish the importance of security aspects of our organization, **Fill in your company Name** (herein also referred to as “the Company”) has developed this **Security Plan** that incorporates emergency preparedness components into a single source. This Plan outlines the process to be used by the Company to make informed decisions that are appropriate for our operations, passengers, employees and communities regarding the development and implementation of a comprehensive security program.

In order to be effective, the activities documented in this Plan focus on establishing responsibilities for security and emergency preparedness, identifying our methodology for documenting and analyzing potential security and emergency preparedness issues, and developing the management system through which we can track and monitor our progress in resolving these issues.

Purpose, Goals and Objectives of Security Plan

This Security Plan demonstrates our process for addressing *security and emergency preparedness*:

Security – The application of operational, technical, and management techniques and principles to recognize threats and reduce vulnerabilities to the most practical level through the most effective use of available resources.

Security Incidents – may include accidents, natural disasters, crimes, terrorism, sabotage, civil unrest, hazardous materials spills and other events that require emergency response. Security incidents require swift, decisive action from multiple organizations, often under stressful conditions. Security incidents must be stabilized prior to the resumption of regular service or activities.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

Purpose

The overall purpose of **Fill in your company Name's** Security Plan is to optimize -- within the constraints of time, cost, and operational effectiveness -- the level of protection afforded the Company's assets, including but not limited to, employees, facilities, vehicles, information, shipments (cargo or passengers), and other individuals who come into contact with the Company, during both normal operations and under emergency conditions.

Goals & Objectives

In this current environment, every threat cannot be identified and eliminated, but **Fill in your company Name** will take steps to be more aware of security concerns that may affect the Company. The Security Plan provides the Company with a security and emergency preparedness capability that will:

1. Meet any applicable Federal security requirements;
2. Ensure that security and emergency preparedness are addressed during all phases of the company's operation, including the hiring and training of personnel; the procurement and maintenance of equipment; the development of company policies, rules, and procedures; and coordination with local public safety and community emergency planning agencies;
3. Promote procedures and practices that will ensure secure operations are maintained through the on-going identification, evaluation and resolution of security threats and vulnerabilities, and;
4. Create a culture that supports employee security and safety, and secures company operations (during normal and emergency conditions) through compliance with company rules and procedures.
5. Achieve a level of security performance and emergency readiness that meets or exceeds the operating experience of similarly-sized companies around the nation,

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

II. Key Company Contacts

General Manager: Name - _____ Primary Phone: _____

Secondary Phone _____

Directors/Managers Name - _____ Primary Phone: _____

Secondary Phone _____

Name - _____ Primary Phone: _____

Secondary Phone _____

Security Coordinator: Name - _____ Primary Phone: _____

Secondary Phone _____

Alt. Sec. Coordinator: Name - _____ Primary Phone: _____

Secondary Phone _____

Other: (Title) Name - _____ Primary Phone: _____

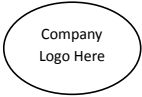
Secondary Phone _____

Other: (Title) Name - _____ Primary Phone: _____

Secondary Phone _____

Date Company Contacts Updated _____

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

III. Key Outside Contacts:

Local Emergency: 911

Local Police Department Contact: _____
(Department Name) (Direct Telephone)

Local State Police Office _____
(Direct Telephone) (Contact name if known)

FBI Local Office: _____
(Direct Telephone) (Contact name if known)

FMCSA: _____
(Direct Telephone) (Contact name if known)

Transportation Security Administration: **1-703-563-3237**
(Transportation Security Ops Center-TSOC)

TSA Local Office: _____
(Direct Telephone) (Contact name if known)

Other Federal Agency: _____
(Agency) (Direct Telephone)

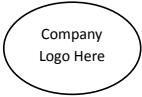
Other Federal Agency: _____
(Agency) (Direct Telephone)

Date Contacts Updated _____

For additional information about TSA/HMC or T-START, contact:

TSA Highway & Motor Carrier Branch
Transportation Security Administration
Office of Security Police and Industry Engagement – Surface Division
601 South 12th Street, Arlington, VA 22202-4220
Website: <http://www.tsa.gov/highway>
E-mail: highwaysecurity@dhs.gov

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

IV. Company Description

Organizational Structure

Fill in your company Name Here

Brief description of your company

Organizational Chart*

(*add in or attach as appropriate)

Area of Operations and Location of Services

Headquarters/Corporate Location Address:

Service is provided to (List states, counties, or cities served):

Additional Facility Locations:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

V. Security Action Items (SAI) - Operational Components

Management and Administration

1. Primary and Alternate Security Coordinators

_____ is designated as *Security Coordinator/Director* for **Fill in your company Name**. (Effective Date _____)

_____ is designated as the *Assistant Security Coordinator/Director* for **Fill in your company Name**. (Effective Date _____)

Duties & responsibilities of the Security Coordinator/Alternate Security Coordinator are:

- Prepare and regularly update the company Security Plan;
- Ensure that all components of the Security Plan are adequately administered;
- Ensure that a documented site specific “Vulnerability Assessment” has been conducted for all company facilities;
- Establish and regularly review all appropriate security guidelines necessary for the Company;
- Ensure that all security guidelines are being followed;
- Ensure that all employees are properly trained in company security policies;
- Ensure that an adequately trained Alternate Security Coordinator is identified to operate in the absence of the Security Coordinator;
- Assume other security responsibilities as deemed appropriate by Company management.

NOTE: Security Director should be a U.S. citizen, preferably with law enforcement, private security, or appropriate military background, or adequate previous on-the-job training.

2. Vulnerability Assessment

A Vulnerability Self-Assessment for **Fill in your company Name** facility located at _____ was conducted on _____ by _____ using the Vulnerability Self-Assessment Tool (VSAT) provided by TSA.

The VSAT Summary for **Your Company** is here attached under Appendix A.

OR if a BASE review has been conducted Insert

A “Baseline Assessment for Security Enhancements (BASE) Review” for **Fill in your company Name** facility located at _____ was conducted on _____ by TSA Inspector(s) _____. The Executive Summary relating to this BASE Review is here attached under Appendix A.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

3. Written Security Plan (Security Specific Protocols)

This document (with Appendices) constitutes the recognized Security Plan for **Fill in your company Name.**

4. Plan for Continuity of Operations

A Continuity of Operations (COOP) Plan is a written plan to address all aspects of **operational recovery** for this site in the event of emergency. A *Continuity of Operations Plan (COOP) Template*, adaptable for use by most companies, can be obtained from the Federal Emergency Management Administration website at: <http://www.fema.gov/planning-templates>. **A COOP Plan specific to this Company has been developed and is here attached under Appendix B.**

5. Communications Plan

A Communication Plan documents the processes used to facilitate the movement of information throughout the company during normal as well as adverse operating conditions. **A written Communications Plan for this site is here attached under Appendix C.**

6. Business and Security Critical Information (Operational Security)

Critical business and security information must be safeguarded from release or dissemination to unauthorized persons. It should be available only to company personnel having a legitimate “need to know.” Information to be safeguarded includes personnel information, security plans, proprietary product information, vulnerability assessments, facility plans, manifests, IT information, or other sensitive information. Employees will be required to execute a “Non-Disclosure Agreement” agreeing to safeguard this information.

7. Industry Best Practices or Security Options for Consideration

The Company recognizes and acknowledges TSA’s “Security Options for Consideration,” as set forth in Module IV of the *Transportation Security and Template for Assessment Review Toolkit (T-START)* or Other Source as Industry Best Practices.

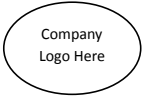
Personnel Security

8. Licensing and Background Checks for Drivers/Employees/Contractors

Written guidelines for addressing Licensing and Background Checks on prospective and current employees are included in the **Fill in your company Name** Employee Handbook.

Company procedures regarding licensing and background checks are here attached under Appendix D.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

9. Security Training Plan(s)

The Company shall ensure that adequate and appropriate Training Plan is developed to provide security training to all employees. The Training Plan shall:

- Provide a general outline of the curriculum to be taught for both new hires and to current employees (refresher or periodic retraining)
- Establish the scheduling timeframe that will be used,
- Document testing procedures for security training provided
- Establish the retention of training records.
- Within 30 days of commencing employment, all company employees will receive Security Awareness Training as offered by the FirstObserver™ Program. The Training shall be:

(Select the appropriate Program for company)

- **First Observer™ School Transportation Security Training DVD (STSA)** – This DVD was produced by TSA specifically for school transportation professionals with the assistance of three major school transportation associations. It is the premier anti-terrorism domain awareness training program created for the school transportation industry. Numerous security-related training modules were developed for highway professionals to accurately and non-confrontationally observe, assess and report potential terrorist or criminal behavior. The program does not replace dialing 9-1-1 in the event of an emergency and does not replace an organization's existing emergency communications plan or program. All surface modes will benefit by having additional surface transportation professional eyes and ears on the ground trained to report suspicious activity. First Observer training/ materials are free. The new training website URL will be formally announced when a firm date has been identified. **To request First Observer DVD information, e-mail request to FirstObserver@tsa.dhs.gov**
- **Operation Secure Transport (OST)** – Since 9/11, the Transportation Security Administration (TSA) has worked to identify and close vulnerability gaps in every section of the Nation’s transportation systems. This DVD training program was created specifically to **meet the training needs of the commercial “over-the-road-buses” (OTRB) operator** and was recently amended to meet the specific training requirements contained in the 2007 congressional mandate¹. **To request DVDs, e-mail request to highwaysecurity@dhs.gov**

- **First Observer™ Security Training for Trucking (Currently under revision)**

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

- Additionally, all company vehicles shall be equipped with a copy of the appropriate TSA **Highway Security Counterterrorism Guide**. TSA has created a uniquely specific Highway Security “Counterterrorism Guide” for each of our four (4) highway modes - Trucking, Motor Coach, School Transportation and Infrastructure. Each guide is a pocket-sized flip chart covering such topics as: Pre-Incident Indicators, Targets and Threats, Tactics, Prevention/Mitigation, Security Exercises, Chemical Biological Radiological Nuclear (CBRN), Licensing and Identification, and Points of Contact. It is TSAs goal to have a Counterterrorism Guide available to the driver of every commercial vehicle on our nation’s highways. **To request Counterterrorism Guides, E-mail your request to highwaysecurity@dhs.gov.**

An Overview of the Training Plan adopted by **Your Company** is here attached under Appendix E.

10. Security Exercises & Drills

The Security Director shall seek to establish point-of-contact information for the local police, fire and EMS offices responsible for responding to security or emergency situations that may arise at the Company facility located at _____. The Security Director shall also seek to identify federal, state or local authorities responsible for conducting emergency training exercises in the vicinity of the Company and shall seek to participate in such exercises to the extent possible. In the absence of outside authorities conducting such exercises, the Security Director shall conduct a security exercise or drill at least annually, engaging with the emergency response authorities to the extent possible.

Exercise/Drill Options Available

- **Intermodal Security Training and Exercise Program (I-STEP)** – Under the Intermodal Security Training and Exercise Program (I-STEP), TSA conducts security exercises (usually mock “Tabletop” exercises) involving all modes of transportation. TSA’s Highway & Motor Carrier Branch organizes and conducts I-STEP Exercises with our transportation industry partners engaged in trucking, school bus, over-the-road-bus (motorcoach), and infrastructure operations. Participants include industry operators, industry associations, TSA field staff, federal agencies, and state/local law enforcement or regulatory agencies. The exercises are free to participants and are held at various locations throughout the country. **To learn more about I-STEP Exercises visit our website www.tsa.gov/highway or request I-STEP information directly by emailing requests to highwaysecurity@dhs.gov**

OR (if Company has participated in past drill/exercise) Insert

An “After Action Report” prepared in response to the _____ Exercise in which the Company participated on _____ is attached under Appendix F.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.




Your Bus & Truck Company - Security Plan

Security Sensitive Information

Facility Security

In lieu of the below options for consideration regarding Facility Security, the here attached PDF File "TSA Site Security Survey Form" may be substituted and inserted under **Appendix F**.



11. Facility Access Control

The Company shall have adequate access control, capable of preventing unauthorized entry at all times. Access control may include:

- Locked and secured exterior doors;
- Locked and secured windows/skylights;
- Locked and secured areas deemed "off-limits by other than specially authorized employees;
- Company issued photo ID badges that must be displayed
- A "Challenge Procedure" for employees to safely confront or report unauthorized persons;
- Advanced physical control locks where appropriate;
- Adequate Visitor Control protocols; and
- Other access control measures deemed appropriate.

Company procedures addressing Facility Access Control are here attached under Appendix F.

12. Physical Security

The Company shall have adequate exterior and perimeter access control, capable of preventing unauthorized entry at all times. Perimeter access control may include:

- Appropriately sized and fully functional fences, gates, and barriers as needed;
- An adequate intrusion detection system (burglar alarm);
- Closed Circuit TV cameras as deemed necessary;
- Adequate exterior lighting;
- Documented key control procedures for all company facilities
- The use of security personnel/guards

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

Company procedures addressing Physical Security are here attached under Appendix F.

13. Cyber Security- Information Technology

The Company shall ensure adequate security of all electronic data and/or information produced by or for the company. Safeguarding such information shall include:

- Limiting access to electronic information/computer files to employees having a legitimate “need-to-know
- Adequate computer “firewalls”
- Written IT security policies (included in IT manual for the Company)
- Requirements for periodically changing computer passwords
- Periodic testing of computer security capabilities
- Off-site backup of all computer generated or housed company data
- Regular computer security training for employees
- Employee awareness training dealing with cyber-attack indicators and vulnerabilities via social media
- Other actions deemed appropriate by management.

If extensive company-specific security measures concerning this SAI have been developed, insert an additional Appendix if needed.

Vehicle Security

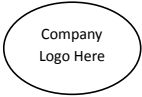
14. Vehicle (En-route) Security

The Company shall ensure that adequate vehicle security measures are in place, which shall include:

- Vehicles are equipped with appropriate door/window locks and their use is required (if not prohibited by State law).
- Vehicles, when parked and unattended, deploy company provided wheel locks/ alarms/ kill switches;
- The use of a unique key for each vehicle and an adequate key control program for all vehicles;
- The use of enhanced technology for entering and/or starting company vehicles;
- The use of on-board (interior or exterior view) cameras and/or GPS technology for vehicles;
- Overnight off-site parking restrictions

If extensive company-specific security measures concerning this SAI have been developed, insert an additional Appendix if needed.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

15. Cargo/Passenger Security Program

The Company shall ensure that adequate vehicle security measures are in place, which shall include:

- The use of adequate locks on vehicle cargo/storage doors, hatches, or valves;
- The use of adequate cargo seals, if appropriate;
- Where appropriate, equipping buses (if appropriate) with a safety/security barrier between the driver and passengers;
- Where appropriate, the use of some type of supplemental trailer security measures (i.e.; kingpin locks, glad-hand locks, high-grade door locks, any type of cargo alarm system, etc.);
- Where appropriate, utilizing some type of cargo, baggage or passenger screening system.

If extensive company-specific security measures concerning this SAI have been developed, insert an additional Appendix if needed.

16. High Alert Level Contingencies

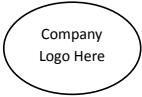
In the event an elevated security alert is declared by DHS, the Company shall implement additional security measures, to include:

- Enhanced communications and control over the location of company vehicles;
- Enhanced measures to ensure drivers are secure;
- Contingencies for safely recalling vehicles, if necessary;
- Initiating supplemental facility control measures;
- Constant monitoring of national news media;
- Other measures deemed appropriate

The following "Information Sharing Resource" should be monitored regularly by the Security Director/Assistant Security Director for additional guidance:

- **The Homeland Security Information Network (HSIN)** is a national secure and trusted web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission. HSIN is made up of a growing network of communities, called Communities of Interest (COI). **"Highway" is the general Community of Interest for most users reading this information.** COI's are organized by state organizations, federal organizations, or mission areas such as emergency management, law enforcement, critical sectors, and intelligence. Users can securely share within their communities or reach out to other communities as needed. HSIN provides secure, real-time collaboration tools, including a virtual meeting space, instant messaging and document sharing. HSIN allows partners to work together instantly, regardless of their location, to communicate, collaborate, and coordinate.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

Other Company employees may also seek HSIN membership. To become a member, please contact the HSIN program at HSIN.Outreach@HQ.DHS.gov. The “Highway COI” is accessible through the TSA email address highwaysecurity@dhs.gov.

You may obtain an application by sending a request to HSIN.Outreach@hq.dhs.gov. Once nominated, the COI Validating Authority will review your membership application and approve or deny your admission to the COI. If the application is approved, an email will be sent to you with instructions on how to log onto HSIN for the first time.

17. Security Inspections

In addition to any pre-trip safety inspection conducted, the Company shall require:

- A pre-trip vehicle security inspection, as detailed in the TSA Counterterrorism Guide for Trucking/Motorcoach/School Bus;
- A post-trip vehicle security inspection, as detailed in the TSA Counterterrorism Guide for Trucking/Motorcoach/School Bus
- An additional vehicle security inspection any other time a vehicle is left unattended;
- If appropriate, passenger reconciliation process (ticket verification, headcount) for every trip;
- Verification, to the extent possible, that the material being shipped match the trip manifest.

For guidance, refer to TSA’s “Counterterrorism Guide” for Trucking/Motorcoach/School Bus

18. Reporting Suspicious Activities

The Company shall ensure that all employees are provided with adequate “Domain Awareness” training, are familiar with reporting procedures, and are required to:

- Report security related “suspicious activities” to management and/or law enforcement.
- Notify the appropriate personnel upon observing suspicious activity;
- File a written report for suspicious activities observed.

For Guidelines on reporting suspicious activities, visit www.firstobserver.com/training

19. Chain of Custody/Scheduled Service

The Company should establish procedures designed to ensure and verify the safety of drivers and confirm that goods/services/passengers being delivered reach their destination as scheduled by:

- Requiring confirmation upon arrival at final destination on passenger trips;
- Requiring confirmation of shipment at final destination for trucking activities;
- Prohibiting the use of alternate drivers without specific authorization

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

If extensive company-specific security measures concerning this SAI have been developed, insert an additional Appendix if needed.

20. Preplanning Emergency Routes

The Company shall ensure that procedures are in place to:

- Prohibit drivers from diverting from authorized routes, making unauthorized pickups or stopping at unauthorized locations without justification.
- Identify and pre-plan alternate routes in the event primary routes cannot be used under certain security related emergencies.

If extensive company-specific security measures concerning this SAI have been developed, insert an additional Appendix if needed.

VI. Managing Threats

In this section we will address specific threats including active shooter, bomb threats, and xxx. The information contained in this section is intended to provide a starting point for entities to use in planning company and/or organizational efforts to counter threats requiring immediate response. It is recommended that companies and/or organizations contact their local law enforcement and response agencies to further develop their planning efforts and ensure that these actions do not impede local response to such threats. These actions are voluntary and are not required by the federal government, but rather are intended to initiate a proactive step in preparedness and protection of critical assets.

Formatted: Font: 16 pt, Bold

Formatted: Font: 12 pt

Response to Emergency Situations

•

1. Active Shooter
2. Bomb Threats
3. XXX

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: Bold

VI. Security Plan Adoption, Review & Revision Record

Date	Action Taken	Name/Signature	Position/Title
	Security Plan adopted		

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

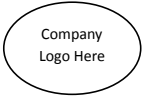
	Security Plan reviewed ___ Security Plan revised ___		
	Security Plan reviewed ___ Security Plan revised ___		
	Security Plan reviewed ___ Security Plan revised ___		
	Security Plan reviewed ___ Security Plan revised ___		
	Security Plan reviewed ___ Security Plan revised ___		

- This page tracks the adoption of, and changes to, the recognized Fill in your company Name Security Plan.
- The Security Plan should be reviewed no less than annually, with the “Security Plan reviewed” tab checked off. If revisions are made, “Security Plan revised” should also be checked off.
- The name and signature of person making the revision or reviewing the Plan should be entered, along with the date of the action taken.
- Only the General Manager or persons authorized by the General Manager may alter or revise the Security plan. Revisions to the Security Plan must be reviewed and approved by the General Manager. **(Modify terms/titles to meet company needs)**

Appendices

Appendix A – Vulnerability Assessment

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

INSERT THE COMPLETED "VULNERABILITY SELF-ASSESSMENT TOOL" SUMMARY HERE (if your company has not participated in a BASE Review)

OR Insert

INSERT HIGHWAY BASE ASSESSMENT "EXECUTIVE SUMMARY" HERE (if your company has had a BASE Review conducted by TSA)

Appendix B – Continuity of Operations Plan (COOP)

Visit <http://www.fema.gov/planning-templates> for guidance in developing a COOP, adapt to meet your needs, and **insert completed COOP plan here.**

Appendix C – Communications Plan (Modify to meet company needs)

Communications Plan: This Communications Plan documents the processes used to facilitate the movement of information throughout the company during normal as well as adverse operating conditions. Generally, normal communications follow a natural flow between company leadership, management and employee as needed, both upward and downward. Additionally, communications laterally between peers is important, as are external communications with non-company entities. It is the purpose of this plan to foster effective communication across all of these nodes.

Normal day-to-day communications are accomplished by methods that have become tried and true and problems are generally minimal. Computers, radios, telephones and cell phones provide the necessary methods for transferring all the information that is needed to effectively conduct company business each day. But should these normal methods of communication become disrupted, employees should know what procedures are to be followed.

Disruption to communications as the result of a security incident (terrorist attack, hi-jacking, cyber-attack, active shooter, other crime, etc.) should be recognized as a possibility and addressed accordingly. It is not possible to plan for every type of potential problem, so it is important to have general guidelines in place to follow that should aid in mitigating most situations. Those steps include:

Know How to Reach External Resources in the Event of an Emergency

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

- 911 is your first resource
- Have Direct Telephone Numbers for Emergency Responders/Security Resources (current and verified annually)
 - Local Police
 - State Police
 - FBI
 - Fire Department
 - Hospital
 - Gas /Electric/Water/Telephone/Internet/Alarm companies
 - Information Sharing & Analysis Center (ISAC)
 - Fusion Center
 - Joint Terrorism Task Force (JTTF)
 - Transportation Security Administration (TSA)
 - Local Federal Security Director (FSD)
 - Local Transportation Security Inspector (TSI)

Know How to Reach Internal Resources in the Event of an Emergency

- Management
- Security Personnel
- Facility/Maintenance employees
- Drivers
- Contractors
- Union Officials

Know your Options and Methods for Contacting Emergency Resources

- Cell Phone
- E-mails
- Instant Messages
- Phone Tree (Primary & Alternate contact numbers - Test quarterly)
- Share point
- Radio (Test daily)
- Public Announcement System (outside & inside)
- Electronic messages
- Bulletins/Meetings/Posters/Training
- Runners
- Duress buttons (Test quarterly)

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

- Panic Switches (Test quarterly)

Plan for Complete Loss of Communications: During the 9/11 attacks in the U.S., telephone as well as cell phone communications were completely lost for a brief period. The possibility of communications again being lost as the result of a significant security incident remains a concern in the U.S. The Company has options available to them regarding vehicles in transit and products that are being moved in the event communications are lost. Dispatcher/Driver options available include returning to the facility, continuing to destination, seeking shelter at a pre-identified secure location, stopping at a commercial truck stop/weigh station or employing other unique options available. The important point is to recognize that this possibility exists and to have a discussion regarding options available prior to an emergency occurring. In the event communications are completely lost, drivers should (insert your company's options/procedures here):

1. _____.
2. _____.
3. _____.

Appendix D – Licensing and Background Checks for Drivers/ Employees/ Contractors (Modify to meet Company needs)

CONDUCTING AN EMPLOYMENT BACKGROUND CHECK

Background checks serve as a means of objectively evaluating a job candidate's qualifications, character, and to identify potential hiring risks for security reasons. They are often requested by employers on job applicants for employment especially on candidates seeking a position that requires high security or a position of trust, including schools, hospitals, financial institutions, airports, and government. Results of a background check typically include past employment verification, credit history, criminal history, citizenship, and driving history.

Who Conducts Background Checks?

There are many avenues to conduct background checks. They fall into several categories and can consist of a detailed and thorough investigation or a simple Internet search. The best method to use varies on the intent behind the background check. It is strongly recommended to base the type of background investigation to the position duties within the transportation industry.

Types of Background Checks:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

- **Internet:** You as the owner or employee may search social media sites (My Space/Facebook) query free data bases, or sites that charge a fee to query a person’s background and criminal history.
- **Private Investigators:** Utilizing a private investigator to conduct a background check may be an option if you don’t have the time or resources to conduct in-depth background checks on potential applicants.
- **Background Screening Companies:** Many of those companies are accredited through associations such as National Association of Professional Background Screeners (NAPBS) offering reliable, complete, and legal compliance with all applicable federal/state/local laws.

Applicable Laws and Regulations:

Due to the sensitivity of the information contained in reports and certain records, there are important laws regulating the dissemination and legal use of that information. The [Fair Credit Reporting Act](#) (FCRA) regulates the use of consumer reports (Information collected and reported by third party agencies) as it pertains to adverse decisions, notification to the applicant, and destruction and safekeeping of records. Individuals are entitled to know the source of any information used against them including a credit reporting company and must provide consent in order for the employer to obtain a credit report. The employer must take into consideration the nature of the offense, when it occurred, and how it relates to the job you’re seeking. http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm#VIII

The Federal Government requires the following background checks:

• **Transportation Worker Identification Credential (TWIC):**

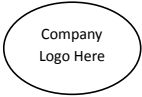
The Transportation Security Administration (TSA) developed the Transportation Worker Identification Credential (TWIC™) Program in response to the Maritime Transportation Security Act of 2002 (MTSA). MTSA requires use of a biometric identification credential by individuals who require unescorted access to secure areas of maritime facilities and vessels. Before issuing a TWIC, TSA must conduct a security threat assessment on the TWIC™ applicant. An applicant who, as a result of the assessment, is determined to not pose a security threat, will be issued a TWIC.

Each applicant for a TWIC™ must provide biographic information, identity documents, biometric information (fingerprints), sit for a digital photograph, and pay the established TWIC™ fee. TSA will send pertinent parts of the enrollment record to the FBI, as well as within the Department of Homeland Security (DHS), so that appropriate terrorist threat, criminal history, and immigration checks can be performed. <https://twicprogram.tsa.dhs.gov/TWICWebApp/>

• **Hazardous Material Endorsement:**

The TSA Hazardous Materials Endorsement Threat Assessment Program conducts a security threat assessment for any driver seeking to obtain, renew, or transfer a hazardous materials endorsement

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

(HME) on a state-issued commercial driver’s license (CDL). The program was implemented to meet the requirements of the USA PATRIOT Act, which prohibits states from issuing a license to transport hazardous materials in commerce unless a determination has been made that the driver does not pose a security risk. The Act further requires that the risk assessment include checks of criminal history records, legal status, and relevant international databases.

<https://hazprints.tsa.dhs.gov/Public/>

Verifying an applicant’s “Right to Work” status

U.S. law requires companies to employ only individuals who may legally work in the United States – either U.S. citizens, or foreign citizens who have the necessary authorization. The Department of Homeland Security (United States Citizenship and Immigration Service) provides a program titled E-Verify. E-Verify is an Internet-based system that allows businesses to determine the eligibility of their employees to work in the United States. E-Verify is fast, free and easy to use – and it’s the best way employers can ensure a legal workforce.

<http://www.uscis.gov/portal/site/uscis/menuitem. eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=75bce2e261405110VgnVCM1000004718190aRCRD&vgnnextchannel=75bce2e261405110VgnVCM1000004718190aRCRD>

Obtaining an applicant’s criminal history

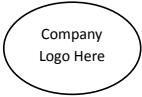
With the exception of TWIC/CDL-HME applicants, and individual requests to the FBI seeking their personal criminal history, there is no one stop shopping to obtain an applicant’s criminal history for all 50 states.

The FBI provides arrest records or criminal background checks at the request of private citizens but ONLY YOU can request a copy of your own “Criminal History Summary” from the FBI—often referred to as an Identification record or a rap sheet. This may be accomplished by submitting a written request to the FBI’s Criminal Justice Information Services Division. The FBI will check various systems for any arrest records, a process that is generally known as a criminal background check. The FBI will also forward, if requested, a copy of the rap sheet to an individual or party identified on the applicant’s signed request form OMB-1110-0052.

The FBI offers two methods for requesting your FBI Criminal History Summary or proof that a record does not exist.

- **Option 1:** Submit the application, letter of request, fee, and fingerprints to the FBI; <http://www.fbi.gov/about-us/cjis/background-checks>
- **Option 2:** Submit to an FBI-approved “channeler,” which is a private business that has contracted with the FBI to receive the fingerprint submission and relevant data, collect the associated fee(s), electronically forward the fingerprint submission with the necessary information to the FBI CJIS Division for a national criminal history record check, and receive the electronic record check result for dissemination to the individual. Contact each channeler for processing times. <http://www.fbi.gov/about-us/cjis/background-checks/fbi-approved-channelers>

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

Note: An FBI-approved channeler may be unable to authenticate (apostille) fingerprint search results. If an authentication (apostille) is needed, please contact the channeler to determine if this service is provided.

General Do's and Don'ts

- Obtain applicant’s written notarized authorization/consent to perform a background check.
- Know what you're getting from a background check. The quality and depth of background investigations vary widely in within the industry.
- Be wary of Web sites offering instant checks. They may not be familiar with compliance and federal law. Some background companies search for criminal history in only one or two counties where an applicant has lived primarily, possibly missing information elsewhere.
- Diligent searches require screening firms to send workers, if necessary, to pull court files by hand for accuracy.
- Know how reference checks are done. Some screening firms grant anonymity to friends and former bosses and co-workers in exchange for unvarnished opinions about applicants. Others identify all sources to guard against unsubstantiated gossip and innuendo.
- Ask how a screening firm checks references and whether you can provide specific questions to be asked that pertain to the position being filled.

Appendix E – An Overview of Training for Your Company
(Modify to meet Company needs)

Training – An Overview

No matter how much effort goes into developing a strong security program, it is only as effective as the employees who carry it out. For employees to clearly understand what is expected of them, they need to receive security awareness training. A strong training program which closely follows the security plan will render the best results. You should teach security to clarify the procedures outlined by your Security Plan. The training should clearly explain the security program’s policies and procedures. Explaining the threats your company and its employees may face, to the level they are known, is critical for them to understand the importance of security. At the conclusion of the training each and every employee should clearly understand what is expected of them and why.

A security awareness training plan should document the training course employees will receive. The training courses should be designed to address groups of employees:

- **New employees**
 - General security policies

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

- Suspicious activity training
- General cyber awareness training
- Disciplinary actions of security policy violations
- **In-service training of current employees**
 - Review of general security policies
 - Review of suspicious activity training
 - Review of cyber security awareness training
 - Include current threat trends and exposures to employees and the company/agency
- **Specific groups of employees**
 - Security personnel
 - Patrol procedures
 - Challenge procedures
 - Gate ingress/egress procedures of employees, visitors, vendors, drivers
 - Physical security
 - Reporting and documenting security violations and suspicious activities
 - **IT personnel**
 - Detailed cyber threats
 - Current trends of cyber attacks
 - The vulnerabilities of social media
 - Security awareness
 - Software and hardware protection
 - Reporting and documenting suspicious activity or cyber-attacks or violations
 - **Dispatchers/Ticket agents**
 - General driver security policies

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

- Suspicious activities or violations of drivers, vendors, customers, co-employees (Insider) or persons on or near premises of company/agency
- Communication with drivers during normal and emergency operations
- Reporting and documenting suspicious activities
- Cyber security detailed around their job duties

○ **Managers**

- General review of security policies of specialized groups
- Insider threat awareness
- Work place violence
- Current threats to industry
- Reporting and documenting suspicious activities

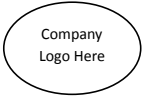
○ **Warehouse Personnel**

- Physical security of warehouse/yard
- Delivery/shipping procedures
- Visitors within warehouse
- Non-warehouse employee policies within warehouse
- Suspicious activities reporting and documentation
- Suspicious package identification, reporting, documentation and procedures to follow

○ **Drivers**

- Vehicle security policies
- Route procedures
- Receiving and delivering cargo/passengers policies and procedures
- In-route policies and procedures during normal and emergency operations
- Communication with dispatcher/company during normal and emergency operations

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

- Unauthorized passengers or route

As the security policy is created, consider how the training will cover the security program being established. Once the security policy is established, consider a “Table Top” exercise to determine if the training programs are effectively supporting the security policies. Remember, the security policies and training must continually evolve to address current threats.

General security training program for all employees should cover:

- Policies and procedures for all employees to maintain proper passenger/cargo security
 - Training should clarify duties and responsibilities of each employee’s duties (i.e. driver, dispatcher, ticket agent/forklift driver, warehouse, gate security, etc.)
- Proper procedures to Identify, safely challenge or report to security, an unauthorized person(s) in restricted areas.
 - Include proper reporting and documentation of suspicious activities and security violations
- Policies and procedures required of employees to maintain strong physical security of buildings, office spaces and support structures
 - Controlled access/exit points of employees to prevent unauthorized access from non-employees
 - Wearing , proper display of ID cards
 - Visitor sign-in/sign-out and ID badges
 - Locking doors, decks, cabinets, etc.
- Policies and procedures required of employees to maintain computer and cyber security
 - Include a strong password and password protection training
 - Protection of computer (Ease dropping, Locking computer when away, etc.)
 - Include protection of personal information
 - Consider Introducing “Nondisclosure” for review and signature
- Policies and procedures required of employees to maintain proper vehicle security
 - Company/agency staff, employee assigned and support vehicles
 - Company/agency “For Hire” vehicles

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

- o Training should center on duties of each employee (vehicle fleet managers, drivers, mechanics, etc.)
 - Physical security of vehicles
 - Pre and post vehicle security and safety inspections
 - Unattended vehicle security
 - Passenger/cargo security
 - In-route policies and procedures during normal and emergency operations
 - Communication with dispatchers/drivers during normal and emergency operations
 - Unauthorized passengers or
 - Unauthorized or out of route
- General security training program for all employees to cover company security policies

Administration/Staff security training program to cover awareness, cyber threats, insider threats, physical security

Security guard training program to cover guard’s duty, patrol practices, gate duties, current criminal threats, awareness

Appendix F – Facility Access Control & Physical Security

(Modify to meet Company needs or use “TSA Site Security Survey Form” PDF here attached)



TSA Site Security Survey Form...

When considering access control and physical security countermeasures, you should determine the needs of your company at that particular location. For example, you may require certain physical security needs in some urban settings and completely different needs in a rural setting. Consult your Vulnerability Self-Assessment or BASE Executive Summary to address your specific needs.

Fencing: Fences are generally the first layer of physical security. There are many types of fencing available. The type and needs of the facility may dictate the type of fencing required. Types include:

- Chain link

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

- Wrought Iron
- Wooden
- Wire

Considerations:

- Perimeter fencing
- Interior fencing around sensitive areas/equipment (generators, fuel tanks, etc.)
- Height
- Gauge
- Reinforcement – Are you attempting to deter persons or stop vehicles?
- Visibility – Do you want people to see into your facility’s grounds?
- Electrified fencing/Fence alarms
- Topping Wire – Barbed, razor, concertina wire, etc.
- Configuration – How many strands/coils? Facing inward, outward, both, combinations, etc.
- Changes in fence gauge at top
- Attachment to buildings
- Proximity to other objects which can enable easier climbing

Gates: Gates determine the point of entrance and exit to the facility grounds. Types include:

- Manual / Automatic
- Keypad / Swipe card / Proximity card / Remote entry
- Open / Locked
- Roller or swing gates

Considerations:

- Date/time Stamp Capabilities
- Access Control issues (see below)
- Gate widths and proximity to road – Will large vehicles be able to easily turn into the facility?
- Weather – Will snow buildup effect the operation of the gate?

Barriers: Barriers can be used to protect buildings, equipment, or other sensitive items.

Barriers can also be used to direct traffic flow (vehicle and pedestrian). Types include:

- Jersey barriers (K-rails)
- Guard rails
- Bollards
- Walls – brick, cinder block, etc.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

- Fencing
- Steel plate / Wedge surface mounted barriers
- Crash beams
- Natural barriers:
- Rocks / Boulders
- Hills
- Water
- Ravines
- Mountain
- Cliffs
- Vegetation (Thorny or thick bushes)

Choke points: Vehicles and pedestrians can be funneled by barriers into choke points providing control and direction. Choke points include:

- Entrances
- Exits
- Doorways
- Inspection points

Window bars: Bars, general wrought iron, installed on glass windows and doors to prevent entry through glass. *Warning: Installation of bars can also prevent exit from doors and windows during an emergency such as fire.*

Lighting: There are many types of lights available for a wide array of situations and coverage. Types include:

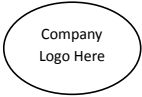
- High Intensity Discharge (HID)
- Halogen
- Light-emitting Diode (LED)
- Incandescent
- Infrared

Positions:

- To provide adequate illumination to all areas with no darkened areas
- Overlapping coverage
- Perimeter facing inward
- Lighting arrays in different areas in the yard

Considerations:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

- Make certain the lights used are compatible with the types of camera systems you may be using.
- Are lights able to be powered by the auxiliary power units in the event of a power outage?

Cameras: There are a wide variety of camera capabilities for a wide variety of circumstances. Types include:

- Fixed
- Pan Tilt Zoom (PTZ)
- Covert (hidden)
- Color
- Black & White
- Infrared

NOTE: Lighting - Ensure there is adequate lighting as required by the type(s) of cameras utilized

Position:

- Overlapping coverage
- Eliminate blind spots
- Wireless / microwave transmitters / receivers
- Interior / exterior

Technology:

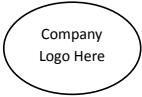
- Camera alarms
- Monitors to view multiple camera views simultaneously
- Remote viewing from alternate locations
- Recording and archiving capabilities
- 24/7 for 30-90 days

Considerations: Are cameras and monitors able to be powered by the auxiliary power units in the event of a power outage?

Alarm systems: Alarm systems are designed to alert personnel to the occurrence of an undesirable event. Types include:

- Entry alarms
- Intrusion alarms
- Passive infrared motion detectors
- Ultrasonic detectors
- Microwave detectors
- Photo-electric beams

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

- Fire alarms
- Fence alarms

Considerations:

- Are alarm systems necessary if employees are present 24/7?
- Should only sensitive areas be alarmed then?
- What type of response should happen for an alarm?

Guard services: Security guards can provide protection of your facility and allow your employees to concentrate on their jobs. Considerations include:

- 24/7 coverage
- After-hours coverage
- Armed or unarmed
- Private security company
- Company employees
- Off-duty law enforcement officers
- Guard shack
- Guard dogs
- Duties -

Patrol facility

Monitoring surveillance cameras

Manning access control points

Conduct entrance/exit inspections

Reports and assessments

Signage: Proper sign placement provides direction and information. Examples include:

- No trespassing
- Area under surveillance
- No parking
- All visitors report to office

Locks: There are a wide variety of locks for different purposes. Types include:

- Padlocks
- Combination locks
- Door locks
- Electronic locks
- Biometric locks

Considerations:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

- Date/time Stamp Capabilities
- Access Control issues (see below)
- Lock vs. door – Putting an expensive heavy duty lock on a weak door.

Auxiliary Power: An alternative source of energy used to power devices during electrical failures. Options include:

Generators

- Standby – Automatically starts upon power outage
- Portable – Manual set up after power outage
- Emergency Power Units for sensitive electronic equipment (Allows enough power to safely power down computers, etc.)
- Consider amount of power required to continue operations (full or limited)

Critical areas: Identify areas of your facility which are critical to operations. These area may warrant additional security measures. Examples include:

- Fuel tanks
- Generators
- IT Department
- Dispatch office
- Facility grounds
- Financial offices
- Management offices
- Product storage/transfer
- Personnel offices and records
- Areas of proprietary operations

Additional access control to be applied to these areas may range from the simple to the high tech, from cheap to ultra-expensive, and may include:

- Keypads
- Combinations of locking options
- Cypher locks
- PIN Codes
- Swipe cards
- Smart cards
- Remote entry (from alternate location or via remote control)
- Intercom systems
- Proximity cards
- RFID chips

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Your Bus & Truck Company - Security Plan

Security Sensitive Information

Biometric Entry

- Fingerprints
- Eye scan
- Voice

Computers Enhancements

- Login ID and passwords
- Firewalls (Internal and External)
- Date/time entry log/stamps
- Access limited to job description/duties
- Computer social media intrusion training

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.