GEMINI TECH SERVICES, LLC
5019 E I-20, Frontage Rd
Willow Park, TX 76087

GTS SECURITY VIOLATIONS POLICY

I. Cleared Facility Eligibility Requirements.

Gemini Tech Services is an organization that has been granted a Facility Clearance (FCL). The company had to meet the following eligibility requirements before the company could reach FCL status:

A. The company must need access to the classified information in connection with a legitimate U.S. Government or foreign government requirement.

B. The company must be organized and existing under the laws of any of the fifty states, the District of Columbia, or Puerto Rico, and be located in the United States or its territorial areas.

C. The company must have a reputation for integrity and lawful conduct in its business dealings. The company and its key managers must not be barred from participating in U.S. Government contracts.

D. The company must not be under Foreign Ownership, Control, or Influence (FOCI) to such a degree that the granting of the FCL would be inconsistent with the national interest.

II. Cleared Employee Eligibility Requirements

GTS employees or candidates (seeking employment with GTS) may be processed for a Personnel Clearance (PCL) when the company determines that access is essential in the performance of tasks or services related to the fulfillment of a classified contract. A PCL is valid for access to classified information at the same or lower level of classification as the level of the clearance granted to the company. The Cognizant Security Agency (CSA) determines eligibility for access to classified information in accordance with the national standards and notifies the contractor that eligibility has been granted. The CSA will also notify the contractor when an employee's PCL has been denied, suspended, or revoked. In these situations the contractor shall immediately deny access to classified information to any employee when notified of a denial, revocation, or suspension.

III. Classified Information Safeguarding Requirements

To maintain Facility Clearance status and Personnel Clearance eligibility, Contractors are responsible for safeguarding classified information in their custody or under their control. Individuals (cleared employees) are responsible for safeguarding classified information entrusted to them. The extent of protection afforded classified information shall be sufficient to reasonably foreclose the possibility of its loss or compromise. Failure to safeguard classified information is a security violation.

IV. What is a Security Violation?

A security violation is the failure to comply with the policy and procedures established by the National Industrial Security Program Operating Manual (NISPOM) and that reasonably could result in the loss or compromise of classified information. Failing to comply with the NISPOM or any security procedures outlined by the company, the project/contract or worksite security managers may result in disciplinary action, up to and including termination. Any person who has knowledge of a potential security violation must immediately report it to the GTS Facility Security Officer team.

V. Investigations

Members of the GTS FSO team are responsible for conducting initial administrative inquiries and other preliminary investigations when a violation is suspected. The FSO team will conduct an appropriate investigation to identify what has occurred, how it occurred, and who is responsible or involved and will make a determination of whether a violation occurred. If the preliminary inquiry confirms a violation, the GTS FSO team will prepare an initial report for the Defense Security Service (DSS) and continue the investigation. A final report will be submitted to DSS in accordance with the NISPOM.

VI. Responsibilities

All potential or actual infractions or violations of classified information/material must be reported immediately to the Facility Security Officer or Assistant Facility Security Officers to ensure the integrity of the information/material and the Company. Failure to report or the misrepresentation of an infraction or violation is in itself a violation and may result in a disciplinary action. It is the duty of all employees to act responsibly and to correct irresponsible or unauthorized behavior in order to prevent the compromise of classified information/material. This also ensures the safety and security of other personnel, property, and the Company.

VII. Actions Guide

The administrative or disciplinary action to be taken for a specific security infraction or violation will be decided upon by the Owners, FSO team and Project Leaders meeting together to discuss the infraction or violation. An actions guide will be used when determining the action to be taken. The guide does not dictate the action to be taken; rather, it establishes a range of options that can be taken to ensure the safety and security of personnel and property. The action taken

will be based upon the severity of each or subsequent infraction(s) or violation(s) and may include none, any, or all of the actions listed. However, multiple infractions and/or violations within the one-year period does raise doubts about an individual's trustworthiness and ability to safeguard classified information/material. The administrative or disciplinary actions that may be taken are:

A. Retraining

B. Verbal warning

C. Verbal reprimand

D. Written reprimand

E. Suspension of security clearance

F. Termination of security clearance

G. Criminal actions

VIII. Other Influences and Procedures

Security infractions or violations may also be addressed using aspects of the Gemini Tech Services Employee Handbook. All security incidents and/or violations will become part of the individual's security record that is maintained by the FSO team.