SCIS CALIFORNIA

Security Officer & Field Services

HANDBOOK

Securitas

THIS PAGE IS
INTENTIONALLY
LEFT BLANK

Paragon Systems, Inc. and Securitas Critical Infrastructure Services is referred to in this book as SCIS

The content of this book is applicable to all security officers and field security personnel within the AeroDefense and Energy Sectors working in California. Some sections pertaining to wage/hour issues may not be applicable to exempt employees.

SEE SOMETHING; SAY SOMETHING

If You See Anything Unusual, Report It

Security officers sometimes prevent crimes and violent, negative events through vigilance and good reporting. The best way to deal with terrorism, workplace violence and criminal acts is to prevent them from happening.

DO NOT ignore signs or "RED FLAGS" that could indicate possible danger. Use your common sense: report unusual, out of the ordinary and suspicious things and activities.

Depending on your job site, **you should know who to contact and alert** when something comes up. It may be your manager, someone from the local office, management at the site, the SCIS hotline **(1-800-574-8637 or www.scishotline.com)**, or for **emergencies 911**.

Here are a few examples of things to report:

- Someone talking excessively about guns, violence or extremist/controversial political topics
- Someone's behavior or comments are aggressive, threatening or intimidating.
- Unusual items or situations: A vehicle parked in an odd location, a package/luggage left unattended, a window/door open that should be closed, a room light on that should be off, a broken door lock, or any out-of-the-ordinary conditions at the job site.
- Eliciting information: A person who does not have a legitimate purpose asks questions about a building's operations, security procedures, personnel or shift changes, etc.
- Observation/surveillance: A person who does not have a legitimate purpose pays unusual or excessive attention to facilities or buildings. This includes excessive loitering or unusual, repeated or prolonged observation of a building (e.g., with binoculars or video camera), taking notes or measurements, counting paces, sketching floor plans, etc.

Some of these activities could be innocent—it's important to consider the context of the situation. It's up to management or law enforcement to determine whether the behavior warrants investigation.

This policy is not intended to violate anyone's civil rights or liberties. Do not report a person because of their race, ethnicity or religious affiliation.

You are instructed to follow the active shooter protocols in place at your security assignment. If your security assignment does not have site specific protocols, then adhere to the following active shooter instructions.

How to Respond if an Active Shooter Comes to Your Job Site

Follow your training. You must follow the active shooter training you received as well as any specific protocols in place at your security assignment. If your assignment did not include training and does not have site specific protocols, then follow the active shooter instructions below.

These are general instructions. The response and actions of the security team and security officers will depend on the unique features of the site and specific facts of the situation.

- Attempt to quickly determine the most reasonable way to protect your own life, and the lives of other people at the site.
- If safely possible, attempt to call 911.
- If safely possible notify other people at the site of the danger.
- If safely possible, attempt to assist others in escaping danger.

How to Respond When Law Enforcement Arrives on the Scene

Security officers should carry out the following, and if safely possible, attempt to help others take these actions:

How to react when law enforcement arrives:

- Remain calm, follow officers' instructions
- Immediately raise hands and spread fingers
- Keep hands visible at all times
- Avoid making quick movements toward officers such as attempting to hold on to them for safety
- Avoid pointing, screaming, and/or yelling
- Do not stop to ask officers for help or direction when evacuating, just proceed in the direction from which officers are entering the premise

Information to Provide to Law Enforcement or 911 Operator:

- Location of the victims and the active shooter
- Number of shooters, if more than one
- Physical description of shooters
- Number and type of weapons held by the shooters
- Number of potential victims at the location

See Something; Say Something

Any time you see something or someone unusual, out of the ordinary, or troublesome, alert your manager, or the SCIS Hotline. Do not ignore signs that could lead to danger.

EMPLOYMENT-AT-WILL STATEMENT POLICY DISCLAIMER

The employment relationship that exists between you and Securitas Critical Infrastructure Services, Inc. (the Company or SCIS) is employment-at-will. You are free to end your employment with SCIS at any time, for any reason, with or without prior notice. Likewise, SCIS may, at any time end your employment, with or without cause or prior notice. These policies, procedures and guidelines, and any other written or verbal communication by a supervisor or manager do not constitute a contract or promise of employment of any kind by the Company. No person in the Company can alter the employment-at-will relationship except the CEO of the Company, who can do so solely in a written agreement with the Employee. SCIS reserves the right to terminate employment, or to alter the terms of your employment, including changing your wages, assignments or shifts, as business necessitates, and may alter any other terms or conditions of employment, with or without cause, with or without notice, with the exception of its policy of at-will employment. To have the necessary flexibility in the administration of policies, practices and procedures, we reserve the right to delete, add to or otherwise modify policies, practices or procedures.

SCIS HAS RECOGNIZED SPECIFIC UNION ORGANIZATIONS AS THE SOLE AND EXCLUSIVE BARGAINING REPRESENTATIVE FOR CERTAIN GROUPS OF EMPLOYEES. COLLECTIVE BARGAINING AGREEMENTS (CBA) OR CUSTOMER SERVICE AGREEMENTS EXIST WHICH MAY, IN SOME RESPECTS, CONFLICT WITH THIS HANDBOOK. THE CBA OR CUSTOMER SERVICE AGREEMENT SHALL BE THE CONTROLLING DOCUMENT WHEN CONFLICTING LANGUAGE OR PROCEDURES ARE IDENTIFIED. IN THE EVENT THAT ANY OF THE PROVISIONS OF THIS HANDBOOK ARE, OR BECOME, INVALID OR UNENFORCEABLE, BY REASON OF THE COLLECTIVE BARGAINING AGREEMENTS, FEDERAL OR STATE LAW, REGULATION OR COURT DECISION, THE REMAINING UNAFFECTED PROVISIONS SHALL REMAIN IN FULL FORCE AND EFFECT.

FOREWORD

Dear Valued Employee,

Welcome to SCIS & Paragon Systems!

We are excited to have you join the team. Paragon is a special company, dedicated to safeguarding American assets at home, abroad, & beyond. You were hired because we believe that you will make a meaningful contribution to the achievement of our mission; to our success; and that you share our commitment and goals.

As a part of our team, we hope that you will discover that the pursuit of professional excellence and an uncompromising demand for integrity and achievement of mission will result in a rewarding and long-term career. It is our expectation that you will share in the ownership of our reputation and pride of our organization's dedication to serving the Federal Government and it's contractors.

At Paragon, we believe that each member of our team is essential to the organization's success. We seek to create an atmosphere within the company that will allow all employees to feel a sense of accomplishment and contribution. We pledge that our management will be fair in all employment decisions and that we will continually strive to improve our organization and the standards of living for each employee. We believe that both the company and its employees should be good citizens. We encourage you to contribute and participate in civic initiatives throughout the communities where we work and live.

Together, we are Paragon. Whether you are joining us straight out of school, the armed forces, as a second profession, or somewhere in between, there is a career filled with opportunities for you at Paragon across the national security landscape. Our flexible career paths and training programs provide a wealth of trajectories for your future. I hope that you will share our enthusiasm about Paragon and its growth and progress. We look forward to the future we will build together!

Sincerely,

Anthony L. Sabatino
Chief Executive Officer

THIS PAGE IS
INTENTIONALLY
LEFT BLANK

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

OUR COMPANY

Securitas Critical Infrastructure Services, Inc.

Securitas Critical Infrastructure Services Inc. (SCIS) is one of the largest providers in the United States of specialized security, fire and emergency response services to meet federal government security requirements in the Aerospace, Aviation, Defense, and Energy industries. As the national security provider for many Department of Defense, Aerospace and Intelligence contractors, SCIS is qualified to provide “Cleared Protective Services” to classified facilities. In addition to physical security, SCIS Investigations’ Sector is also a leading partner in the vetting of Federal civilian, military, and contractor personnel.

Our Mission

The mission of SCIS is to strive to preserve national security and improve the protection of the personnel, programs, resources, and facilities of our clients by providing high quality security services.

Our Values

Our business is built around a core set of values: integrity, vigilance and helpfulness. These values are simple, unchanging, and essential to the way we do business.

Integrity – The customer feels comfortable allowing us to work on their premises, knowing that we are trustworthy.

Vigilance – Our industry is based upon watchfulness, seeing, hearing, observing, protecting, evaluating, and reporting.

Helpfulness – SCIS strives to give its customers the very best service possible in assisting the client with their security needs.

Our SCIS Code of Business Ethics and Conduct (see Appendix) further reinforces our core values.

Our Company – A Look Back in History

The SCIS team has grown its security services with the acquisition of Paragon Systems, Inc. to include uniformed and armed security officers responsible for access control, law enforcement, personnel protection, theft prevention, surveillance, vehicular and foot patrol, crowd control and the prevention of sabotage, counterterrorism and crime deterrence. Extensive training, industry expertise and passionate dedication to excellence mark the cornerstones of Paragon’s history.

Today, our officers support vital homeland security programs and protect some of the nation’s most sensitive infrastructure. Through Paragon, our clients include the Department of Homeland Security, NASA, the Department of the Treasury, the Federal Bureau of Investigation, the Drug Enforcement Administration, the Federal Emergency Management Administration, the Social Security Administration, and the National Park Service.

Paragon is based in the Washington D.C. area and a subsidiary to SCIS. The relationship to the global security leader, Securitas AB, affords Paragon the ability to leverage the buying power, bench strength and economies of scale of an $11 Billion Dollar parent company. SCIS and Paragon are guided by a distinguished group of Americans who form our proxy Board of Directors.

In 2020, the Investigations and Energy sectors of Paragon's legal parent Securitas Critical Infrastructure Services, Inc. consolidated under the venerable Paragon brand to provide broader service capabilities and best represent our commitment to safeguarding American assets at home, abroad and beyond.

About our Team

SCIS is a diverse organization built upon teamwork and a collective commitment to quality, service, and integrity. Our employees bring to SCIS many different perspectives, experiences, and educational backgrounds. Much like our nation, we believe that our diversity has made our Company stronger and more competitive.

We take great pride in the many awards SCIS has won for excellence and dedication to service. We are a government approved vendor in all 50 states, Guam and the Virgin Islands. We are qualified to provide guard services and professional security services through the Federal Supply Schedule to all agencies of the federal government. Paragon is certified by the Virginia Department of Criminal Justice Services and dozens other state licensure boards. We hold facility clearances that permit us to perform classified work and provide cleared personnel.

Our Company's long history of accomplishment has been made possible by the commitment of SCIS's employees and their dedication to a common goal. Together, we believe the accomplishments are limitless.

Our Expertise

With over 14,000 professionals, Paragon and SCIS are the leading provider of specialized security, fire, investigations, inspections, cybersecurity, risk management, and mission support services to the U.S. Federal Government and other critical infrastructure clients. Following is a brief summary of our service lines:

SCIS and Aerospace Defense

The Aerospace & Defense sector secures highly sensitive controlled facilities on a national, regional and local basis. As the national security provider for many of the top department of defense, aerospace and intelligence contractors, SCIS is qualified to provide "cleared protective services" to classified facilities.

Paragon Cyber

Our newest business sector, Paragon Cybersecurity provides cleared, certified personnel - cyber professionals that can ensure digital assets are safe and secure, as part of a comprehensive security program. We focus our nationwide resources in two key areas: (1) Skilled Staffing and support, (2) Assessments.

Paragon Energy

Paragon Energy provides specialized protective services for owners and operators of nuclear power, fuel storage, and energy facilities.

Paragon Inspections

Paragon Inspections supports a variety of inspection needs to the Federal and State agencies across the country.

Paragon Investigations

Paragon Investigations includes federal background investigations and inspections, corporate due diligence investigations, and professional staffing services.

Paragon Mission Support

Paragon Mission Support is responsible for sourcing, assessing, hiring, training, and managing staffing needs to effectively execute the mission of Federal agencies. This can include a wide range of services from transportation to research support, from security personnel to customer service desks, from procurement specialists to professional services, from training personnel to quality control monitors and inspectors.

Paragon Protective Services

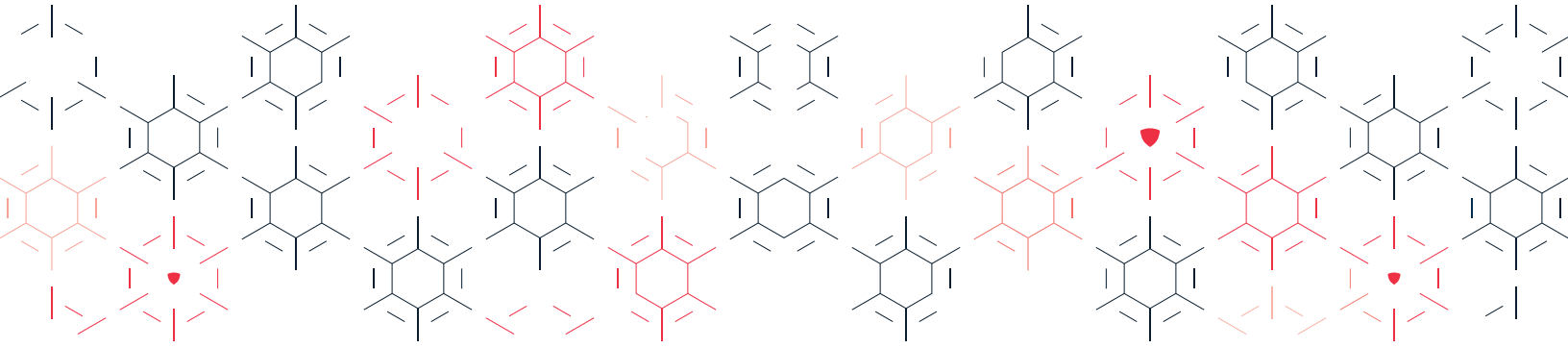
Paragon offers professional uniformed security services for Federal facilities. Our uniformed personnel are carefully screened, selected, and trained to offer the highest level of service.

Paragon Risk Management

Providing a combination of analytics, innovative technology and unparalleled experience, Paragon Risk Management is focused on identifying, managing, and mitigating the business risks of our clients.

SCIS Training and Instruction

Paragon provides its personnel one of the most comprehensive instruction and developmental training programs offered in the industry. Based upon the core principle that an officer will react the way the officer trains, our curriculum is designed to attract, develop, and retain the most highly qualified physical security professionals.



PRODUCTIVE WORK ENVIRONMENT

EEO & Affirmative Action Statement

SCIS is an equal employment opportunity employer. We recruit, hire, train, and promote persons in all job titles without regard to race/ethnicity, color, national origin, ancestry, sex/gender, gender identity/expression, sexual orientation, marital/parental status, pregnancy/childbirth or related conditions, religion, creed, citizenship status, age, disability, genetic information, veteran status, or any other status protected by local, state, or federal law. SCIS ensures that all personnel actions such as hiring, compensation, benefits, Company-sponsored training, education, transfer, discipline, demotion, assignment, termination, layoff, and social and recreational programs will be administered without regard to protected group status.

SCIS has in place an Affirmative Action Program that sets forth the specific affirmative action and equal employment opportunity responsibilities of managers, supervisors, and all SCIS employees. You may obtain a copy of the Affirmative Action Program by contacting your local office or a Human Resources representative.

All employees are required to follow the SCIS equal employment opportunity and affirmative action objectives stated above. You are asked to report any incident that you think may be a violation of this policy.

Diversity Policy

SCIS is committed to maintaining a work environment that represents a culture of diversity and acceptance, as employees' differences are respected and valued. We embrace our employees' differences and characteristics that make each employee unique. We believe that these differences contribute to our overall achievements as a Company. All employees of SCIS have a responsibility to treat others with courtesy and respect at all times.

Non-Discrimination on the Basis of Disabilities and Reasonable Accommodations

In accordance with the provisions of the Americans with Disabilities Act (ADA) and other applicable federal and state laws, no program or activity administered by SCIS shall exclude from participation, deny benefits to, or subject to discrimination any individual solely by reason of his or her disability. Equal employment opportunity will be extended to qualified disabled persons in all aspects of the employer-employee relationship, including recruitment, hiring, upgrading, training, promotion, transfer, assignment, discipline, layoff, recall, and termination. SCIS will make reasonable accommodations for the known disability of an otherwise qualified individual unless undue hardship on the operation of the business occurs. Employees who may require a reasonable accommodation should contact their local Human Resources representative.

Policy Against Discrimination and Harassment

SCIS is committed to providing a professional and productive work environment, based on a culture and atmosphere of mutual respect, and free from unlawful discrimination and harassment.

SCIS does not tolerate unwelcome verbal or physical conduct, advances of a sexual nature, or any discrimination or harassment based on gender (including gender identity/expression), sex, sexual orientation ("A person's actual or perceived sexual and emotional attraction, or lack thereof, to another person."), pregnancy, childbirth or related medical conditions, race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, citizenship status, marital status, military or veteran status, age, or other protected characteristic which violates local, state and/or federal law. Any individual who commits such a violation may be subject to discipline and possible termination of employment.

Sexual harassment is a serious form of employee misconduct which will not be tolerated by the Company. Additionally, in some cities, states or local geographies, sexual harassment is illegal. This includes Chicago, Illinois. Any employee found engaging in sexually harassing conduct will be subject to serious disciplinary action up to and including termination of employment. Sexual harassment in the workplace and retaliation for filing or assisting in the investigation of a complaint of sexual harassment is unlawful under federal, state, and most local laws

Each supervisor or manager strives to keep the workplace free of harassment. No supervisor or manager may threaten or insinuate that refusal or willingness to submit to sexual advances will affect an employee's employment. Supervisors are required to immediately forward reports of harassment to Human Resources or Company management.

All harassing, discriminatory, or offensive conduct in the workplace is prohibited, whether committed by an SCIS employee, member of the public, or client employee or agent. Examples of prohibited conduct include, but are not limited to:

- Unwanted physical contact or conduct, sexual flirtations, touching, kissing, brushing up against someone's person, advances, propositions, or assault
- Verbal harassment based on any protected characteristic, lewd comments, sexual jokes, or offensive/suggestive sexual references
- Demeaning, insulting, intimidating comments, objects, messages, pictures, or photographs
- Inappropriate comments about an individual's personal appearance
- Creating or forwarding demeaning, insulting, intimidating or sexually suggestive written, recorded, or electronically transmitted messages, including screensavers, texts, emails, websites, blogs, etc.
- Request for sexual favors or other verbal or physical actions where:
    - » Submission to or rejection of such conduct is made implicitly or explicitly a term or condition of employment or is used or threatened to be used as the basis for employment decisions; or
    - » Submission to or rejection of such conduct by an individual is used as the basis for any employment decision affecting the individual

» Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creates an intimidating, hostile or offensive working environment.

Inappropriate remarks about co-workers on social network sites, such as Facebook, or other similar types of social media.

If you believe any Company employee's or non-employee's actions or words constitute unwelcome harassment of any kind, you have a responsibility to report the situation to a Human Resources representative, your immediate supervisor, your local office management, or the SCIS Hotline (**1-800-574-8637 or www.scishotline.com)** as soon as possible.

The Company prohibits retaliation against any employee for making a complaint of discrimination, harassment, or retaliation in good faith. Any person taking retaliatory action against an employee for filing a complaint shall be subject to immediate dismissal. In certain geographies, retaliation for reporting sexual harassment is illegal. This includes but is not limited to Chicago, Illinois.

Any employee who believes that he or she has been subject to discrimination, harassment, or retaliation should promptly report the situation to a Human Resources representative, their supervisor, local management or the SCIS Hotline. The Company will undertake a fair, complete, and timely investigation by qualified and impartial personnel. The investigation will be documented and tracked to ensure reasonable progress and timely closure and will be kept confidential to the extent reasonably possible, consistent with the need to conduct an adequate investigation, and in accordance with applicable law. Corrective, remedial action, up to and including termination of employment, will be taken if misconduct is found.

Employees may also report complaints of discrimination, harassment or retaliation to the Equal Employment Opportunity Commission (www.eeoc.gov) or state fair employment agency (e.g., the California Department of Fair Employment and Housing, www.dfeh.ca.gov.) Additionally, you may also reach out to your local or state agencies. For those local and state laws, requiring specific information detailed in the policy, you may find that information below. For all others, you can find information via the EEOC and your state agencies.

Connecticut: Commission on Human Rights and Opportunities - 1-888-999-5545

Illinois: Illinois Human Rights Commission - 312-814-6269

Massachusetts: Commission against Discrimination (MCAD) – 617.994.6000

Vermont: Vermont Human Rights Commission – 800.4162010 / 802.828.2480 or the Office of the Attorney General – 802.828.3171

Rhode Island: Rhode Island Commission for Human Rights – 4021.222.2661

Gender Identity and Transition

SCIS seeks to ensure that employees who change their gender identity are treated in an equal and inclusive manner. Transgender employees shall not be subject to unwanted questions regarding their status, medical history, or sexual orientation. Also, any rude or inappropriate behavior towards transgender individuals, including the repeated or deliberate use of improper pronouns, is prohibited.

All employees are to comply with the appearance policy for their gender identity/gender expression and it is expected that employees will use the restroom and similar facilities appropriate to and reflective of their full-time gender identity. We ask that all employees maintain an environment of understanding and respect at all times.

If you believe any client personnel, tenant agency personnel & visitors' actions or words constitute unwelcome harassment or disrespect of any kind you have a responsibility to report the situation to a Human Resources representative, your immediate supervisor, your local office management, or the **SCIS Hotline (1-800-574-8637 or www.scishotline.com)** as soon as possible.

Policy Against Retaliation

SCIS prohibits retaliation against any person who, in good faith, reports a complaint of unlawful discrimination, harassment, or other suspected unlawful activity, testifies, assists, or participates in any investigation or proceeding conducted by SCIS or a government enforcement agency. All employees shall be free from coercion, intimidation, retaliation, interference, or discrimination for filing a complaint of sexual harassment or assisting in the investigation of such complaint. Any person taking retaliatory action against an employee for filing a complaint shall be subject to immediate dismissal. In certain geographies, retaliation for reporting sexual harassment is illegal. This includes but is not limited to Chicago, Illinois.

Pay Transparency Policy Statement

SCIS will not discharge or in any other manner discriminate against employees or applicants because they have inquired about, discussed, or disclosed their own pay or the pay of another employee or applicant. However, employees who have access to the compensation information of other employees or applicants as a part of their essential job functions cannot disclose the pay of other employees or applicants to individuals who do not otherwise have access to compensation information, unless the disclosure is (a) in response to a formal complaint or charge, (b) in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or (c) consistent with SCIS's legal duty to furnish information.

Company Hotline

All employees have access to the SCIS Hotline confidential reporting system. The SCIS Hotline is a way for you to advise SCIS in a simple and confidential manner of any situation that may adversely impact SCIS, its clients, or its employees. The following are examples of situations which should prompt a timely report to SCIS Hotline:

- Concerns about possible violence in the workplace
- Use of drugs or alcohol on the job
- Any form of harassment, discrimination, retaliation, or threats of violence
- Insider Threat

- Violation of safety or security policies
- Violation of any Company policy, practice or procedure
- Theft or fraud
- Misappropriation of Company or client property/funds
- Ethical violations
- Wage and hour violations
- Workers' Compensation fraud
- Benefit concerns or pay issues
- Violation of Federal Acquisition Regulations (FAR)

You may contact an SCIS Hotline Communications Specialist by dialing **1-800-574-8637** or go online to **www.scishotline.com** to confidentially file your report, seven days per week, 24 hours a day.

All calls and web reports will be promptly assigned to the designated Company contact for a response. You may call or file a web report anonymously.

Drug-Free Workplace

As part of the goal of maintaining a safe work environment, the Company has established a strong commitment to maintain a drug-and-alcohol-free workforce and workplace.

The illegal manufacture, distribution, possession, use, or being under the influence of narcotics, drugs, or alcohol is strictly prohibited by all employees while on duty, in uniform, or on Company and/or client premises. Any illegal substances found in the workplace will be confiscated and turned over to the appropriate law enforcement agency immediately. The Company's program includes the following, in accordance with applicable state law:

- Post-Offer Drug Test
- Reasonable-Cause Drug Test
- Post-Injury/Accident Drug and/or Alcohol Test (only if there is reason to believe drug and/or alcohol use caused or contributed to the cause of the workplace injury/illness and as permitted under applicable state law)
- Random Drug Testing (where required by client contract and/or permitted by state law)
- Under certain circumstances, applicants and employees may undergo alternative drug testing methods

Applicants or employees who test positive for alcohol or for drugs that are illegal under federal law will not be hired, or if already employed, will be terminated. A positive drug test for marijuana will

disqualify an individual from employment or continued employment, regardless of whether marijuana has been legalized for recreational or medicinal purposes under state law, unless the applicable state law provides otherwise.

All employees are provided a copy of the SCIS Drug-Free Workplace booklet. Any employee who violates the Drug-Free Workplace policy will be subject to disciplinary action, up to and including termination. If you do not have a copy of this policy, you may obtain one by contacting your local office. If you see any illegal drug activity while at work, report it to a supervisor, Human Resources, local management, or the SCIS Hotline.

Preventing Workplace Violence

As part of the goal of maintaining a safe work environment, SCIS has a zero-tolerance policy regarding violence in the workplace. Acts or threats of violence, including intimidation, harassment, and/or coercion will result in immediate employment termination. The prohibition against threats and acts of violence applies to all persons involved in Company operations including, but not limited to, SCIS personnel, contract workers, temporary employees, and anyone else on Company or client property.

Examples of workplace violence may include:

- Threats or aggressive behavior, including the use of threatening gestures or glances
- The intentional destruction or threat of destruction of property
- Harassing or threatening phone calls or notes, including electronically transmitted messages
- Surveillance not required by job responsibilities
- Stalking
- Bullying - repeated inappropriate behavior, either direct or indirect, verbal, physical, or otherwise, conducted by one or more persons against another or others, in the workplace and/or in the course of employment. Bullying can also be excluding or disregarding an employee, either socially or physically, in work-related activities.

Reporting Unsafe Conditions and Security Risks

If you become aware of any unsafe work conditions and/or security risks, including actual violence, pending violence, or threat of violence, immediately contact local law enforcement by dialing 911. Immediately after contacting law enforcement authorities, report the incident to your direct supervisor or another member of SCIS management. Follow post orders related to Client notifications.

You should always know your written post orders. They will explain additional duties and responsibilities for handling emergency situations and should contain the names and telephone numbers of individuals to contact in various emergency situations. You may also call the SCIS Hotline (1-800-574-8637) if you are unable to reach supervisory or management personnel.

In the event of a natural disaster, you should be familiar with the client's emergency evacuation plans, contact information for relevant law enforcement, first responders, client contacts, SCIS management,

and any information included in your post orders relative to natural disasters. The supervisor should provide training to security officers regarding safety regulations, rules, and procedures. If you have questions, seek clarification from your supervisor.

PROFESSIONAL DEVELOPMENT

SCIS is committed to the ongoing professional development and recognition of our employees. We want to be the best, so we want you to be your best! Development is a core focus of our operations; well-trained professionals provide superior service and satisfied clients. At SCIS, we truly believe that our People Make the Difference.

Professional development can help you increase your expertise, give better client service, and have more satisfaction on the job. SCIS practices promotion from within SCIS whenever possible. Training and development can help you prepare for advancement.

To help you excel on the job, SCIS has a full range of professional training, recognition, and communication programs.

Training Programs

SCIS maintains libraries of training books and videos on virtually every security subject. Our Center for Professional Development prepares and coordinates a broad range of training resources. Courses are available in e-learning programs and electronic management through the SCIS Online Academy. SCIS has a wide range of security-related self-study books, video courses, and instructor-led courses. Completion of training is done according to applicable law.

If you're interested in advanced training, you must first get approval from your supervisor or manager. Some available programs include:

The Five Star Security Officer Training Program

- Self-paced, available in books or online
- Certificates of Completion awarded after each level
- Progressively aligned with your career path
- SCIS merchandise earned upon completing levels 2-5
- Five levels to increase your professional knowledge

The SCIS Safe Driving Program

- Designed to teach you the latest defensive driving techniques

Recognition Programs

SCIS appreciates our employees' outstanding performance. We have a number of discretionary recognition awards to help us show our appreciation including:

- **Certificate of Training** – for completion of training.
- **Certificate of Merit** – for outstanding service.
- **Client Service Awards** – for distinguished service.
- **Officer of the Month** – each participating office honors its outstanding officer with a cash award and commemorative plaque.
- **Officer of the Quarter** – each participating office honors its outstanding officer with a cash award and commemorative plaque.
- **Officer of the Year** – usually chosen from Officers of the Month and Officer of the Quarter. The Officer of the Year receives a cash award and commemorative plaque.
- **Supervisor of the Month** – each participating office honors its outstanding supervisor with a cash award and commemorative plaque.
- **Supervisor of the Quarter** – each participating office honors its outstanding supervisor with a cash award and commemorative plaque.
- **Supervisor of the Year** – usually chosen from Supervisors of the Month and Supervisor of the Quarter. The Supervisor of the Year receives a cash award and commemorative plaque.
- **Officer of the Year for Performance** – this prestigious national award is presented to one or more officer(s) each year. The officer is nominated by his or her peers and managers for consistent outstanding performance and receives a substantial cash award and commemorative plaque at a ceremony of honor.
- **Officer of the Year for Heroism** – this prestigious national award may be presented to one officer each year. The officer is nominated by his or her peers and managers for heroic action and receives a cash award and a commemorative plaque.
- **Employee Referral Award** – participating offices may provide you a cash bonus each time SCIS hires someone you refer to us for employment. Contact your office for details.
- **Client Referral Awards** – participating offices may provide you a cash bonus if you give SCIS a sales lead that results in a new contract for permanent business. Contact your office for details.

BUSINESS ETHICS

It is SCIS policy that our business be conducted ethically. If you are asked to go against an established policy or practice or to engage in questionable ethical activity, whether by a supervisor, another employee, or by a client, report the issue and clarify any ethical questions you may have. This includes addressing the matter with the appropriate supervisor, management, Human Resources, or the 24-hour SCIS Hotline reporting system (1-800-574-8637 or www.scishotline.com) to obtain clarification and understand the issue in question. Questions and concerns may also be addressed confidentially to the SCIS Ethics Officer at ethics@scisusa.com. A copy of the full SCIS Code of Business Ethics and Conduct is included in the Appendix.

Attendance Standards

All employees are required to maintain satisfactory attendance and report to work on time every day. Due to the critical nature of your job and the need to correctly staff security posts at all times, you are required to report to work as scheduled. You will be notified of your schedule and break periods, as applicable. You are required to be at your post (and/or place of clocking in) and ready to begin work at your scheduled start time. If you do not report for duty or call to report an absence or late arrival, you will unfairly inconvenience a fellow employee, create scheduling problems, or leave a client facility unprotected. You are considered late if you are not at your work area at the starting time of your shift. **You are not required to be early for your shift, but you must not be late.**

You are expected to personally call your supervisor and/or the scheduler as far in advance as possible, and not less than four (4) hours in advance of the start of your shift (except in an emergency situation or instances involving sudden illness that makes four or more hours advance notice infeasible) when you know that you will be absent, late, or must leave work early, in order to allow for the necessary replacement. To avoid mistakes and misunderstandings, you should personally place the call. If your supervisor is unavailable, notification should be made to the next level of authority within your office. Leaving a voice mail message is not considered acceptable notification. Excessive absences of any kind can warrant discipline up to and including termination based on the circumstances. Your office and/or client site reserves the right to establish more stringent attendance and/or call off policies, in which case you will receive written notification.

Nothing in this section allows an employee to report or depart from work in a manner which contradicts management's directions.

If your absence is due to illness, the Company may request that you furnish a doctor's certification where the circumstances warrant and as permitted by applicable law.

When requesting a day off, you will be required to follow the guidelines established by your local office management. Failure to report to work or notify your supervisor of your absence within the proper timeframe ("No call-no show") is a serious violation of Company policy. It is also a policy

violation to leave post without proper relief or authorization from Company supervision. This is considered “job abandonment”.

Failure to show up or call may be considered grounds for termination.

Non-solicitation Policy

The purpose of the SCIS non-solicitation policy is to maintain an orderly workplace, to avoid intrusion upon employees and others, and to preserve employee safety and security for SCIS and its clients as to premises, funds, supplies, records, and confidential information. Accordingly, all employees are to observe the following rules and report violations to their supervisors. This policy includes charity solicitors, salespersons, questionnaire surveyors, union organizers, or any other solicitor or distributor.

- SCIS employees may not solicit for any purpose during work time. Work time includes that time for which the employee is paid and expected to be performing work. Work time includes both the soliciting and/or the solicited employee’s work time. Work time excludes meal or break periods.
- SCIS employees may not distribute or post literature during work time or in work areas.
- Except for legitimate SCIS purposes, and with prior authorization, individuals not employed by SCIS may not at any time solicit, survey, petition, or distribute literature on SCIS property.

Safety Policy

SCIS is committed to creating and maintaining a safe and healthy work environment. Each employee should become familiar with all safety regulations and report any unsafe or unhealthy situations. It is important that you recognize and follow all safety-related policies and procedures set forth by the Company or cited in client Post Orders.

SCIS’s Safety Policy is based on the following guidelines:

Company Commitment to a Safe and Healthy Workplace

Maintaining safe working environments is one of SCIS’s most important goals. The Company will not knowingly permit unsafe working conditions or permit employees to engage in unsafe acts. The Company will comply with all applicable workplace safety and health requirements and promote occupational safety and health standards that equal or exceed the best practices in the industry.

The Company will provide safety training and guidance to employees and will work to ensure that all employees comply with safety procedures and regulations, in accordance with OSHA guidelines. Reports of unsafe and/or unhealthy issues will be promptly investigated to determine cause and prevent the recurrence of similar issues.

The Company encourages all employees to provide suggestions and recommendations for achieving a safer, healthier workplace.

Employees Should Report all Safety Concerns

SCIS requires that employees work safely and assist in the prevention of accidents in the workplace. Signs, posters, and client Post Orders are made available to ensure that you consistently work in a safe manner. If you have questions regarding safety, supervisors, managers, and Human Resources are available to assist you in understanding all safety procedures and regulations.

Employees should report all safety and/or health issues, including occupational illnesses and injuries in a reasonable period of time, proportionate to the seriousness of the injury or illness. Prompt and appropriate reporting will allow the Company to immediately address the issue and assist the employee in seeking prompt medical attention if necessary. The timely reporting of injuries or illnesses will also enable the Company to notify fellow employees of the safety and/or health concerns in the workplace and help to prevent additional employee exposure. Retaliation for reporting work related injuries or illnesses is prohibited. Employees are expected to participate in all required safety training, wear required personal protective equipment and report hazards and unsafe work practices.

Reporting Unsafe or Unhealthy Working Conditions

The Company provides multiple avenues for reporting unsafe or unhealthy working conditions. If you or another employee identifies a potentially unsafe or unhealthy condition or situation, you should immediately contact your supervisor and document the issue(s) on an Incident Report or memo. This should be done so supervision can take the noted concern to the client to get the condition or situation corrected and the hazard eliminated. The other option is that employees may also report such issues directly to management, and/or file a report with the Company's 24/7, anonymous-enabled SCIS Hotline (1-800-574-8637 or www.scishotline.com), or as otherwise indicated by client Post Orders. The following of this process is highly encouraged as it gives the Client and the Company a chance to give immediate attention to the issue and complete the remediation of the hazard quickly. If a safety concern is not addressed in a timely manner, then officers are perfectly within their rights to file a complaint with OSHA.

SCIS prohibits retaliation against any person who, in good faith, reports a complaint, testifies, assists, or participates in any investigation or proceeding conducted by SCIS or government enforcement agency. Employees who engage in retaliatory behavior will be subject to disciplinary action, up to and including termination.

Uniforms and Appearance

In the security business, your appearance reflects your professionalism.

You will be issued either “wash-and-wear” or “dry clean- only” uniforms, at no cost to you. Wash-and-wear uniforms are designed and manufactured to be highly durable. They require only washing, drying, and hanging up with no additional maintenance. You are not entitled to pay for the time or expense for this type of routine maintenance.

If you are issued a uniform that requires dry cleaning or other special care, the local office will make arrangements for dry cleaning and will provide clean uniforms to you or reimburse you for dry cleaning expenses and the time spent driving to the cleaners. Contact your local office if you have any questions as to uniform dry-cleaning expenses.

You are also required to maintain ties, shoes, belts, and any other uniform-related items in a neat and clean condition. This means maintaining these items in a manner similar to your normal ties, shoes, belts, etc. These items do not require any type of special maintenance. If you have any questions as to how to maintain your shoes, belt, or other uniform-related items, please contact your local office for instructions.

If your uniforms require repair or alterations, or are worn out, please contact your local office for instructions. SCIS pays for uniform repairs and alterations, and any time the employee spends to have the uniform repaired or altered and provides new uniforms as appropriate. If you have any questions or concerns regarding uniform maintenance, please contact your local office.

Acceptable personal appearance and personal hygiene is requirement of employment. Unconventional personal grooming and hygiene standards are not permitted. You must comply with the following personal appearance standards:

You must comply with the following personal appearance standards.

1. You are required to wear Company uniforms. Only conventional belt buckles may be worn. Ornate buckles, unauthorized pins, patches or devices, political or other organizational symbols, of any kind, are not permitted, while on duty.
2. Basic black shoes, belts, and socks are required.
3. Appropriate undergarments are required under your uniform. In those instances, where ties are not a part of your uniform issue and open-neck shirts are permitted, only white tee shirts may be worn, unless otherwise stated by management.
4. Hairstyles must be neat and styled in a manner that is appropriate in the work environment. Unconventional or extreme colors of hair and/or hairstyles are not acceptable. For example, Mohawks are not considered appropriate hairstyles for the workplace. Hair ornamentation that is considered unconventional in style or color is inappropriate while in uniform. For example, excessive or unconventional clips, beads or feathers in your hair would not be considered appropriate in the workplace. Hair bonnets, “doo-rags,” kerchiefs, and similar hair coverings are not permitted unless specifically authorized by Human Resources. If you have a question about a particular hairstyle, contact Human Resources to confirm approval

5. Fingernails must be clean, neat, and not extreme in length or color.
6. Extreme looking facial hair, such as mutton chops, handlebar mustaches, and Van Dykes are not permitted. Beards, goatees, sideburns and/or mustaches may be worn if authorized by management and must be neatly trimmed.
7. Acceptable earrings are to be small hoop and “stud-like” in size and conservative in style and color. Over-sized earrings are not permitted.
8. Excessive jewelry may not be worn unless authorized by local management.
9. Visible body piercing accessories or visible tattoos are not permitted, unless authorized by management.
10. SCIS shoulder patches or client-furnished patches are the only acceptable insignia while on duty or in the work area.
11. When you wear an issued jacket, the breast badge must be on the outer garment and visible. Only jackets, coats, or raincoats issued and approved by SCIS may be worn over your uniform during work hours.
12. Where required, Company-issued caps must be worn at all times except when you are inside a vehicle or facility, or when special safety headgear is required. Doo-rags are not permitted.
13. You may not wear your uniform while you are off duty except when you are traveling to and from work.
14. When in uniform, you must not enter bars, lounges, taverns, casinos, or other places where alcoholic beverages are served, unless you are assigned to such an establishment while on duty.
15. You are not authorized to substitute personal items of clothing for SCIS uniform issue.

If found in violation of this policy, you will be subject to disciplinary action up to and including termination, depending on the circumstances.

Reasonable accommodations will be made for employees whose religious beliefs or medical conditions, or other legal requirements, require deviations from this policy, consistent with client requirements and safe operation of the business.

Management has the authority to modify the appearance standards set forth in these guidelines, according to business and client requirements.

Post Orders

Each client site has certain requirements for maintaining security on their premises. These requirements are explained in a document called the post orders. You must know the post orders applicable to your site and comply with them. Read the post orders, but only while you are on duty. If you have any questions or concerns, contact your supervisor.

If in the event a post order conflicts with applicable wage and hour law and/or SCIS wage and hour policies, the applicable wage and hour law and/or SCIS wage and hour policy controls. If the post orders cause you any concern, report the matter to your supervisor, local management, Human Resources, or the SCIS Hotline.

Company Issued Tools and Equipment

All equipment and/or tools required to perform job duties will be provided by SCIS and/or the client site where you are assigned. You are required to follow site-specific rules and procedures for storage and use of such equipment. On termination of employment, all equipment provided must be promptly returned.

Company and Client Communications Equipment

SCIS and client telephones are to be used for business purposes only. Do not make personal calls from Company or client telephones except in the case of an emergency.

Telephones, cell phones, 2-way radios, voice mail, computers, electronic mail (e-mail) systems and Internet access are maintained by SCIS and/or the client in order to facilitate business. There is no expectation of privacy when using these modes of communication. Therefore, all messages sent, received, composed, and/or stored on these systems are the property of SCIS or the client. If your message does not relate to Company business, is not an emergency and/or is not one you would want shared with your supervisor, or local SCIS management, please do not send it on Company and/or client equipment. Transmitting or downloading violent, pornographic or other inappropriate materials is strictly prohibited.

Unless specifically authorized by management, all personal electronic devices including recorders, pagers, digital cameras, tablets, and personal laptop computers should be locked in employee automobiles or another designated area during the time an employee is on post or at work. Employees may carry personal cell phones for emergencies, unless prohibited according to client requirements. Personal cell phone use may occur during authorized breaks.

Workers who damage Company or client equipment through intentional misconduct may be required to pay for damages, where permitted by state law.

All employees assigned a Company cell phone must comply with all state laws regarding “hands free” usage and/or the usage of cell phones.

Use of Personal Cell Phones / Devices

Security officers and other non-exempt/hourly employees are not required or expected to use their personal cell phones, computers, or other personal electronic devices for business purposes, and should not do so. You may be asked to provide a means of contacting you in the event of opportunities to work extra shifts. However, you are not required to provide a cellular device, or any device, for this purpose if you prefer not to be contacted and offered such opportunities. Similarly, if you provide a cell phone number as your contact number, that number may be used to reach you to offer you opportunities for extra work, but you are not required to respond. You will not be disciplined for not responding to calls/texts regarding extra work opportunities. Using your cell phone or other personal device for this purpose is not a compensable business expense.

If any security officer or other non-exempt/hourly employee believes he or she is being required to use a personal cell phone or similar device for business purposes (e.g. responding via phone, text, or email to questions about the security officer's work-related duties), the security employee should contact Human Resources. The Company reimburses employees for any authorized expense associated with the necessary business use of their personal cell phones and similar devices where such expense causes their compensation to fall below the applicable federal minimum wage (or overtime compensation) for all hours worked. Where applicable state law requires greater reimbursement, SCIS complies with applicable state law.

As a reminder, non-exempt employees are not permitted to work off-the-clock. All time spent performing work-related duties, including performing work remotely, must be reflected on an employee's timesheet.

Use of Computer Software

SCIS holds ownership rights to computer software programs and licenses and the right to use such programs obtained from outside companies. SCIS employees are prohibited from reproducing or copying software at work.

Employees are required to use software products in accordance with the license agreement for all local area networks (LANS) and multiple-computer networks. If you are aware of the unauthorized use of SCIS computer software applications or related documentation within SCIS you must immediately notify your local office. SCIS employees, who reproduce, acquire, or use unauthorized copies of computer software products may be subject to disciplinary action up to and including termination.

Acceptable Usage and Electronic Communications Policy

All SCIS employees are required to adhere to the following guidelines with regard to electronic communications. This policy also applies to consultants and contractors who have agreed to and acknowledged this policy, and covers all Company electronic data and communication equipment, including but not limited to:

- Electronic Email
- Instant Messaging
- Telephones
- Facsimile machines
- Internet publishing
- Wireless connections
- Cell Phones
- Pagers
- Copiers
- Voicemail Systems
- Computers
- VPN Connections
- Network
- Dial-Up Connections
- Flash drives/memory sticks
- External hard drives
- Cameras
- Personal Digital Assistants (PDAs)
- Tape Recorders
- Text Messages

Appropriate Usage

- Legitimate Company business use
- Consistent with all Company policies
- Appropriate business etiquette
- Emergencies

Prohibited Usage

Employees are prohibited from using Company or client electronic equipment or devices to knowingly create, view, display, transmit, retrieve, or store any data, material, or information that is:

- Personal use (except emergencies with supervisor or management approval)
- Spam, chain letter or mass emails
- Illegal communication
- Obscene or pornographic
- Political activities
- Derogatory or defamatory
- Rude, obscene, or inappropriate communication
- Misrepresenting or concealing one's identity
- Discriminatory, harassing, or threatening communication
- Threats of harm
- Any communication inconsistent with Company policies or Company business interests
- Communication directly or indirectly intended to diminish the business interests of SCIS
- Communications directly or indirectly intended to induce any employee to leave the employment of SCIS
- Communications to unauthorized persons regarding SCIS or client trade secrets and/or proprietary, confidential business information
- Electronic hacking

Monitoring: Employees may work at sites where monitoring and/or recording occurs. You may be subject to the monitoring of your use of Company and client electronic devices to include telephones, computers, and facsimile machines. Some Company and client facilities are equipped with security cameras; employees assigned to these facilities may be videotaped.

Recording: Employees are not permitted to record things at work except when directed by post orders or when directed by supervisor, or manager, or for legitimate business purposes (such as a safety issue), and as permitted under applicable law. Tape recording disciplinary sessions and/or investigations are only permitted according to applicable law. If questions arise regarding this provision, contact your Vice President, Human Resources.

Removal of Equipment from Company or Client Premises: Company or client communications or equipment may not be removed from Company or client premises without written authorization from your supervisor or Site Manager.

Breaching Employee Confidentiality: Employees must respect the privacy and confidentiality of other employees' electronic communication and data. Employees are prohibited from engaging in, or attempting to engage in the following:

- Monitoring or intercepting files or electronic communications of other employees, client employees, or third parties
- "Hacking" or obtaining access to systems or accounts to which they are not authorized
- Searching and viewing data not related to one's own job responsibilities
- Using logins or passwords of others
- Breaching, testing, or monitoring computer, network, or telephone systems without management authority
- Browsing or looking at another user's communications and data unless this is part of their job function, or they directly manage that employee.

Cameras: Employees are not permitted to take pictures while on duty unless required by Post Orders, or when directed by your supervisor or manager, or for legitimate business purposes (such as a safety issue), and as permitted under applicable law. This applies to cell phone cameras and/or any other photographic or video devices.

Social Networking

Employees are prohibited from conducting personal blogging or social networking activities while working and are prohibited from using any client-owned equipment, including computers, cell phones, or other electronic equipment for such activities. Internet postings by SCIS employees should comply with all applicable workplace policies stated elsewhere in this handbook and should always be sensitive to SCIS's objective of protecting the security and privacy of its clients. Examples of prohibited employee conduct on social media include:

- Postings that are threatening or menacing to anyone
- Postings, including unauthorized photographs or recordings, that infringe on the copyrights, trademarks, logos, or other intellectual property of SCIS or its clients
- Postings, including unauthorized photographs, recordings and or other comments, that reveal confidential or proprietary information of SCIS or its clients, including but not limited to trade secrets, security related procedures, equipment or systems, or that depict or disclose any non-public client facility or non-public area of a client facility
- Postings that violate SCIS's policy prohibiting harassment and other forms of discrimination, including but not limited to hate speech, racial epithets, and obscene or sexually offensive material
- Postings that maliciously disparage the quality of products or services of SCIS or its clients.

Any employee who engages in the conduct described above may be subject to personal liability, as well as discipline up to and including, termination.

Note: *Nothing in this Acceptable Usage and Electronic Communications Policy is intended or should be construed to interfere with employee communications regarding wages, hours or other terms and conditions of employment, or to interfere with our employees' ability to engage in collective or concerted activity for their mutual aid or protection as authorized by Section 7 of the National Labor Relations Act. By way of example, refusing to perform an act directed by management based on an employee's good faith belief that the act would be unlawful or unsafe is not "insubordination" within the meaning of this policy. Similarly, voicing good faith concerns about the terms or conditions of employment is not necessarily "derogatory" conduct prohibited by this policy and/or conduct against the best interests of the Company, as that term is used in this policy.*

Employee Arrests and Convictions

If you are arrested, charged with, or convicted of any crime during the course of your employment, you are required to notify SCIS management within three (3) days, regardless of whether or not you are incarcerated. In many areas, criminal convictions have an impact on your ability to carry a security officer's license or maintain a government personal security clearance and may be grounds for termination. Upon notification to SCIS of an arrest, and depending upon the circumstances, you may be placed on an unpaid leave for the duration of the legal proceedings. This policy shall be applied as permitted under applicable law.

Confidential Information

SCIS's and the client's trade secrets, confidential and proprietary information, and other internal information represent valuable assets. Confidential information is any and all information disclosed to or known by you due to employment with SCIS that is generally not known to individuals outside the company about its business. Protection of this information is important and should always be secured. Your obligations with respect to the proprietary information of SCIS and the client are as follows, to the full extent consistent with applicable law:

1. This information may not be disclosed to people outside of SCIS and the client
2. This information is not to be used for one's own benefit or for the benefit of people other than SCIS and the client; and
3. This information may only be disclosed to other SCIS and client employees on a "need-to-know" basis.

Special safeguards should be observed for Company information classified as "SCIS Private" or "SCIS Proprietary." These classifications impose "need-to-know" restrictions. Trade secrets and proprietary information includes, but is not limited to, business and strategic plans, divisional and regional revenues, hours of service, costs and profits, unpublished financial/pricing information, customer lists, vendor lists, detailed information regarding customer requirements, preferences, business habits and plans, computer log-on codes and passwords. You should contact your supervisor if you have a question regarding trade secrets or proprietary information.

Employees who leave SCIS have an obligation to not disclose Company trade secrets and proprietary information, unless the information becomes publicly available, or SCIS no longer considers it a trade secret. Correspondence, printed matter, documents of any kind, procedures, and special SCIS methodologies, whether classified or not, are all the property of SCIS. Any employee who violates these policies will be subject to discipline, up to and including termination of employment.

Conflicts of Interest - Outside Employment or Other Activities

While working, employees are required to devote their full effort, energy, and loyalty to SCIS. SCIS allows outside employment and activities as long as outside employment does not create an actual, perceived or potential conflict of interest, disruptions, or distractions that interfere with workplace productivity, or may be in competition with SCIS, pursuant to applicable law. Further, any outside employment not in conflict cannot be conducted in the workplace and should not be used as an excuse to not work overtime. You must advise and consult with management regarding this policy before becoming involved in outside employment, activities, or relationships that could violate this policy. SCIS employees are not permitted to work for two SCIS affiliated companies at the same time.

Employment of Relatives and Workplace Relationships

Employees' relatives will not be eligible for employment with SCIS where supervision, safety, security, morale, or other potential conflicts of interest may exist. Relatives include an employee's spouse, parent, child, sibling, aunt, uncle, in-law, foster parents, step relationship and cohabiting employees, dating couples, fiancés, or life partners.

Romantic or sexual relationships that create an actual, perceived or potential conflict of interest, potential charges of sexual harassment, discord, or distractions that interfere with workplace productivity are prohibited.

All questions and issues relating to employment of relatives and/or consensual relationships must be addressed with your management. An employee in a close personal or familial relationship with a co-worker or client employee must inform SCIS management immediately.

Release of Company Information/Press Inquiries

You are not authorized to issue any statement on behalf of the company, written or oral, to any news media representative or grant any public interview pertaining to SCIS's operations or financial matters. If you are contacted by a news media representative, please indicate that you have "no comment" and refer them to management. Management will forward all requests for information to the SCIS Director of Marketing, or designee, for an appropriate response.

Employment Verification

All requests for verification of current or prior employment may be submitted to The Work Number®. Whenever you need to have your employment or salary data verified, such as for mortgage applications, reference checks, loan applications, or apartment leases — anything you need that requires proof of employment, you are to contact The Work Number® by calling 1-800-996-7566 or through the internet at www.theworknumber.com. All requests received by local offices or management for verification of current or previous employment will be referred to The Work Number®.

Safeguarding of Personal Information

Personal employee information is considered confidential by SCIS, and as such will be safeguarded and shared only as required. The Company will only collect personal information that is needed for its business operations and to abide by government reporting and disclosure requirements. Personal employee information records will be kept in secure areas with access restricted to those who have a need for such access. SCIS is committed to abiding by the provisions of all applicable state and federal laws related to the safeguarding of employee information.

Smoking

Smoking (including e-cigarettes) and chewing tobacco are prohibited in all locations on Company and client property including inside Company vehicles, client vehicles, leased vehicles, and personal vehicles if being used while on duty. Employees are not permitted to smoke while on post. Only if approved by the client, smoking may be done within specifically designated smoking areas. Specific client sites may prohibit smoking or chewing of tobacco at any time on their premises.

Possession of Firearms and Weapons

You may not possess firearms, special security devices, or weapons at work without written approval of your management and/or where permitted under applicable local/state/federal law. This includes carrying a personal weapon or prohibited special security device on post, on client property, or in your personal vehicle parked at a job site or on Company property, unless expressly permitted by applicable law).

Examples of prohibited special security devices weapons include, but are not limited to: handguns, Tasers, lasers, knives, batons, brass knuckles, explosives, bullets, gun powder, tear gas, and billy clubs. Additionally, employees are not authorized to carry pepper spray, mace or handcuffs on duty unless authorized by appropriate management. **If you suspect that any employee is in possession of a prohibited special security device on the job, immediately contact your supervisor, Company management or the SCIS Hotline.**

Those security officers who carry firearms as required or permitted by the client contract may only carry Company-issued weapons and ammunition when approved by management and may only

do so after obtaining documentation and training showing they have been certified or approved by any applicable required licensing/certification board. In all weapons transportation situations, firearms are to be carried safely, securely and in accordance with applicable law. Company-issued firearms may not be altered in any way and are to be returned along with any other issued security devices immediately upon request or departure from the Company for any reason. Company-issued firearms may not be used while off duty for any reason.

Limits of Authority and Use of Force and Special Security Devices

Security personnel generally ***do not*** **have police powers beyond that of an ordinary citizen** and must operate under the laws regarding private person arrests and use of reasonable force. Officers are not permitted to touch, search, or arrest any individual except under limited circumstances. Arrest authority may only be conducted upon approval/authorization by the local authority having jurisdiction. The only circumstances under which a security officer may touch, search, or deter an individual are as follows:

1. When the individual has freely and voluntarily consented to the search
2. When acting in self-defense
3. When protecting the safety of other individuals
4. When instructed to do so by law enforcement

Use of Force. Security personnel are required to exercise extreme caution and good judgment when considering the use of force and the use of force should not be used for the retrieval of property. When faced with a clear and immediate threat of bodily harm, the security officer must always consider retreating with any other people present to a secure position.

A security officer must only use the degree of force necessary to repel an attack or threat of an attack. The use of deadly force should never be considered.

When a use-of-force situation arises, call the police for assistance and call Company management. Security officers who improperly use or apply excess force may be subject to disciplinary action and may be held criminally liable for their actions.

Documentation. In the event of any physical altercation involving a security officer, the officer must make every effort to secure names and addresses of all witnesses, along with names and addresses of person(s) involved. The officer will submit a detailed written report of the incident to appropriate Company supervision. This should be as soon as possible (preferably before end of shift, if officer is able) while all facts are still clear in the officer's memory.

Except as set forth in specific nuclear site training authorized by Federal law, deadly force is never to be utilized for the protection of property or information. "Deadly Force" is any use of force that is likely to cause death or serious bodily injury. Deadly force must only be used to defend life. Security officers who improperly use or apply excessive force may be held liable for their actions in a court of law.

Special Security Devices. Generally, security devices are not appropriate or necessary for normal security assignments. Accordingly, security personnel do not carry or use special security devices unless the facts and circumstances of a particular post assignment indicate that the use is reasonable and appropriate. In every situation, special security devices must be approved and authorized in writing by appropriate management. These devices may include handcuffs, firearm, holster, ammunition carriers, mace or pepper spray, soft body armor/bullet-proof vests or clubs. Unless approved by management, SCIS will issue the equipment, and officers will be trained in its use, and responsible for its proper transport, storage, and handling. All issued weapons and security devices are to be immediately returned upon request or upon departure from the Company. In addition, some states require security personnel to have permits to carry non-lethal weapons in addition to certified training. Applicable laws must be followed, without exception.

Vehicles

Whether driving a company vehicle, a rental/leased vehicle, or a personal vehicle while on company business, all employees must maintain a valid driver's license for the state in which the employee resides and for the class of vehicle they will be operating. The employee must also successfully complete the SCIS Safe Driving Training course. Upon introduction and prior to use of a new vehicle to the workplace, employees are to receive documented safety training on the proper use and precautions to be taken for each type of motorized vehicle they will be required to drive (e.g., car, truck, van, golf cart, Segway, Trikke, T3, etc.) while performing their specific duties. Refresher training is required every three years and/or whenever the employee is involved in any at fault motor vehicle accident.

Employees are required to exercise reasonable care, caution, and defensive driving techniques at all times when using motorized vehicles and equipment and are responsible for maintaining the security of the vehicle and its contents.

Each Company owned, rental/leased, client, or personal vehicle if used on Company business, must be inspected while on duty at the beginning of each shift or prior to use. If any vehicle malfunctions or safety concerns are noted, or if the vehicle needs any type of repair, notify your supervisor immediately to determine if the vehicle is to be used or removed from service and/or if a different vehicle will be provided. Employees are responsible for repairs of their personal vehicles. Repairs of Company vehicles must be approved by management, and generally, only a supervisor on duty can sign for gas and oil unless approved in site post orders.

Employees operating a Company, rental/leased, client, or personal vehicle while on Company business must comply with all local regulations, Company, and client driver safety policies. This includes complying with all applicable cell phone laws. Driving employees shall not operate any company/client vehicle at any time or operate a personal vehicle while on duty while using or consuming alcohol, illegal drugs, including marijuana, or prescription medications that may affect an employee's ability to drive.

Employees are not permitted to eat or smoke in vehicles while driving on duty (except during meal and rest periods). Employees are not allowed to drink anything other than water in company vehicles while driving on duty. Employees are required to exercise reasonable care in keeping Company

equipment and Company cars clean.
Per SCIS policies and procedures, any traffic violations or fines due to the employee's failure to comply with applicable laws will be the responsibility of the employee. All incidents, accidents, thefts, vehicle damage, or traffic violations that occur driving a motorized vehicle (regardless of whether it is a Company, client, leased, or personal vehicle) while on duty are required to be reported within a reasonable amount of time to supervision or the local office.

Employees must immediately notify the local SCIS office of any legal or physical changes that would affect the employee's driving privileges or insurability. All employees that drive on Company business must have a driving record free of serious traffic violations as outlined in the SCIS Safe Driving Program.

Any employee involved in a vehicle accident with a Company, client, rental/leased or personal vehicle while on company business where there is reasonable suspicion that the employee may have been under the influence and/or where property damage occurs or there is medical treatment needed, will be subject to a drug/alcohol test, where allowed by state and/or federal law.

Employees who operate Company, client, rental/leased, or personal vehicles may NOT carry passengers (SCIS or client employees, or any other individuals) without the written permission of the client and/or local office management. The vehicle must be capable and approved for passenger use. SCIS insurance requirements make this rule mandatory.

SCIS DOES NOT MAINTAIN PRIMARY LIABILITY OR COLLISION/COMPREHENSIVE INSURANCE FOR YOUR PERSONALVEHICLE. If using a personal vehicle to perform company business, you must at all times have and maintain liability insurance on your personal vehicle that is at least at the minimum level that is mandated by state law and be able to show proof of such insurance and provide a copy of the certificate of insurance to SCIS annually which will be maintained in the employee's personnel file. Insurance on personal vehicles used on Company business must be consistent with Company policy. Driving employees must notify the employee's insurance carrier that the employee will be using the employee's personal vehicle while performing work duties, and must provide SCIS with evidence of insurance coverage, which will be maintained in the employee's personnel file. Upon each renewal, or changes in carrier or policy, employees are required to again provide updated evidence of insurance. Please note that upon an at fault accident in your personal vehicle you will be responsible for any deductible payments to your insurance company. The mileage reimbursement you receive for using your personal vehicle for company business includes the cost of insurance.

If you use your privately owned vehicle while on official duty, you will be reimbursed according to Company policy and applicable law. Management, in accordance with federal guidelines, will determine the rate of reimbursement, and you will be advised on the rate of reimbursement that you will receive prior to your use of the vehicle. Use of a personal vehicle for any non-authorized work reason is prohibited.

YOUR EMPLOYMENT

EEO & Affirmative Action Statement

Your employment with SCIS is “at-will,” having no specified term, meaning you or SCIS can terminate the employment relationship at any time, with or without cause, and without prior notice.

Employment Classification and Status

Your employment with SCIS is “at-will,” having no specified term, meaning you or SCIS can terminate the employment relationship at any time, with or without cause, and without prior notice.

Introductory Period. Your first 90 days of employment are considered an introductory period. During this time, you will participate in an orientation to SCIS and receive any training required for you to perform your job duties. This “getting-acquainted” or introductory period gives your supervisor the opportunity to determine how well you perform your job. It also provides you the opportunity to decide if you are satisfied with the position. SCIS reserves the right to extend the duration of the introductory period when determined appropriate at the Company’s discretion. Upon completion of the introductory period, an informal performance evaluation may be conducted. Successful completion of the introductory period does not change the at-will employment relationship. Employees are employed on an at-will basis both during and after the introductory period.

Your continued employment at SCIS will be determined by your performance and the needs of the business. Here are some helpful definitions:

Full-Time Employee: For medical benefits purposes only, a full-time employee regularly works a minimum of 30 or more hours per week on a continuing basis and has completed the introductory period. For all other purposes, full-time employment is 40 hours per week / 2,080 hours annually

Part-Time Employee: For medical benefits purposes only, a part-time employee is hired for an indefinite period, but works less than a normal workweek of 30 hours per week.

Non-Exempt Employee: Employees who are paid on an hourly basis, such as security officers, are entitled to overtime pay according to applicable laws.

Exempt Employee: Exempt employees (such as certain supervisors or managers) are exempt from overtime provisions and not entitled to overtime pay.

Rehired Employee: Former employees who left the Company in good standing may be eligible for re-employment. Employees who are rehired following a break in service in excess of 30 days, other than an approved leave of absence, are considered new employees from the date of re-employment and will be required to complete the new hire process. For purposes of certain laws and benefits, the employee’s prior service will be counted where required by applicable law.

Mandatory Arbitration Program

SCIS has a mandatory arbitration program for resolving employment-related disputes. All non-union employees are subject to the Company's Arbitration Program. Arbitration is not intended to and does not replace existing internal Company dispute resolution mechanisms, such as informal complaints to supervisors or managers, Human Resources representatives or other Company representatives, or the use of the Company's Hotline. In the event a dispute between an employee and the Company cannot be resolved through informal means, the dispute will be resolved through binding arbitration, instead of the court system, except to the extent prohibited by applicable law.

Workers' Compensation and unemployment compensation benefits are not covered by the arbitration program. The arbitration program does not limit employees from filing workers' compensation claims or claims with the EEOC or other government agencies.

Application of the arbitration program may vary depending on applicable law. The terms and conditions of the Arbitration Program are contained in the Company's Dispute Resolution Agreement, which is provided to all employees. Please contact your local office if you need a copy of the Agreement.

Terms and Conditions of Employment

Security officers and field services staff are employees of SCIS and not the client site to which they are assigned. Clients contract with SCIS to provide services determined by a signed agreement. Based on client contracts and business necessity, you may be assigned to various clients, have a varied work schedule/workweek, different rates of pay and related benefits. Work related problems or concerns should be addressed by contacting your immediate supervisor, manager or Human Resources Manager.

As a further condition of employment, you are required to cooperate with the Company and its clients during any investigation or any other procedure requested by management. SCIS policy strictly prohibits retaliation in any manner toward individuals who provide information in good faith during an investigation.

Transfers and Promotions

SCIS encourages the professional growth of all employees. When opportunities for promotion occur, we will consider current employees along with qualified candidates from outside SCIS. Job openings may be posted on employee bulletin boards or in publications issued by your local office.

From time-to-time management will, when appropriate, fill job openings or make transfers without posting notices. If you request a transfer, you must have been in your current position for at least six (6) months, meet the requirements of the new position, and have a satisfactory performance record. A transfer out of a particular client site or out of the area is dependent on several factors. Please contact your Human Resources Manager for details.

Hours of Work

It is an SCIS policy to comply with all applicable wage-hour laws. You will be paid for all time worked. Your supervisor will determine your schedule of hours, and your meal and rest periods will be determined according to the unique features of your post assignment. You will be advised when your official workweek begins and ends.

Overtime

Because of the round-the-clock nature of security work, your supervisor may schedule overtime or extra shifts when necessary. Non-exempt security officers are paid overtime compensation in accordance with California law and the federal Fair Labor Standards Act (FLSA). Security officers are paid one and one-half times their regular rate for work in excess of 8 hours per day or 40 hours per week, and two times their regular rate for work in excess of 12 hours per day. Paid leaves, such as holiday, sick, PTO, bereavement time, and jury duty does not apply toward work time. If a security officer works seven consecutive days in one workweek, the officer will be paid at one and one-half times his or her regular rate for the first 8 hours, and at two times his or her regular rate for work in excess of 8 hours. All overtime must be approved in advance by your supervisor. Although an attempt will be made to give employees advance notice of the need to work overtime when it is feasible to do so, this is not always possible. SCIS will attempt to schedule overtime in a fair and consistent manner.

Pay Periods

Your local office will advise you of the frequency and timing of pay periods and paychecks.

Reimbursement of Expenses

If you are required to incur personal expenses as a function of your job, please contact your supervisor and such expenses will be reimbursed by SCIS as required by applicable law.

Training Pay

When you are assigned to work at a new client site, you may be required to undergo a short training period. During this period, you may be paid the applicable state minimum wage or in accordance with client contract provisions. If you obtain supervisory approval to take additional training courses, applicable to your job, you may be paid training wages at the applicable state or local minimum wage.

Travel Time

You will not be compensated for your commuting time to and from your home to your work assignment. However, if you are required to travel beyond your normal commute, the extra travel time will be

compensated as hours worked. For example, if you report to your regular job assignment and are then instructed to travel to another location to perform work, the extra travel time will be compensated as hours worked.

Meal Periods

At some assignments, off-duty meal periods are applicable. At such sites, officers take off-duty, unpaid meal periods. If you take an unpaid meal period, you will be relieved of all duties during such period.

In addition, because of the nature of the duties and responsibilities of a security officer, and the unique features and conditions at client sites and posts, some post assignments do not allow officers to leave the job site for meal periods. As a result, security officers sometimes take paid on-duty meal periods. In some states, the paid meal breaks are for 30 minutes. As a result, you will be provided an opportunity to voluntarily sign an On-Duty Meal Period Agreement and you will be paid for on-duty meal periods that you take pursuant to that Agreement. This agreement also applies to any second meal period when you are scheduled to work in excess of 10 hours, or the hours set by applicable state law. If you do not want to have paid, on-duty meal periods you may choose not to sign the On-Duty Meal Period Agreement, or you may contact your supervisor and request an unpaid meal period assignment. All applicable state laws will be followed.

Lactation Accommodations

SCIS will comply with all applicable federal and state laws in accommodating nursing mothers. SCIS will provide reasonable breaks from work to allow nursing employees to express breast milk. Reasonable efforts will be made to provide an appropriate area in close proximity to the employee's work area, other than a bathroom, which will be shielded from view and free from intrusion. The breaks will be unpaid except to the extent they run concurrently with other paid break time. If you have a need for such accommodation, please contact your Human Resources representative and/or local management directly. They will generally respond within 5 business days.

Timekeeping

All employees are paid in accordance with applicable federal and state and local wage and hour laws. It is important that you are familiar with the timekeeping procedures at your job site to ensure proper payment of wages for all time worked.

Rest periods and meal periods may be scheduled by your supervisor to ensure that your position and duties will be covered.

You are required to complete a daily timesheet. You are required to accurately record the actual time you begin work and the actual time you end work. Security officers and field services staff who have unpaid, off-duty meal periods must record the start and stop times of their meal periods as well. For sites where timesheets are used, all timesheets must be completed in ink. If you voluntarily arrive early for work, but do not actually begin to work, you must only record the actual time you begin

working versus your arrival time.

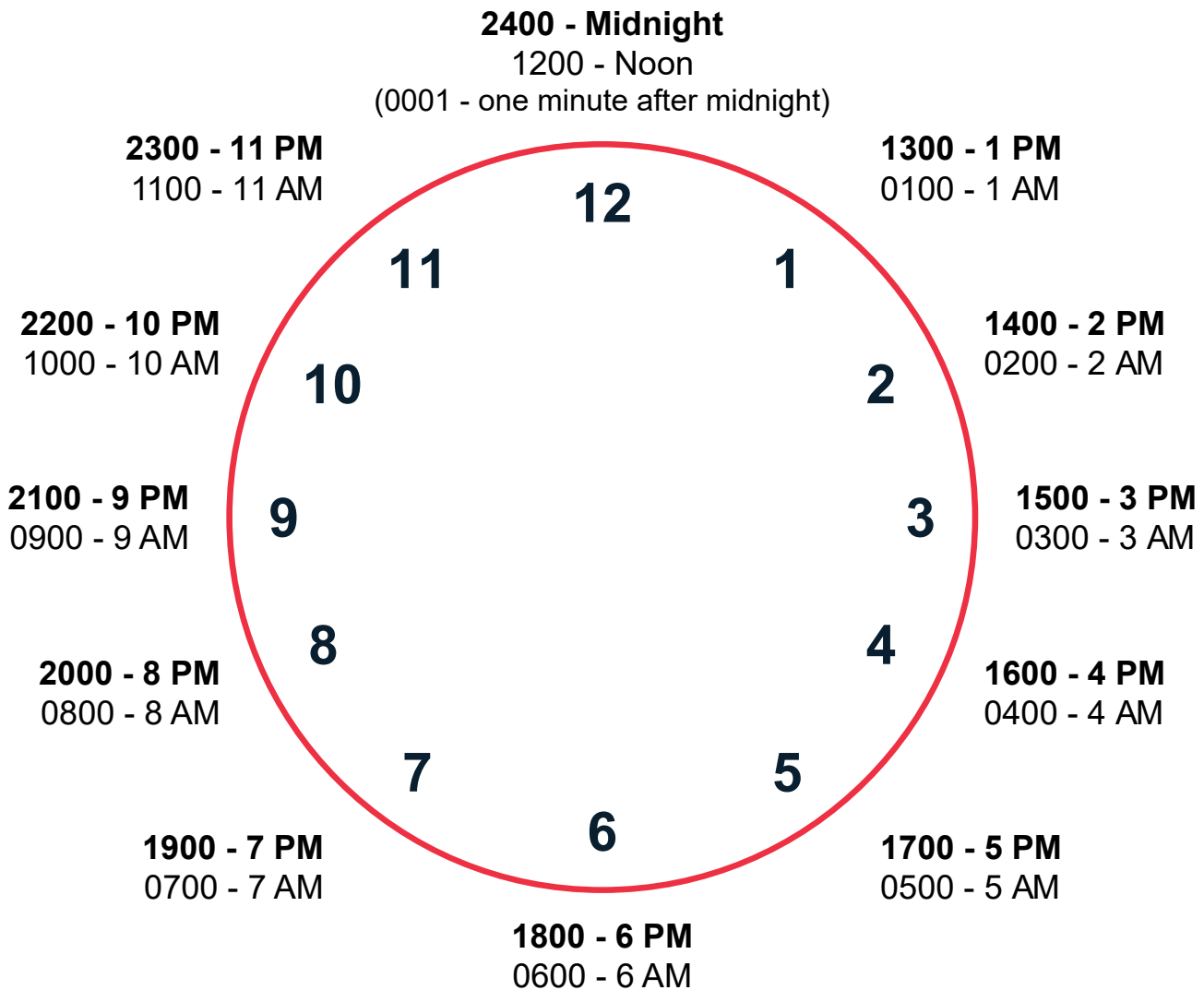
Employees are not permitted to work “off-the-clock” for any purpose. All time spent performing work on behalf of the Company must be reflected on an employee’s timesheet.

Each employee is solely responsible for the accuracy of his/her timesheet and must advise management of any discrepancies even after the timesheet is submitted.

Filling out another employee’s time record or falsifying any time record is prohibited.

Employees are required to contact the SCIS supervisor or office if they encounter any problems or concerns regarding being paid for all time worked.

24-Hour Time



Pay per Client Contract

You will be paid according to the client contract that applies to your assignment. If you work at more than one client site in a work week, with a different hourly rate at each site, the Company uses a weighted average (as required under federal law) to calculate any overtime rate. If you have a question about your pay, contact your supervisor or local management office.

Personal Status Change

Employees are required to notify the local office of any change in your personal status such as address, telephone number, withholding exemptions, etc. This is necessary to support scheduling efficiencies, as well as avoid confusion and errors, which could affect your pay or receipt of Company mailings.

Leaves of Absence

It is the practice of SCIS to grant a leave of absence in compliance with all state, federal, and local laws. Unless specifically provided for otherwise, all leaves of absence are available only on an unpaid basis. If you have a need to request a leave of absence, check with Human Resources for eligibility requirements and more information. Failure to return to work following the scheduled expiration of a leave of absence may be considered job abandonment and processed as a voluntary resignation.

FMLA Leaves of Absence. SCIS complies with the provisions of the federal Family and Medical Leave Act (FMLA) and all applicable state and local family and medical leave laws. FMLA provides eligible employees with up to 12 weeks of unpaid, job protected leave during a 12-month period for qualifying reasons, and up to 26 weeks to care for a qualifying injured or ill military service member. Eligibility: FMLA defines eligible employees as individuals who meet all of the following requirements:

- Have worked for SCIS for at least 12 months (52 weeks)
- Have worked at least 1,250 hours during the 12 months preceding the start of leave
- Work at or report to a worksite where the Company employs 50 of more employees within 75 miles of the worksite.

Once SCIS becomes aware that your need for a leave is for a reason that may qualify under the FMLA, you will be notified as to whether you are eligible for FMLA leave and, if eligible, you will be provided a notice of rights and responsibilities under the FMLA. You will be notified if the leave will be designated as FMLA leave, and if so, how much leave time is available. If you are not eligible, you will be provided a reason for ineligibility.

Qualifying Reasons and Duration of Leave: Eligible employees may take up to 12 weeks of unpaid leave, during a 12-month period, which is measured forward starting from the first day of the employee's leave, for the following reasons:

- The birth of an employee's child
- To care for a newborn or a child placed for adoption or foster care

- To care for a parent, spouse, or child who has a serious medical condition
- To recover from or obtain treatment for the employee's own serious medical condition. A serious medical condition is generally defined as a condition that requires any period of incapacity or treatment connected with inpatient care; any period of incapacity involving continuing treatment by a healthcare provider which requires an absence of more than three days; any period of incapacity, or treatment thereof, due to a chronic serious medical condition; or any incapacity due to pregnancy or prenatal care
- A "qualifying exigency" arising out of a covered family member's active duty or call to active duty in the Armed Forces.

Eligible employees may take up to 26 weeks of unpaid leave to care for a spouse, son, daughter, parent, or next of kin who is a member of the Armed Forces, and who is undergoing medical treatment, recuperation, or therapy for a serious injury or illness incurred in the line of duty. Leave to care for an injured or ill service member, when combined with other FMLA qualifying leave, may not exceed 26 weeks in a 12-month period.

Employee Rights under FMLA: Employees who take leave under FMLA generally have the right to return to the same position held when leave commenced, or to an equivalent position with equivalent benefits, pay, and other terms and conditions of employment. However, employees on leave have no greater rights to reinstatement or to other benefits and conditions of employment than if the employee had been actively reporting to work during the leave. During the leave period, the Company will continue health benefit coverage, when applicable based on client contract, as if the employee had continued to work; seniority will also continue during the leave period. Under certain circumstances, employees may take family and medical leave intermittently or on a reduced leave schedule.

Employee Responsibilities: Employees are responsible for providing proper documentation to support leave covered under FMLA, prior to such leave being approved as FMLA. Depending on the type of qualifying leave, this may include medical certification from a licensed practitioner, such as a completed Certification of Health Care Provider form, or proof of a qualifying family member's call to duty or active military service. Periodic re-certifications and/or fitness-for-duty reports may also be required.

If you believe that you may qualify for unpaid, job-protected leave under the provisions of FMLA, you should notify the Human Resources representative at your local office in writing, at least 30 days prior to your anticipated departure from work. If such notice is not possible, you are required to give as much notice as is reasonably possible under the circumstances.

If approved, you will be provided a Certification of Health Care Provider form to be completed and returned. If you fail to provide appropriate certification of your need for leave or fail to return from your leave when scheduled or fail to report in regularly during your leave (where requested to do so), or fail to request an extension if needed, you may forfeit your rights under FMLA. Additional details on your rights and obligations under FMLA and complete Company policy are available at your local office.

You may be required to use any accrued paid leave you may have, depending on state law, the reason for your leave under the FMLA, and whether you are receiving compensation from another source.

You may file a complaint with the U.S. Department of Labor, Wage and Hour Division, or may bring

a private lawsuit if you believe there has been a violation of FMLA. The FMLA does not affect any federal or state law prohibiting discrimination or supersedes any state or local law or collective bargaining agreement that provides greater family or medical leave rights.

Pregnancy Leave. SCIS complies with the Pregnancy Discrimination Act, FMLA, ADA, and all relevant Federal, state, and local laws with respect to leaves of absence for pregnant employees.

Medical Leave. SCIS will grant unpaid leave of absence for employees who are not FMLA eligible, but who need a temporary leave of absence as a reasonable accommodation under ADA, unless the leave would pose an undue hardship for the Company. A doctor's certification will be required validating the need for time off for treatment of a medical condition.

Personal Leaves of Absence. SCIS may grant a leave of absence for justifiable reasons for periods not to exceed 30 consecutive calendar days for employees who have had at least 12 months of continuous service. Your local management has full discretion and makes the final authorization in granting any leave of absence. However, if for any reason the leave has been misrepresented or business needs require your return to work, the leave may be canceled.

Because of scheduling requirements, SCIS cannot guarantee that requested time off will be granted.

Paid Family Leave. According to applicable state law, you may be eligible for paid family leave, which generally is a form of partial wage replacement provided by the state where an employee is on a leave of absence for certain reasons, such as caring for new child or family member with a serious health condition. Please check with your HR Representative for more information.

Military Leave. SCIS will comply with all applicable federal and state laws regarding military leave of absence and returning veterans' re-employment rights.

Jury and Witness Duty. A leave of absence resulting from jury duty or testifying as a subpoenaed witness will be granted in accordance with federal, state, or local laws. You will be granted an unpaid leave of absence (unless applicable law requires payment, in which case we will follow applicable law) for this purpose, provided a notice is presented to your supervisor. When practical, you should continue to report to work on days when you do not report for jury duty. It is your responsibility to return to work immediately following the expiration of jury or witness duty. If you are required to testify as a witness in an SCIS-related case, or on behalf of a client, you will receive your appropriate wage for the period of time required by the legal proceedings.

Bereavement Leave. Employees may be granted up to three consecutive workdays, without pay, unless specified by client contract, following the death of an immediate family member to arrange for and/or attend the funeral. Additional time may be requested with the approval of your supervisor. You may be requested to provide necessary documentation validating family relationship, proof of death, or funeral schedule.

For the purpose of this policy, "immediate family members" are defined as:

- Mother/father – to include in-law, step and foster parents
- Brother/sister – to include in-law and step relations

- Grandparent and grandchildren
- Spouse
- Child – to include step and foster child(ren)
- Legal guardian
- Domestic partner

Other Time Off. SCIS understands that you may occasionally need time off from work to address personal matters. Unless otherwise required by law, requests for time off work will be evaluated according to business necessity, scheduling needs and management discretion. SCIS will comply with its legal obligations under applicable state laws by providing you time off, where necessary, to vote, to perform emergency duty as a volunteer firefighter, to appear at your child's school or for certain school activities, pursuant to the request of the school, to attend an adult literacy education program, or in accordance with any state and/or federal laws. Time off that is provided under this policy will ordinarily be unpaid except where the law requires that it be compensated.

BENEFITS

Health Insurance

Benefit programs vary by location and client contract. Check with your local office or Human Resources representative for information on programs applicable to you. You may also consult the governing Summary Plan Description (SPD) for further plan and specific coverage information.

Life Insurance

SCIS generally provides group term life insurance in the amount of $10,000 for all full-time (30 hours or more per week) security officers and field staff employees, who have been employed for more than 90 days. In some cases, additional insurance may be available. Contact your local Human Resources representative for further details.

Employee-Paid Voluntary Benefits

SCIS provides employees with the opportunity to enroll in various voluntary benefit plans, depending upon location, for which the employee pays the full premium amount via authorized payroll deduction. See your Human Resources representative for more information or to enroll in any of these plans.

Medical/Dental/Other Insurance Client Site Specific

Certain locations and client contracts provide partially subsidized insurance coverage for employees and in some instances for immediate family members, as well. Your local office will inform you of any plans that may apply to you and will provide coverage and enrollment information. If you have questions, please contact your local Human Resources representative or your manager.

Employee Responsibility for Premium Contributions

When an employee temporarily ceases to make timely payments for his or her health insurance premium contributions, either through direct payment or payroll deductions, that health insurance coverage is subject to cancellation of coverage and loss of benefits. Employees on approved leaves of absence must make payments directly to the address indicated on the billing statements received. Certain leave benefits may be canceled in compliance with current regulations after a period of time. If applicable, you will be offered COBRA upon termination of benefits. Once you return to active duty, your benefits can be reinstated although specific plans and premiums may differ depending upon assignment. Please contact your local Human Resources representative for more information.

401 (k) Plan

All security officers and 5000 Series employees who have completed six (6) months of service and are at least 18 years old are eligible to participate in the Securitas Security Services USA Incentive Savings and Retirement Plan. This plan permits pre-tax salary deferrals and offers a variety of investment options through the plan administrator.

Unless otherwise provided for per client contract or collective bargaining agreement, most security officers receive a Company match of ten cents ($.10) on the dollar for the first three percent (3%) of salary that the employee contributes. The employer match fully vests at the end of three years of employment. Your own deferrals are always fully vested and may be rolled over to an individual IRA account or another qualified 401 (k) plan even if you leave SCIS prior to the vesting of your employer match. Depending upon the client site to which you are assigned, different waiting periods and additional matching or profit-sharing contributions may apply.

If you do not receive enrollment information after you become eligible to participate, contact your local office or Merrill Lynch at 1-800-228-4015.

Short-Term Disability

Where required by state law, short-term disability benefits are provided either through a state program or insurance plan. Contact your local office to find out if your state has this benefit. For those residing in a state that does not provide short-term disability, SCIS provides employees with the opportunity to enroll in voluntary short-term disability for which the employee pays the full premium amount via authorized payroll deduction.

Employee Assistance Program

In recognizing that the success of SCIS and our business depends upon the well-being of our employees, SCIS offers an Employee Assistance Program (EAP) to all full-time employees who have completed 90 days of service and their qualified dependents.

Qualified employees and family members may receive assistance in managing life's challenges outside the workplace such as financial and credit problems, loss of loved-ones, personal relationship issues, substance abuse or dependency, concerns regarding parents or children, stress, anxiety, and any other personal circumstances that may require skilled professional help.

For up to five face-to-face counseling sessions per family member, per incident, per year there is no charge to the employee. An employee or eligible family member may obtain assistance by dialing 1-800-865-1044, 24 hours per day, 7 days a week. Online member services are also available at anthem.com / eap. Access code is "paragon".

Payroll Choices

Under the Payroll Choices Program, and where allowed by state law, SCIS offers two options to receive your pay; either by Direct Deposit, or a personalized and secure MasterCard ® Payroll Card, provided by Wirecard Prepaid Services. With direct deposit, you can select the bank account(s) of your choice, while the Payroll Card requires no bank accounts.

Advantages of Direct Deposits:

- Choose your own bank
- Deposit funds in up to three separate accounts
- No lost checks or delivery delays
- No check cashing fees

Advantages of Pay Cards:

- No bank account required
- Pre-Check option included
- Make purchases anywhere MASTERCARD is accepted and get cash at ATMs or banks
- No waiting for checks to clear

Please contact your local office for an enrollment form to set up either direct deposit or request a pay card. Employees who prefer a traditional paper paycheck may also request that option, where such an option is required by applicable law.

Workers' Compensation

SCIS has Workers' Compensation insurance coverage, as required by law, to protect employees who are injured on the job. This insurance provides medical, surgical, and hospital treatment in addition to payment for loss of earnings that result from work-related injuries. The cost of this coverage is paid by SCIS.

If you are injured while working, you must report the incident within a reasonable amount of time proportionate to the seriousness of the injury or illness to your supervisor regardless of how minor the injury or illness may be. If you have any questions regarding the Workers' Compensation Insurance Program, please contact your local office.

Holidays

Holiday schedules vary depending upon your client site. Normally you will not be paid for the holiday unless you work on that day.

Vacation/PTO

Eligible employees will accrue time off in accordance with the terms of the SCIS vacation pay policy and applicable law. In some jurisdictions, the vacation policy may be replaced by a Paid Time Off (PTO) policy.

Some general highlights of the policy are:

- Vacation/PTO is determined by the number of hours worked during the anniversary year subject to certain policy or applicable law maximums.
- Vacation/PTO accrual may vary based upon applicable state or local law, client contract and/or a collective bargaining agreement.

Generally, employees should submit known vacation/PTO requests to their supervisor in advance in accordance with your local office's requirements. If you have any questions regarding your eligibility for vacation / PTO, or need further information on the Company policy, please contact your local office.

Sick Days

SCIS provides for paid sick days according to state or federal law, or pursuant to client contract, or a collective bargaining agreement.

For those employees who receive paid sick days, unless otherwise provided, the paid sick days may not be used for purposes of vacation.

DISCIPLINE AND TERMINATION

Voluntary Separation

A separation is considered voluntary when you elect to resign. Whenever possible, you are requested to submit, in writing, the reason for resignation and your anticipated departure date.

If you are thinking of resigning, please talk it over with your supervisor and/or your local management before doing so. If you do decide to leave, we would appreciate two weeks' notice, although this is not required. Employees who provide adequate amount of notice will be considered to have resigned in good standing and generally will be eligible for rehire.

If you fail to report for work after three (3) consecutive workdays without contacting your supervisor or fail to return from a leave of absence on the designated date, you may be considered to have voluntarily terminated your employment with SCIS.

Involuntary Separation/Layoff

There are certain times when it may become necessary to lay off employees as a result of changing business conditions. Examples of these conditions include but are not limited to:

1. Reduction in work force
2. Loss of client contract
3. Reorganization resulting in the elimination or modification of a job.

When SCIS concludes that a layoff or reduction in force is necessary or appropriate, the positions and/or employees to be eliminated will be selected based on a number of factors, which may include demonstrated performance and skills, ability and reliability, and seniority.

Other Employer-Initiated Separations

When any employee fails to meet SCIS's and/or client's expectations, SCIS may end the employment relationship. Misconduct will be cause for termination. Generally, employees who are unable or unwilling to meet performance, attendance and conduct expectations will be subject to discipline up to and including termination of employment.

DISCIPLINE AND TERMINATION GUIDELINES

Actions That Warrant Immediate Termination of Employment

Below is a partial list of conduct which, depending on the circumstances and severity of conduct, warrants involuntary termination on the first occurrence. Such offenses include, but are not limited to, the following:

1. Threatening or committing physical violence or intimidating behavior.
2. Illegal conduct, discrimination, or harassment.
3. Misuse, excessive, or inappropriate use of Company or client property, such as telephone or computer.
4. Insubordination or derogatory behavior.
5. Breach of confidence, including misappropriation or misuse of confidential information.
6. Falsification of any Company record, providing false information or false statements to management.
7. Theft, unauthorized taking or removal of client or Company property or the property of another person or other dishonesty.
8. Violation of Company policy or misconduct of any kind.
9. Damage to Company or client property.
10. Disruptive or inappropriate conversations at work.
11. Filling out or completing a Company time record for another person, or knowingly allowing someone else to fill out one's own timecard or timesheet or falsification of time records, or other violation of wage and hour laws.
12. Carrying or the possession of weapon(s) such as gun(s), dangerous devices or other weapons on Company and/or client premises including parking lots without proper written authorization by Company management, and/or in violation of applicable laws.
13. Conviction of or pleading guilty to violation of any criminal statute or code, whether or not such a crime is committed against SCIS or any of its employees when, in SCIS's opinion, and in accordance with applicable law, such conviction or guilty plea is reasonably related to the nature of the employee's work or continued employment could jeopardize SCIS or client interests.
14. Participation in events or activities that create a conflict of interest with SCIS, as permitted under applicable law.
15. Use of or being under the influence of alcohol, intoxicants, illegal drugs or controlled substances during work hours, or on Company property or in Company or client vehicles, testing positive for illegal drugs or controlled substances (including marijuana) following a Company drug test; violation of Drug Free workplace policy, as permitted under applicable law.
16. Sale, purchase, attempted sale or purchase, possession, or transfer of intoxicants, illegal drugs or controlled substances during work hours, or while on the job, on Company property, or in Company vehicles.
17. Leaving post without proper relief or authorization from your supervisor or "no call, no show".

18. Willful or repeated violation of safety rules.
19. Willful or repeated violation of Company Code of Business Ethics, our Sexual Harassment Policy, or other forms of unlawful discrimination.
20. Failure or refusal to participate in a lawful company investigation.
21. Participating in any relationship or activity that creates a conflict or potential conflict of interest, discord or distractions that interfere with the productivity of the workplace.
22. Repeated failure to accept assignments.
23. Unauthorized or improper use of a Company or client vehicle.
24. Falsifying the reasons for a leave of absence.
25. Significant violation of a client's Post Orders.
26. Sleeping while on duty, or the appearance of sleeping while on duty.
27. Inability to obtain and retain government security clearance, if required.
28. Behaviors or actions that would result in the loss of government security clearance.

Note: *Nothing in this policy is intended or should be construed to interfere with employee communications regarding wages, hours or other terms and conditions of employment, or to interfere with our employees' ability to engage in collective or concerted activity for their mutual aid or protection as authorized by Section 7 of the National Labor Relations Act. By way of example, refusing to perform an act directed by management based on an employee's good faith belief that the act would be unlawful or unsafe is not "insubordination" within the meaning of this policy. Similarly, voicing good faith concerns about the terms or conditions of employment is not necessarily "derogatory" conduct prohibited by this policy and/or conduct against the best interests of the Company, as that term is used in this policy.*

Actions That May Result in Warning Prior to Termination of Employment

SCIS may, depending on the circumstances and the severity of the conduct, either issue a disciplinary warning or terminate employment for:

1. Inefficient or substandard performance of an assigned duty or responsibility.
2. Pursuant to applicable law, unauthorized use of radios, televisions, personal cell phones, pager, recording devices, computers, electronic games and/or devices, or reading materials while on duty.
3. Excessive absenteeism and/or tardiness in reporting to work or returning from rest periods or meal periods.
4. Failure to report an absence in accordance with the attendance policy or failure to report a work-related injury.
5. Carelessness or negligence in the performance of an assigned duty or in the care and use of Company or client property.
6. Abusive, foul, or inappropriate language.

7. Discourtesy to other SCIS employees, clients, or other individuals.
8. Posting of notices or other written material on Company property without prior written approval of SCIS.
9. The circulation or distribution of unauthorized written material of any type in working areas or during work time.
10. Personal use of a pager or cellular telephone while on duty.
11. Failure to work overtime when an emergency occurs.
12. Repeated failure to adhere to dress code and/or grooming standards.
13. Violation of internal chain of command (employees will not be subjected to negative treatment as a result of complaining about their working conditions).
14. Allowing personal visitors to remain at post while on duty.
15. Bringing pets to work (except as authorized in advance as a reasonable accommodation for a disability).
16. Showing up or socializing at a client site when not scheduled to work.
17. Violation of Post Orders.

Group Health Benefits and COBRA

Your health benefits will terminate at the time of separation in accordance with that plan's coverage contract. In most instances, you may continue basic health benefits under the Consolidated Omnibus Budget Reconciliation Act (COBRA). You will be advised of this option by the Benefits Department after your local office has provided notice of your separation.

Life Insurance Portability/Conversion

Separated employees covered by the Company's Group Term Life Insurance will be provided with notices regarding options to continue or convert their term life insurance coverage. Appropriate paperwork must be signed and submitted to the Insurance Carrier directly within 30 days of employment termination. If you are interested in continuing or converting your life insurance, you should contact your local office or the Securitas USA WOC Benefits Department.

Final Wages

Your final paycheck will be provided to you as required by applicable state law.

LOCAL OFFICE ORGANIZATION & TELEPHONE NUMBERS

Local Office

Local Office — Phone #

Scheduler — Phone #

HR Representative — Phone #

Police — Phone #

APPENDIX A

SCIS Code of Business Ethics and Conduct

1.0 Purpose

The intent is to establish policy and procedures relative to business ethics, integrity, and honesty for Securitas Critical Infrastructure Services, Inc. (“the Company” or “SCIS”).

2.0 Applicability

This policy is applicable to all SCIS employees and those of its subsidiaries or affiliates. This policy does not apply to employees of Paragon Systems, Inc. or its subsidiaries.3.0

3.0 Policy

Compliance with this policy is mandatory. Failure to follow this policy exposes SCIS, and possibly its employees, to legal sanctions and damages, and could damage the reputation of the Company and its employees. It is the policy of SCIS that its business will be conducted according to the standards set forth in this policy, the Securitas Values and Ethics Code (Exhibit A) and the Securitas Anti-Corruption Policy (Exhibit C).

4.0 Procedure

SCIS employees will maintain high ethical standards in conducting business. This policy also requires that each employee conduct Company’s business consistent with applicable laws.

The following is a summary of the Company’s policy with respect to (1) bribes, gifts, and entertainment; (2) business amenities, and (3) certain other matters:

4.1 Bribes, Gifts and Entertainment

Gifts offered by employees of different companies vary widely. They can range from widely distributed advertising novelties of nominal value, which you may give or accept, to bribes, which you unquestionably may not give or accept. Gifts include not only material goods, but also services, promotional premiums and discounts. The following are SCIS’s general guidelines on giving and receiving gifts and business amenities. Under these guidelines, senior management may also approve giving or receiving higher value gifts and business amenities provided the gifts and business amenities are not prohibited by law or known client business practice.

Receiving Gifts

Neither an employee nor any member of their family may solicit or accept from a supplier or client money or a gift that could influence or could reasonably give the appearance of influencing SCIS’s business relationship with that supplier or client. However, unless SCIS has specified to the contrary, they may accept promotional premiums and discounts offered by transportation companies, hotels, auto rental agencies, and restaurants if they are based upon membership in bonus programs for individuals and are offered to travelers generally. Furthermore, employees may accept a gift of nominal value, such as an advertising novelty, when it is customarily offered

to others having a similar relationship with the client or supplier. If employees have any doubt about a particular situation, they should consult their manager. If they are offered a gift which has more than nominal value or which is not customarily offered to others, or money, or if either arrives at their home or office, inform management immediately. Appropriate arrangements will be made to return or dispose of what has been received, and the supplier or client will be reminded of SCIS's gift policy.

Giving Gifts

Employees may not give money or any gift to an executive, official, or employee of any supplier, client, or any other organization if doing so would influence or could reasonably give the appearance of influencing the organization's relationship with SCIS. Employees may, however, provide a gift of nominal value, such as an SCIS advertising novelty, if it is not prohibited by law or the client's known business practices.

4.2 Business Amenities

With management approval, employees may give or accept customary business amenities, such as meals and entertainment, provided the expenses involved are kept at a reasonable level and are not prohibited by law or known client business practice. Suppliers frequently find it appropriate to provide education and executive briefings for their clients. An SCIS employee may provide or accept some services in connection with this type of activity, such as transportation, food, and lodging, with management approval.

4.3 Referral Fees

When authorized by SCIS, employees may refer clients to third party vendors such as SCIS authorized remarketers, SCIS authorized assistants, third party software organizations, or financial institutions. However, SCIS employees may not accept any fee, commission or other compensation for this activity from anyone except SCIS.

4.4 Relationships with Government Employees

Acceptable practices in the commercial business environment, such as providing education, transportation, meals, entertainment, or other things of value, may be entirely unacceptable, and may even violate certain federal, state, local, or foreign laws and regulations, when dealing with government employees or those who act on the government's behalf. Therefore, employees must be aware of, and adhere to, the relevant laws and regulations governing relations between government employees and clients and suppliers in every country where they conduct business. Employees should contact the SCIS Ethics Officer for guidance. Employees must not give money or a gift to an official or an employee of a governmental entity if doing so could be reasonably construed as having any connection with SCIS's business relationship.

4.5 Personal Conflicts of Interest

SCIS employees are expected to refrain from any private business or professional activity, or from having any direct or indirect financial interest, which would place them in a position where there is a conflict between their private interests and their legal, fiduciary, or contractual responsibilities to the Company. In their transactions with others, all employees are expected to act in the best interest

of the corporation and not for their own private advantage. They must not engage in any private or professional activity or enter into any financial transaction which involves the direct or indirect use of inside information (information that has not become public information), gained through their position with the corporation, to further a private interest or for private gain for themselves or another person or entity. They must not use their position in the corporation in any way to induce or coerce any person or entity to provide any financial benefit to themselves or another person or entity.

Each employee shall make a prompt and full disclosure in writing to the Company's Vice President of Human Resources and SCIS Ethics Officer of any situation that may involve a conflict of interest. These include but are not limited to: Ownership by an employee, or a family member, of a significant financial interest in any outside enterprise that does or seeks to do business with, or is a competitor of, the Company.

- Ownership by an employee, or a family member, of a significant financial interest in any outside enterprise that does or seeks to do business with, or is a competitor of, the Company.
- Serving as a director, officer, partner, or consultant or in any other key role in any outside enterprise that does or seeks to do business with, or is a competitor of, the Company.
- Acting as a broker, finder, or other intermediary for the benefit of a third party in transactions involving the Company or its interests.
- Any other arrangement or circumstance, including family or other personal relationships that might dissuade the employee from acting in the best interests of the Company.

Employees may not hold positions as a director, officer, employee, partner, or other position (including consulting) in any business or professional enterprise which interferes with the performance of their duties as officers or employees of the corporation or which involves obligations, which may conflict with the interests of the corporation unless specifically approved by the President.

4.6 Organizational Conflicts of Interest

No contract will be negotiated or executed if the interests of the particular customer are of such a nature as to compromise or threaten the Company's ability to maintain unbiased objectivity in serving its other customers. In instances where potentially conflicting situations may be created, agreements may be entered into if the parties involved have full knowledge of the potential conflict and consent to the arrangements in advance. The contract file should contain a statement documenting that the responsible SCIS employee has made the disclosures and obtained the consents which are necessary hereunder.

4.7 Political Participation & Contributions

SCIS encourages its employees and officers to participate in the political process, and nothing contained herein shall be deemed to prohibit any officer or employee from engaging in political activities in an individual capacity on his own time at his own expense or from making political contributions or expenditures of his personal funds or resources. However, no expenses incurred or contributions made for political purposes will be reimbursed by the Company.

SCIS will not make direct or indirect contributions to any political party or candidate for political office, or regarding any ballot measure, whether in the United States or any other country, without the

express authorization of the Board of Directors and such authorizations shall be recorded in minutes of the Board of Directors. In addition, in supporting the political process, SCIS will not:

- nfluence or attempt to influence public officials by offering gifts, gratuities, or other promises or reward or benefit;
- Offer or accept a bribe in connection with an election;
- Make a campaign contribution or expenditure in the name of the company or on its behalf; or
- Reimburse anyone who makes a contribution to a political party, candidate, campaign or cause.
- Submit false, incomplete or misleading information to government agencies that oversee and enforce campaign finance laws.

Pay-to-Play Rules

The U.S. federal government and U.S. state governments have varying “pay-to-play” rules (i.e., laws that regulate or restrict campaign contributions by contractors). These laws generally do one or more of the following:

- Require SCIS and certain personnel to disclose campaign contributions;
- Prohibit SCIS and certain personnel from making campaign contributions; or
- Disqualify SCIS from being a state contractor if campaign contributions are made.

It is important that you consult with the SCIS Ethics Officer before making any political contributions.

Lobbying

“Lobbying” is any effort to influence the legislative, regulatory or other administrative process of a government entity, and includes efforts to make contacts with government officials or employees in order to obtain contracts and other business engagements with such entity. To ensure compliance with these laws, SCIS personnel may not engage in any of these lobbying activities, as described above, or retain any other person or entity to do so on behalf of SCIS without prior approval from the SCIS Ethics Officer.

4.8 Foreign Corrupt Practices Act (FCPA)

The Foreign Corrupt Practices Act (FCPA), a U.S. law, makes it a crime to pay money or to give anything of value to a foreign official, a foreign political party, a candidate for a foreign political office, or any person when it is known that all or a portion of such money or gift will be offered or given to a foreign official, political party, or candidate, for purposes of influencing such individuals in order for SCIS to obtain or retain any business, or direct any business to another person. Any such payments of money or gifts to a foreign official, political party, or candidate must have prior review by the SCIS Ethics Officer, even if such payment is common in that country. Keep in mind that foreign officials, under the FCPA, can include executives and employees of government-owned corporations, universities, and other entities. Always ascertain the government ownership/involvement of any transaction. In countries where local customs call for giving gifts to clients or others on special occasions, they may, with prior approval from management and the SCIS Ethics Officer, present gifts that are lawful, appropriate, and of nominal value, provided the action cannot be seen as seeking special favor.

4.9 Hiring

Certain legal or ethical restrictions may exist with respect to the hiring by SCIS of current or former employees of the government or their family members. Employees should consult with SCIS management and the SCIS Ethics Officer before any attempt, even preliminary discussion, is made to hire any such person.

4.10 Accounting Records and Controls

Certain legal requirements in effect within the United States require that the Company maintain accurate records and accounts that fairly reflect the Company's transactions. The Company is required to maintain a system of internal accounting controls to ensure:

- Transactions are executed and access to Company assets is permitted only in accordance with the appropriate management authorization, consistent with policy.
- Company transactions are recorded to maintain accountability for its assets and financial statements are prepared in accordance with generally accepted accounting principles.

SCIS employees must fulfill their responsibilities to ensure that the Company's records and accounts are accurate and that they are supported by the appropriate documents. All vouchers, bills, invoices, and other business records must be prepared with care and complete candor.

False or misleading documents, accounting entries, bank accounts, funds, or other assets which are not properly recorded in the Company's books will not be permitted. No payment shall be made with the intent or understanding that such payment, or any part thereof, is to be used for purposes other than those described in the documents supporting the payment.

SCIS requires that if employees are in a position which requires the use of Company funds or if they incur personal expenses which are reimbursed by the Company, that good judgment will be exercised on the Company's behalf. Employees shall spend Company monies for business purposes and never for personal benefit. Expenses must always be driven by business necessity and be consistent with Company policy.

4.11 Government Security Information

SCIS is committed to safeguarding the security of government classified information to which it has access. SCIS maintains policies and procedures to safeguard classified information in the possession of SCIS and ensures that SCIS complies with the Proxy Agreement, the International Traffic in Arms Regulation (ITAR), Export Administration Regulation (EAR), and the National Industrial Security Program Operating Manual (NISPOM). The facilities in which we operate have established security procedures with which SCIS will also comply.

4.12 In the Marketplace

Accurate Invoicing and Payments: Invoices submitted for payment must accurately reflect the true prices of products sold or services rendered as well as the terms of sale. Payments due must be made to SCIS customers, representatives, consultants, and suppliers in accordance with contract stipulations unless otherwise approved by an SCIS manager. Practices and procedures that might

facilitate wrongdoing, bribery and kickbacks, as well as any illegal or improper payments or receipts, are strictly forbidden.

Statements in Sales, Advertising and Publicity: Company promotional materials must be truthful. A monetary advantage gained through misrepresentation or exaggeration can jeopardize SCIS's future success. This applies equally to our discussions with others.

Competition: It is unlawful in the United States and elsewhere to collaborate with competitors or their representatives for the purpose of establishing or maintaining prices at a particular level.

It is SCIS's policy not to discuss client service rates with competitors at any time. Employees must never reveal information that might affect client service rates to any individual outside SCIS's employ. Within SCIS, such information must be limited to those with a "need to know."

It is also unethical and unlawful to collaborate with competitors or clients or their representatives to restrain competition in any form or fashion.

Estimates Must Be Reasonable: Those individuals who supply estimates to government procurement personnel, taxing authorities, audit agencies, customers, and suppliers must have a reasonable basis for such estimates. For the purposes of this policy, "reasonable" means based upon known facts in instances where facts exist or, in the absence of facts, upon the estimator's plausible and honest judgment.

Reciprocal Dealing: It is SCIS's policy to sell its services by virtue of superior client service. Collusion, expressed or implied, is unacceptable and inconsistent with SCIS's corporate values.

5.0 Compliance Requirements

SCIS has made a commitment to prevent and detect criminal and/or unethical conduct within the organization. The following procedures have been established to maintain that goal.

Awareness Programs: As part of each new employee's initial hiring process, the SCIS Code of Business Ethics and Conduct will be reviewed and discussed in detail, including the internal control procedures.

Annually SCIS will provide mandatory refresher training to every employee on the Code of Business Ethics and Conduct in order to remind employees of the content of the codes and the importance of complying with the codes.

Internal Controls

The Vice President of Governance and Compliance will serve as the Ethics' Officer of the Company. Questions regarding the legality of any transaction or conduct should be directed to ethics@scisusa.com.

> ***Additional Reporting Requirements:*** SCIS requires all employees to be diligent in accomplishing our goal to prevent and detect criminal and/or unethical conduct and promptly report all such offenses to an immediate supervisor or the SCIS Ethics Officer at ethics@scisusa.com.

If the above reporting provisions are not appropriate, all employees have access to the SCIS Hotline confidential reporting system. The Hotline permits employees to advise the SCIS Ethics Officer in a simple, anonymous, and confidential manner of unethical conduct. The Hotline can be contacted 24 hours a day by dialing 1-800-574-8637 or on-line at www.scishotline.com.

The SCIS Ethics Officer will report immediately to the SCIS Chief Executive Officer (CEO) any violations to the SCIS Code of Business and Conduct. If the violation involves the SCIS CEO, the SCIS Ethics Officer will report the incident to the SCIS Chairman of the Board of Directors.

Employees are encouraged to report all questionable issues without fear of retaliation and with the knowledge that all calls or web reports can be submitted anonymously. It is against SCIS policy for supervisors and upper-level management to retaliate against employees for reporting potentially unethical behavior. Employees should contact the SCIS Ethics Officer or use the Hotline to report any such retaliation.

Disciplinary Action: SCIS has a zero tolerance policy for violations of the policies in the SCIS Code of Business Ethics and Conduct and any known violations of federal or state law or regulation or special requirements of a government contract. If a violation of this policy occurs, progressive discipline could be imposed pursuant to SCIS policy. Any questions regarding unique situations will be forward to the SCIS Vice President of Human Resources.

Failure to report known unethical conduct is grounds for disciplinary action as well, which may include termination.

Internal Audit Process: SCIS has established a series of internal audit processes to periodically ensure that the company and all employees are in compliance with the policy. As part of the Operations Audit and National Accounts Site Audit Programs, compliance will be monitored and reported to SCIS management.

Policy Review: The SCIS standing committee on policy review will conduct an annual review of SCIS's procedures, policies, and internal control to ensure Company compliance with the Code of Business Ethics and Conduct. The SCIS Ethics Officers will report the findings of that review to the Board of Directors during their annual meeting.

6.0 Dealing with the Government

From time to time, SCIS contracts with government entities or is a subcontractor to a prime contractor that contracts with a government entity. While integrity is the foundation for all dealings with clients, special rules apply when the government is a client. Violations can result in criminal and civil penalties as well as exclusions from bidding on future government contracts.[1]

[1] Under the Federal Acquisition Regulation, Contract means:

[A] mutually binding legal relationship obligating the seller to furnish the supplies or services (including construction) and the buyer to pay for them. It includes all types of commitments that obligate the Government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing. In addition to bilateral instruments, contracts include (but are not limited to) awards and notices of awards; job orders or task letters issued under basic ordering agreements; letter contracts; orders, such as purchase orders, under which the contract becomes effective by written acceptance or performance; and bilateral contract modifications. Contracts do not include grants and cooperative agreements covered by 31 U.S.C. 6301, et seq. For discussion of various types of contracts, see part 16.

48 C.F.R. § 2.101.

Those involved in bidding on or providing services under a government contract need to know these rules:

- Never seek or accept confidential bid information or government sensitive information related to a competitor
- Never give or authorize the giving of any cash payment from SCIS funds to any government officials
- Never give or authorize the giving of payments in goods to any government officials
- Never offer or provide gifts, gratuities or entertainment to any government official without prior written approval by the SCIS Ethics Officer
- Know and follow anti-kickback rules, including restrictions on gifts by those seeking business from the government and from government contractors, including suppliers in the supply chain to such contract
- Conform strictly to the contract's terms and conditions
- Billings must always be accurate, complete, and in full compliance with all rules and regulations
- Labor hours and other costs, especially when performed under cost-reimbursable, time and materials, and labor-cost type contracts must always be accurate, complete, and in full compliance with all rules and regulations
- Be truthful, accurate, and complete in all invoices, representations and certifications
- Know your government client's specific rules and regulations
- Do not initiate any discussions about employment with any current or former government employee or agency with which you have had a business relationship without first contacting the SCIS Ethics Officer. This includes employment with SCIS or with a government agency

6.1 False Claims Act

The False Claims Act prohibits the knowing submission of false or fraudulent claims to the federal government to obtain payment from the federal government or to decrease an obligation owed by the federal government (e.g. intentionally misrepresenting hours worked on a timesheet). The False Claims Act also prohibits knowingly making false statements to the federal government to obtain a false or fraudulent claim paid by the federal government or to decrease an obligation owed by the federal government.

As a result, all SCIS employees must ensure that all statements made to government officials are accurate and to the best of your knowledge.

6.2 Mandatory Disclosure

The Federal Acquisition Regulation (FAR) mandates that SCIS timely disclose, in writing, to the agency Office of the Inspector General (OIG), with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of a Government contract or any subcontract thereunder, SCIS has credible evidence that a principal, employee, agent, or subcontractor of SCIS has committed either:

- A violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code; or
- A violation of the civil False Claims Act.

If the violation relates to an order against a Government-wide acquisition contract, a multi-agency contract, a multiple award schedule contract such as the Federal Supply Schedule, or any other procurement instrument intended for use by multiple agencies, SCIS must notify the OIG of the ordering agency, and the Inspector General of the agency responsible for the basic contract.

SCIS may be suspended and/or debarred for a knowing failure by a principal to timely disclose to the Government, in connection with the award, performance, or closeout of a Government contract performed by SCIS or a subcontract award thereunder, credible evidence of a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in title 18 of the United States Code or a violation of the civil False Claims Act. SCIS may also be suspended and/or debarred for a knowing failure by a principal to timely disclose to the Contracting Officer credible evidence of a significant overpayment, other than overpayments resulting from contract financing payments as defined in FAR 32.001.

If you have any questions relating to these requirements seek the guidance of the SCIS Ethics Officer. If you believe one of the various offenses detailed in this subsection have occurred, this Code of Conduct requires you to report the matter to the SCIS Ethics Officer and cooperate with any subsequent action taken. Failure to report such a matter to the SCIS Ethics Officer, or to cooperate in any subsequent action taken, may result in immediate termination of employment.

6.3 U.S. Anti-Kickback Act

The U.S. Anti-Kickback Act prohibits the payment of gratuities to an employee of a prime contractor or higher tier subcontractor of the U.S. Government for the purpose of improperly obtaining or rewarding favorable treatment in connection with a prime contract or a subcontract relating to a prime contract. To ensure compliance with this law, it is the Company's policy to prohibit the offering of such gratuities, except for logo or promotional items having an aggregate value of no more than $25 per person per year.

In the event that it is impractical to obtain advance approval of the receipt of a gratuity based on severe time constraints, or in the event that an employee receives a gratuity which is contrary to this policy from a source other than a vendor (e.g., a dignitary from another country) or under circumstances where the return or charitable disposition may be interpreted as an insult based on local custom, the gratuity may be accepted, provided, however, that the receipt of such gratuity must be disclosed, as soon as practicable, to the SCIS Ethics Officer and the recipient must comply with any instructions for disposition of the gratuity given to the recipient by the SCIS Ethics Officer.

6.4 Contract Charges

Only costs properly chargeable to a contract may be billed to or reimbursed by the U.S. government. Improper charging of costs may arise from various causes, including false or otherwise incorrect entries on timecards; false or otherwise incorrect subcontractor charges; false or otherwise incorrect classifications of costs as between direct and indirect categories; submission of false or otherwise incorrect expense accounts; or false or otherwise incorrect charges of time or materials to a work order or other cost account.

SCIS shall not knowingly claim reimbursement from the government for any cost or expenses that are unallowable. No employee shall submit or knowingly concur in the submission of false claims,

bids, proposal or documents. Employees shall properly record all time, costs and contract charges to appropriate accounts. Supervisory personnel shall ensure that all time charges of employees under their supervision are recorded promptly and accurately.

6.5 Cost and Pricing Submissions

In addition to the general requirement that data submissions to the United States government are not to be intentionally false or misleading, there are specific requirements relating to the submission, retention and disclosure of cost or pricing data in support of contract proposals and negotiations. All employees who are involved, directly or indirectly, in supporting a proposal must take adequate precautions to ensure that cost or pricing data are current, accurate and complete, properly disclosed and documented, and retained in appropriate files.

Intentional deviation from applicable specification requirements, including product or service substitution, can have consequences as serious as submission of false cost data. Such improper substitution includes such activities as the delivery of services -- except as authorized by waivers, deviations or other contractually permitted procedures -- that are not the same as called for by a specification, even though generally it may be thought that the substituted product or service is equal to or better than the one called for by the specification. No deviation is permissible without the required authorization.

6.6 Classified Government Information

It is important that all employees deal with U.S. government classified and proprietary material in the proper manner, both as a matter of national security and to assure compliance with applicable laws, regulations and U.S. government contractual requirements. Unauthorized access, dissemination, acceptance or handling of that material is prohibited and may constitute a violation of law.

6.7 Procurement Integrity

In order to safeguard the integrity of the government procurement process, all employees, consultants, agents, and representatives must respect the confidentiality of proprietary and competition-sensitive information, whether prepared by the Company, consultants, agents, representatives, or other companies or the U.S. government. Employees, consultants, agents, and representatives should not seek to obtain, solicit, or accept classified, confidential, proprietary, or competition-sensitive information prepared by or for the government or another company, or concerning a procurement or the procurement process, in a manner not permitted by law or regulation or the authorized government procurement process. Information subject to this provision includes, without limitation, trade secrets and other proprietary technical data, information concerning a competitor’s costs, prices or proposals, procurement plans, and technical or price evaluations concerning a particular procurement prepared by or for the procuring agency. Potential violations of this section should be reported to the Office of the General Counsel immediately so that prompt and appropriate action may be taken under applicable government regulations.

7.0 Code of Conduct

All officers, directors, and employees are required to comply with the SCIS Code of Conduct (Exhibit B). As stated in the Awareness Section of this policy, the Code of Conduct will be reviewed and discussed

in detail during each new employee's initial hiring process. Annually, SCIS will provide mandatory refresher training to every employee on the Code of Conduct in order to remind employees of the content and the importance of complying with the code.

8.0 Immediate Reporting Requirements

If asked to deviate from this policy, whether by a supervisor, another SCIS employee, or a client, all SCIS employees have a right and responsibility to clarify any ethical questions that may arise. This includes addressing the matter with the appropriate level of supervision until resolution is obtained and understood by all involved. The SCIS Ethics Officer will report any attempts to deviate from this policy immediately to the SCIS CEO.

6.6 Insider Trading and Confidential Information

Securitas abides by all applicable insider trading laws and regulations and does not use or disclose insider information inappropriately in connection with stock trading. Employees and business partners must not use any non-public information about Securitas or any other company to influence his/her, or any third party's, decision to trade in securities.

6.7 Privacy and Data Protection

Securitas respects the individual's right to privacy and is committed to handling personal data responsibly and in compliance with applicable privacy and data protection laws.

6.8 Confidentiality (Trade Secrets)

All employees and business partners are expected to exercise particular care to prevent any unauthorized use or disclosure of Securitas' confidential or proprietary information. Non-public information belonging to our customers or business partners to whom we gain access through our business must also be protected, in accordance with all legal and contractual requirements.

6.9 Intellectual Property

The entire value of our long history of providing professional security services is vested in the Securitas trademark. Securitas, as well as all employees and business partners, must work to safeguard this trademark and respect the valid intellectual property rights of others.

6.10 Protecting Company Property and Resources

Securitas' property, resources and information systems must be protected and kept secure at all times from unauthorized use, damage, disclosure, diversion or removal, whether through accident, improper act or breach of trust.

6.11 Government Work

Many of our customers are government agencies and public and international authorities and agencies. Securitas is strongly committed to abiding by all applicable laws and regulations relating to working with governments and public authorities, including certain special requirements associated

with government contracts and transactions.

6.12 Disclosures, Records and Internal Control

Securitas recognizes the importance of having an open communication with those that are affected by our operations, whether they are employees, business partners, customers, investors or the public and their representatives. The Securitas share is listed on the NASDAQ OMX Stockholm stock exchange and all information is provided in compliance with relevant laws, stock exchange rules and corporate governance codes applicable to our business. Comprehensive and accurate corporate information is available for interested parties and Securitas will respond in a timely manner to inquiries. All reporting and accounting documentation clearly identifies the true nature of business transactions, assets and liabilities in conformity with relevant regulatory, accounting and legal requirements and is given to the best of our knowledge. Our aim is full accountability. Securitas' accounting and reporting standards are set out in the Group Policies and Guidelines and in the Securitas Reporting Manual. We apply the Securitas Communication Policy in all our communications. Securitas' internal control policies are consistent with the COSO Internal Control Integrated Framework. The Securitas AB Board of Directors is ultimately responsible for the work performed in our internal control functions.

7. Environment and Sustainability

Securitas strives to conduct its business in an environmentally sustainable way and shall comply with or exceed environmental requirements set by applicable laws, regulations and international agreements. We are expected to continuously seek ways to reduce the consumption of resources, emissions and waste. Targets for emissions are set out in the Securitas Emissions Policy.

8. Community Involvement

Securitas acts as a good corporate citizen wherever it operates and supports local, regional and global communities in appropriate ways. We also participate in social projects in regions where we see a pressing need for the local community to be strengthened. Through our entities, we interact with the local communities where Securitas operates, implementing such initiatives as sponsoring schools, orphanages and organizations for the disabled. Securitas recognizes the importance of a proactive and continuous social dialogue with all our stakeholders.

9. Implementation and Compliance

It is the responsibility of each Securitas employee and Board Member to observe and promote the Code. The Divisional/Regional President is responsible for ensuring the implementation of the Code in his/her territory, however the ultimate responsibility for the proper implementation of the Code by all employees and business partners lies with the Country President within his/her respective territory. The Code shall also be communicated and implemented, to the greatest extent possible, in all business partner and employee contractual relationships. For the purposes of the Code, our customers are not regarded as business partners. Business partners may include suppliers, subcontractors and other partners. Implementation of and compliance with the Code will be monitored on an ongoing basis as part of our Enterprise Risk Management process. The Code shall be reviewed annually. The ultimate responsibility for this rests with the Securitas AB Board of Directors. It is also the responsibility of each Securitas employee and business partner to raise concerns about compliance with the Code. When

an employee or business partner wishes to make a complaint or report a violation of the Code, his/her manager or a representative of the local management should be informed. If the employee finds it difficult to bring up an issue locally, if a complaint is not resolved or where the allegation is of a serious or sensitive nature, it should be reported through one of the following channels:

13900 Lincoln Park Dr., Suite 370
Herndon, Virginia 20171
www.scisusa.com

Securitas