

Security Department File Database: Standard Operating Procedures



Accessing File...

Please Wait, Do Not Disconnect Monitor...



:|| **WARNING** ||:



LEVEL 4 AUTHORIZED

Security Department

STANDARD OPERATING PROCEDURES

File Accessed

THIS DOCUMENT IS CLASSIFIED

BY ORDER OF THE

**SECURITY
DEPARTMENT'S HIGH
COMMAND STAFF**

ACCESS IS STRICTLY FORBIDDEN

SECURITY PERSONNEL ONLY

UNAUTHORIZED READING OR SHARING OF THE CONTENT OF
THIS DOCUMENT WILL RESULT IN DEPARTMENTAL DEMOTION
AND A CLASS-E SENTENCE RELATIVE TO THE SEVERITY OF THE
VIOLATION OR LEAK

Section I - Introduction

Document classification status and privacy regulations

1. This information is classified, all individuals handling this information are required to protect it from unauthorized disclosure in order to represent the best interests of the security department.
 - 1.1. As stated on the cover page, this document is restricted to Security personnel only. This is with the exception of select personnel who may be given access by the Overseer or in the case the Overseer is indisposed, the Overwatch. Likely personnel to be given access are certain Level – 4 personnel and the Overwatch of other departments.
 - 1.2. Personnel who do not fall under that description whom request access are to consult the Overseer, who is the **only** Security Department member who may give access to personnel who are not described in part 1.1.
2. This document, the Standard Operating Procedures, which shall be henceforth be referred to as the “SOP” is the cornerstone guide to all procedures and protocols within the department. Any other document is deemed secondary, if any other document contradicts the contents of this document, then that secondary content is to be omitted or ignored. The only documents which override the SOP are the Code of Ethics, the Ethical Code of Conduct or content written by the O5 head or the Administrator. Personnel refusing to acknowledge or respect the contents of this document will be omitted from the Security Department and appropriately punished.
3. No document nor organization has the power to override the contents of this document with the exception of O5-7, the O5 Head, the Commissioner, the Administrator, the Code of Ethics and the Ethical Code of Conduct.
 - 3.1. Department administration, High command specifically, is responsible for the maintenance and any updates to this document should the Code of Ethics or Ethical Code of Conduct be amended or one of the listed above personnel request change.
4. The standing Overseer of the Security Department has the ultimate and final say in all matters regarding the Security Department. No rank may override the Overseer’s order with the exception of the O5 Head, the Commissioner or the Administrator.
5. In the unlikely situation that the standing Overseer becomes incapacitated or unable to make administrative decisions, the standing Overwatch personnel is to take complete control until the return or replacement of the Overseer. Should Overwatch become incapacitated alongside the Overseer, administration of the department is to be managed by high command. If O5 command defers temporary command of the department to other personnel or groups, then that is final

Section II – Rank Structure

All Security Department Personnel, regardless of rank, are subject to equipment regulations which dictate what equipment they may use on site. For more information see the Equipment Regulations table in Sub-Section 13.

Enlisted

The **Enlisted** personnel are the primary force within the Security Department and are tasked with the basic duties of the Security Department. They have a level of authority over other Foundation Personnel, but **not** over each other.

Security Trainee - Fresh out of the academy, Security Trainees are new members of the Security Department and show a basic understanding of what is expected of them as members of the Security Department. Security Trainees are expected to maintain a high level of professionalism and abide by the code of conduct and security guidelines stringently.

Security Sentinel - Security sentinels are the main brunt of the Security department. They are members of the onsite security who show an in-depth understanding of their duties as security personnel and have proven the requirements Security Sentinels may rank up further to Senior Sentinel by first meeting the requirements and then proving competence to your commanding officers. Security Sentinels may also join specialised divisions if offered by the division's commanding officer.

Senior Sentinel - Senior Sentinels are the senior-most members of the Security departments Enlisted personnel. Senior Sentinels are equipped with comprehensive knowledge of what is expected of them and know how to utilise this knowledge to perform their duties onsite effectively and professionally. Senior Sentinels are expected to act as exemplary members of the department, acting as a role model and providing valuable guidance and insight to lower-ranking personnel and maintaining a good image for the department.

Specialist - Specialists are Security Personnel who are handpicked by division commanding officers because they have not only proven themselves to possess an exceptional understanding of their duties as Security Personnel but also have a high degree of skill with firearms, a strong sense of intuition, be adaptable, and maintain an exemplary standard of professionalism and maturity onsite. Specialists may be selected from any personnel that is of the Security Sentinel rank or higher, at which point they will be jumped to the specialist position. Note that this does not signify any increase in power or command, but is recognised as a position of respect, and should be treated as such by your peers.

Junior officer - Junior officers are security personnel who have demonstrated to the Security Department's Central Operations that they possess basic leadership and administrative skills. Personnel with this rank are officers in training and are consequently still classified as Enlisted personnel, with potential to either rise to an officer position or return to their previous post. Only Senior Sentinels and Specialists may be considered for this rank. Personnel may be given this rank if they receive recommendations from two or more standing officers. They will advance to Security Sergeant only after being reviewed and interviewed by high command.

Central Operations

The Security Department's **Central Operations** handles all instructor duties of the Security Department. Their primary task is to complete the more menial tasks such as activity logging and are responsible with training other personnel. Members of Central Operations also handle the Enlisted ranks and are the most commonly seen of the Security Department's Officer Corps. These personnel have authority over the Enlisted Operations and may co-ordinate and command Enlisted personnel onsite as well as receiving more equipment.

Security Sergeant - Security Sergeants are Security Personnel who have a comprehensive knowledge of their duties as security personnel and have proven to the department's high command that they possess qualities that make them fit for positions of responsibility and leadership. Sergeants are granted authority over lower-ranking personnel and have more equipment in their arsenal. They are expected to lead their subordinates onsite regularly and will be assigned responsibilities and duties by the First Sergeant that they must complete. As officers, they will also be granted one recommendation every two weeks that they may use to recommend non-officer personnel for a junior officer position.

First Sergeant - The First Sergeant rank is awarded to the Security Sergeant who has proven to High Command that they are skilled leaders and are especially competent with administrative duties. The First Sergeant is assigned with the task of managing the Sergeants activities and ensuring that they are completing their assignments on time and to a high degree of quality - note that these "assignments" include things such as activity logging, disciplinary logging, and disciplinary meetings. They have authority over all ranks below them. The First Sergeant communicates directly with High Command whom will assign tasks to the First Sergeant whom they distribute them among the Sergeants for them to complete within a certain timeframe. This position is restricted to a maximum of two officers, ideally only having one, but to account for departmental growth a second may be added.

Security Lieutenant - Security Lieutenants are officers who have repeatedly displayed a high degree of skill in all areas of their work and have subsequently been chosen by high command from the existing pool of officers to become senior members of the departments Central Operations. Security Lieutenants work directly under and with Security captains in the management of divisions. There are 3 Security Lieutenant positions, two of which are tasked with co-leading their assigned divisions and the remaining one being tasked with more general management of the department as a whole and co-managing the I&P academy. As expected, Lieutenants have a larger arsenal of equipment available and have authority over all ranks below them.

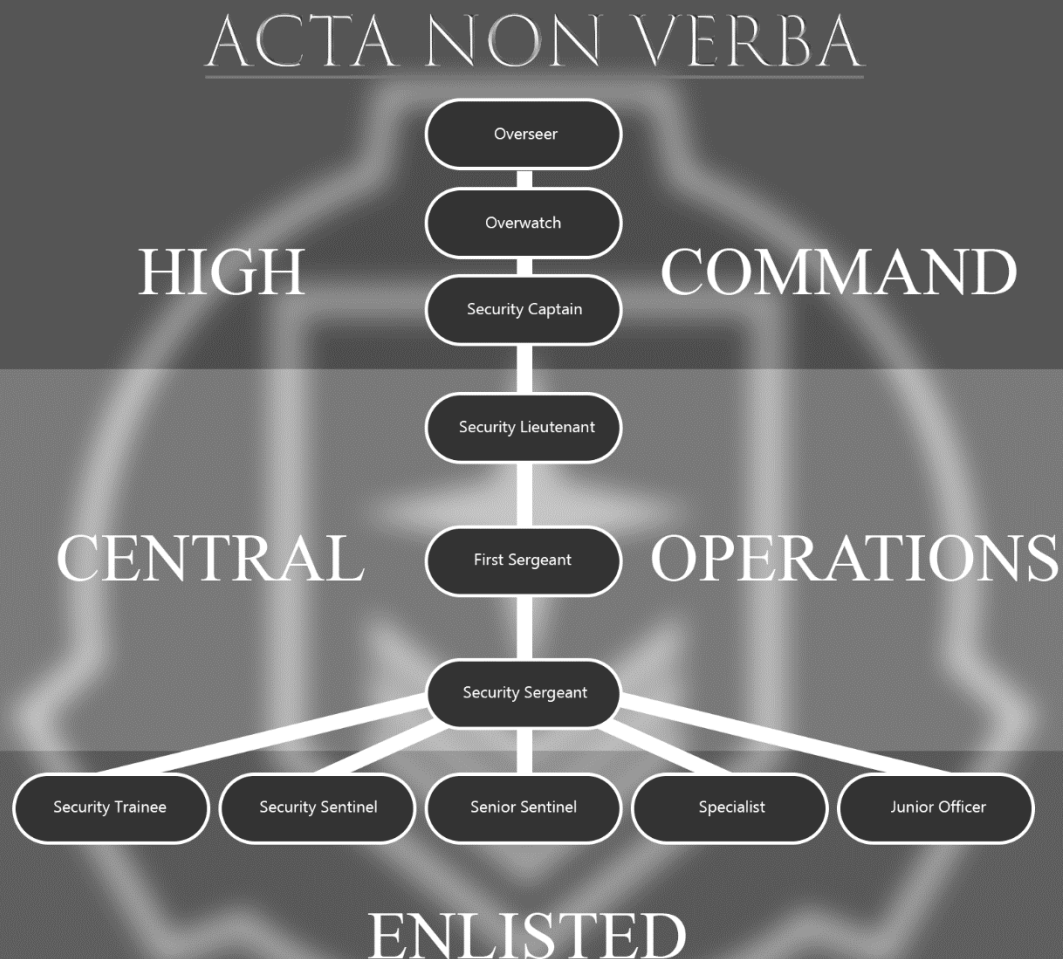
High Command

The Security Department **High Command** is tasked with handling all administrative matters of the department. This of course includes handling promotions and other such changes. These personnel have authority over both Enlisted and Central Operations.

Security Captain - Security Captains, handpicked by Overwatch and the Overseer, and have proven to be excellent leaders and masterful administrative staff. Alongside Overwatch and the Overseer, they are tasked with the day to day running of the department, taking suggestions from the rest of the department, co-ordinating trainings, events and ensuring that High Command is maintaining an active presence on site. At any time, there are only **three** available Security Captain positions. Two of these Security captains lead and manage specialised divisions while the remaining will manage and spearhead the I&P academy's training of new personnel. Each of these Security captains will have access to a vast arsenal of equipment, knowledge and experience which they may use. These Security Captains will also directly work with an assigned Security Lieutenant who will help co-lead and manage their assigned divisions.

Overwatch – Overwatch is the Security Department's hammer; they provide departmental oversight, regulate workflow and manage the maintenance of the department's documentation and resources. They receive ideas and commands from O5 command and enact them into reality, passing these changes through the chain of command to distribute the workload and ensuring they are completed to the Overseer's expectations. All the while providing regular updates and reports to the Overseer and maintaining the department's wellbeing and reputation.

Overseer – If Overwatch is the hammer, then the Overseer is the carpenter swinging the hammer. In charge of all Security Department affairs. The Overseer is a member of the O5 council, given the task to manage and administer the Security Department as a whole, as well as dealing with Foundation wide affairs relevant to its Security.



Section III – Operational Procedures

Sub-Section 1 - Departmental Rules

1. Members within the Security Department are to prioritize personnel safety, site security, and actively work to counter and mitigate hostile threats.
2. Any members of the department found aiding hostile groups of interest will be subject to immediate Foundation-wide punishment and blacklisting from the Security Department.
3. Members of the department are prohibited from engaging freely in conversations without proper precedent to do so. Instances that count as proper precedent but are not limited to include:
 - a) Warning foundation personnel of potential or defined threats.
 - b) Alerting foundation personnel of potential or occurring breach events.
 - c) Directing Class-D personnel where necessary.
 - d) Department orientated communication in various events such as riots.
5. Radio usage must be done in accordance with **Sub-Section 12 - Radio Operations**.
6. Recontainment is never to be conducted by Security personnel without O5 approval.
7. Security Officers must maintain professionalism, maturity, and grammar always. Clear communication must be adhered to and duties must be conducted appropriately with all parties in mind as well as the directive at hand.
8. Safety and security of foundation personnel is the priority of the department. This can be achieved through vigilance and remaining in a constant state of awareness. Instances where this rule is void:
 - a) Personnel that are disobeying the code of ethics or infecting themselves with SCPs may be fired upon after they've received a warning, or with the permission of a supervisor.
 - b) Uncooperative or disobedient Class-Ds may be terminated after 2-3 warnings.
9. All Security personnel must complete 3.5 hours of activity per week, this must be logged within the respective discord channel. Failure to do so must be explained accordingly.

Sub-Section 2 – Oath of Silence

Members of the onsite Security force are bound by an Oath to remain silent. However, this Oath may be disregarded if certain conditions are met, these conditions are as follows:

1. The Security Personnel must speak in order to relay to the non-combatative that there is potential for danger, or they are actively in danger, and that the non-combatant must vacate the premises immediately in order to mitigate this danger.
2. The Security Personnel must communicate with fellow combatants in regards to combat situations or the potential for such situations, this is inclusive of course to combatants discussing changing battleplans, threats, problems and solutions within a firefight.
3. The Security Personnel must speak in order to direct Class-D personnel, for example directing them into a briefing chamber or to back onto a wall, general commands and orders relevant to their current situation.
4. Necessary interdepartmental requests, for example, Medical treatment which should be ideally communicated with a “+” to indicate you need healing, or requests for engineers for CDC repairs, etc.
5. Security Personnel may also speak if given permission by a member of the Department’s High command, or a member of the O5 council. **High ranking personnel of other departments are not applicable to this rule and do not have the authority to grant the free ability to speak.**

Note: Security Personnel may speak freely amongst themselves in whisper or team chat, with the assumption and requirement that any conversation does not adversely affect their ability to operate or is noticeable to people outside of the security force.

Sub-Section 3 – Termination guidelines

As a member of the onsite security force, you are expected to manage and eliminate possible threats. The threats that the Security Department will face are generally human, inhuman threats are to be exclusively left to the MTF’s expertise. As our threats are generally human, the Code of ethics applies to them and to every action they take, and every action you take against them. But during active duty it is guaranteed that Security personnel will be required to fire upon hostile threats, therefore this sub-section will be dedicated to the regulations and grounds for ethical termination of hostile personnel.

- 1) Security Personnel are to immediately terminate **ALL** members of hostile groups and personnel seen to be aiding them, such as The Serpents hand, or the chaos insurgency. Security personnel are to do so in all situations with the exception for it being their termination being disallowed by a member of the O5 Council.
- 2) Security personnel are to terminate Class-D personnel who do any of the following:
 - a) Cross the termination line.
 - b) Interfere with Security operations of any type.
 - c) Possess any form of contraband that has the potential to cause damage or harm to foundation personnel or assets.
 - d) Purposefully avoid punishment.
 - e) Cause any Class-D to cross the termination line or break any of these rules.
 - f) Vertically stack on top of other Class-D.

- g) Repeatedly ignore or act against Security Personnel's instructions or operations.
- h) Class-D whom make real life threats to your physical safety in a **serious** manner, this should also be reported to your commanding officer.
- i) Aid or abet other Class-D personnel who break these rules.

Note: Security Personnel cannot “revenge kill”, this being the act of being killed by a Class-D and returning to the CDC and terminating them, Security personnel must terminate the Class-D in the same life that they witnessed the possession of the harmful contraband.

Sub-Section 3B – Foundation Personnel Termination guidelines

- 1) Security personnel are to only terminate foundation personnel in the most extreme scenarios, the conditions that must be met for their termination are as follows:
 - a) Personnel in question repeatedly refuse to co-operate with Security personnel.
 - b) Personnel in question are actively and purposefully interfering and disrupting inter-departmental actions, i.e. preventing an engineer from making a repair, repeatedly interfering with a test.
 - c) Personnel have been given three verbal warnings and then a warning non-lethal shot.
 - d) Personnel have seriously breached the Code of Ethics.
 - e) Personnel are armed.
 - f) Personnel break the game's ToS or create/wear graphic or incredibly offensive content.

Note: All or most of these conditions must be met for the termination to be ethical and it is recommended that if you are in this situation, you immediately start recording as this will aid your case in the event it is taken to the ethics committee.

Sub-Section 4 - Solitary Confinement

While on active duty within the CDC, Security personnel will most likely interact with in-cooperative or hostile Class-D, in these interactions the Class-D's actions generally result in their termination. To prevent repeated action, they are to be given punishment in the form of Solitary Confinement given that the following conditions are met:

- 1) The Class-D has done anything that has warranted his or her termination at least 3 times.
- 2) The Class-D has repeatedly harassed or acted with malicious emotional intent against Security personnel with the purpose of provoking an emotional response.
- 3) The Class-D has provoked **other** Class-D to act against the foundation, either by exciting them, rallying them or by other means.
- 4) The Class-D has intent of causing harm or damage to foundation assets and/or personnel.
- 5) The Class-D is conspiring against the foundation.

Note: The duration of the Solitary Confinement is entirely up to the Security personnel carrying out the punishment, although it is expected that it be no longer than 5 minutes for first offenders, while 10 minutes+ may be warranted for repeat offenders. Extreme durations, periods longer than 20 minutes, are to only be permitted by a member of the departments High Command or the O5 council.

Sub-Section 5 – Watchtower regulations

1. Within the CDC there is a Guard Tower, the interior of this Guard Tower is armed with an M40 Sniper rifle and lockdown controls for the CDC, the regulations for this guard tower are as follows:
 - 1.1. Security personnel may only position themselves on the tower if they are of the rank “Sentinel” or higher, or otherwise have permission from a member of Central Operations.
 - 1.2. Security personnel may only position themselves on the tower if there at least 3 other Security personnel guarding the ground floor.
 - 1.3. The only personnel permitted to use the M40 Sniper rifle are Senior Sentinels+ or a member of a Mobile Task Force. This rifle is **NOT** to be used outside of the CDC.
 - 1.4. There is always a maximum of 2 Security personnel on the guard tower, if an officer enters the guard tower, they are exempt and the other 2 personnel may remain.
 - 1.5. The lockdown control buttons in the interior may **only** be used by members of the Central operations permission from officers may also be given. The controls may also be used post-riot if the CD population is particularly high and a high risk is present.

Sub-Section 6 – Class-D Mealtime procedures.

These steps are to be carried out during the “Class-D Meal-time” schedule.

Note: The Class-D Mealtime should only be held if the Class-D personnel are behaving well and there are enough Security Personnel to manage both the escort and the CDC. Generally a minimum of three guards are needed to escort the Class-D’s to the cafeteria, although the ideal ratio of Security Personnel to Class-D’s is 1:4

1. Upon the beginning of the schedule, Security personnel are to request that other foundation personnel beginning food. If this is not possible then two select Class-Ds, preferably ones that have shown to behave are to be escorted into the canteen by two Security personnel. They are to prepare food for the other Class-Ds.
2. Upon completion of this task, they are to be seated as per normal and must be guarded by one of the guards while the other returns to assist with escorting the main convoy.
3. The rest of the Class-Ds must be lined up inside of a briefing room, and once sufficient Security personnel are present and ready to escort, the door must be opened so that all Class-Ds may be escorted to engage in meal-time.
4. One Security personnel must remain by the CDC guard area as to prevent newly joining Class-Ds from passing the yellow line and breaking termination guidelines.
5. Upon completion of meal-time all Class-Ds are to be escorted back into the CDC and the canteen must be cleared of strays and swept for hiding Class-D personnel.

Sub-Section 6B – Class-D Mealtime briefing

Security Personnel should start by announcing to the Class-D personnel that they are to be given meal-time, then proceed to order them into a TSTA of your choice. Security Personnel are to then order the Class-D personnel to stand on or behind the line with their backs to the wall, Personnel are then to brief the Class-D personnel on what the mealtime involved and what behaviour is expected of them, A standard mealtime brief is generally outlined in the academy and should be known by all Security personnel, however for guidance on the ideal brief refer to the following:

Listen up Class-Ds,

You are now being escorted to the cafeteria for meal-time.

You are to follow all direct orders from combative personnel, failure to do so may result you being excluded from meal-time.

Once you are being escorted to the cafeteria, do not stray from the escort party. Doing so will result in termination.

Inside the cafeteria, you are authorised to speak freely. Be warned, this is a privilege and can be revoked

Am I understood?

Sub-Section 7 - Test procedures

1. This procedure must be carried out during the ‘Testing Time’ schedule.
 - 1.1. There must be enough Security Department personnel on-site to be able to fulfil test requirements while leaving a sufficient number of Security Personnel to safeguard the CDC.
 - 1.2. Class-D personnel need to be properly briefed before departure. See **Below** for further detail.
 - 1.3. Once briefed, have the Class-D personnel file behind the ScD or MD who issued the request and depart to the destination.

Sub-Section 7B - Test briefing

1. In the event Scientific personnel request Combatives and/or Class-D personnel for a test, Security personnel are to first select Class-D’s, preferably well-behaved ones, and then move them into the TSTA chamber specified by the Scientific Personnel.
2. The Class-Ds must then be lined up behind the yellow line with their backs to the wall and a brief must be delivered.
3. A standard testing brief is generally outlined in the academy and should be known by all Security personnel, however for guidance on the ideal brief refer to the following:

Listen carefully, I will only say this once.

You have been selected for a test, throughout this test you are to obey the following rules or face termination.

Permission to speak is now in effect, speaking without permission may result in a warning.

You will receive three warnings, two from Foundation Personnel and one from combatants.

Exceeding more than three warnings will result in termination.

Disobedience and disrespect is not tolerated, disobeying direct orders may result in a warning.

You will not attempt to flee from escort, breach any SCPs or harm any Foundation Personnel.

Am I understood?

Upon conclusion of the brief, step back and allow the Scientific Personnel to speak to the Class-D personnel, once they have finished, order them to form a Column (SFL) behind the Scientific Personnel and let them take charge.

Sub-Section 8 – Breach Procedures

In the inevitable scenario where a breach occurs, available Security Personnel must perform the following steps in order and must do so with absolute efficiency:

1. Switch to TACTICAL radio comms and alert your fellow combatives to do so as well. A key advantage in any breach or hostile scenario is always having up-to-date information, as this can allow individuals to make rational decisions as the situation unfolds.
2. Dispatch a number of Security personnel that is appropriate to the severity of the breach and the danger the specific breach represents.
3. Ensure that sufficient Security Personnel remain in the CDC to ensure its safety, in extreme scenarios and with officer or MTF permission, you may use the control panel to lockdown the CDC to divert the entirety of the onsite security to the breach.
4. Alert MTF via Discord if they are not already online, do not ping the entire role, instead ping individual operatives that have online statuses.
5. In a breach, Security Personnel's **primary and sole** role is to **quarantine the affected area and evacuate non-combative personnel from the area**, Security personnel are to alert the public on the General radio comms that the affected area is quarantined and therefore closed off to public entrance.
6. Security Personnel are to stand guard at the entrances and exits to the affected area, ensuring that no unauthorized personnel enter the area.
7. If the severity of the breach warrants it, the breach alarm is to be activated by a Level-4 and non-combatives are to enter the breach shelter, priority is placed on the evacuation of high-ranking personnel first.

8. Stand guard and maintain the quarantine until MTF units give the all clear, then you may return to regular operations.

Sub-Section 8B – Emergency Recontainment

In the event MTF are not responding or are otherwise unavailable to recontain the breached SCP, Security Personnel may perform an emergency recontainment. This is where, as you'd expect, Security personnel recontain the SCP in place of the MTF Personnel. This procedure is only to be done under the most extreme breach scenarios, where it must be done to prevent a greater loss of foundation assets and personnel. It is to be done only when MTF have been alerted, but have not responded for 20+ minutes, or if the SCP is in a highly populated area, 10+ minutes. This is with the exception of course of O5 approval, at which point recontainment can be carried out regardless of timeframe or situation.

Note: If the breached SCP is in a highly populated area, for example 173 is in the CDC, if there are no immediately available MTF to recontain it, direct it to a side area, for example a TSTA chamber, where it can wait until MTF has arrived or the conditions listed above for an emergency recontainment have been met.

Sub-Section 9 – Leaving the facility

Security personnel may only leave the facility if they have express permission from either a member of the Security Department's High Command, or a member of the O5 council. **For more information on the High Command, see the ranking table in Sub-Section I.**

Sub-Section 10 – Checkpoint regulations

The Security Enforcement Regiment is a handpicked, elite division of the Security Department. The Security Enforcement Regiment handles all internal affairs regarding the Security Department, which includes investigating Departmental & Code of Conduct violations. The Security Enforcement Regiment is primarily stationed at the Sector - 2A Checkpoint Zone, where personnel are scanned to ensure no illegal contraband is brought into Sector – 2. For reasons relating to the operational security relating to the SER sub-division, it's guidelines are restricted to members only.

Sub-Section 11 – Addressing officers

Security personnel must refer to each other as described in the table below, the only exception to this rule is when Security personnel are in high intensity situations such as a firefight, where typing out formal ranks could prove detrimental to Security Personnel's ability to fight and defend their position, in this scenario or one similar, Security personnel may simply refer all of their superiors as "Sir" or "Ma'am".

Trainee - Junior Officer	Referred to by	Their rank
Sergeant - Captain	Referred to as	Sir or Ma'am
Overwatch	Referred to as	Overwatch, Sir or Ma'am
Overseer	Referred to as	Councilman or Councilwoman

Sub-Section 12 – Radio operations

1. The radio is not to be used for irrelevant purposes irrelevant to your duties. Security operations are classified to those within combative departments. All radio traffic should be checked with a supervisor before communication with others.
2. The radio can be activated with **P**. Team chat with **/team** before speaking is to be utilized when in-game to prevent leakage of radio chatter to Class-Ds or other Foundation Personnel.
3. During raids, riots or when commanded to do so you are to utilize the **tactical radio** which is also to prevent radio clutter and leakage of classified information. When switching, alert other personnel that you are on the tactical radio through stating “[**RANK**], **Check.**”
4. Remain vigilant before rapidly sending radio messages, maturity and grammar are required at all times. If you do forward a message onto the radio accidentally, follow it with “**Hotmic.**”
5. Remember that when sending a message, everyone onsite can view it, this influences other’s view of the department and personnel who are found to intentionally misuse the radio will be punished harshly and appropriately.
6. All Security Department personnel are to when logging on, message on the radio with “**Security [RANK], signing on.**” Similarly, when signing off, message on the radio with “**Security [RANK], signing off.**” If you fail to do this because of unknown parameters such as crashing, let the department know through #general in the discord.
7. Tests and other events that request Security personnel must be responded to over the radio with “**Copy.**” or “**Denied, [REASON].**” You may not leave a request unacknowledged. This is to let other Security personnel that you are carrying out the request, or letting the requestor know that it cannot be fulfilled.

Sub-Section 13 – Equipment regulations

Security personnel have access to a large arsenal of equipment and weapons, although each item is subject to strict weapon regulations, limiting their uses to specific ranks or members of certain divisions within the department. Every independent weapon regulation may be overridden by members of the Security Department’s Central Operations, this is for certain

scenarios that require large-scale access to certain weaponry. Below you will find the table that illustrates every weapon and their regulations.

UMP~45	Trainee +
AUG A1	Sentinel +
M40 Sniper Rifle	Senior Sentinel +
M4 Carbine	Security Sergeant +
Scanner	Security Sergeant +
Handcuffs	Security Sergeant +
IFAK Pouch	Security Lieutenant +

Sub-Section 14 – Weapon Conditions

There are three stances that Security personnel may stand in, dictated by the use of their firearm, members of the department's Central Operations may order lower ranking personnel into any of these conditions at any given time. They are as follows.

Condition Alpha – Holstered and unequipped.

Condition Bravo – Equipped but not ready to fire.

Condition Charlie – Presented and ready to engage with the sights aimed in.

Sub-Section 15 – Warnings and punishments

1. Punishments are distributed within the Security Department Discord server via roles. Upon being found guilty of committing an offense, the offender will receive a warning.
 - 1.1. A warning is represented as the '1W' role in the discord.
 - 1.2. Strikes are represented as the '1X' and '2X' roles in the discord.
 - 1.3. One warning is represented as the '1W' role in the discord.
 - 1.4. Two warnings are represented as '1X'.
 - 1.5. Three warnings are represented as '1X' and '1W'.
 - 1.6. Four warnings are represented as '2X'.
 - 1.7. Five warnings are represented as '2X' and '1W'.

Six warnings will immediately remove the offender from the Security Department. There is no '3X' role in the discord.

Qualification for a warning or a strike are actions considered by Central Operations and High Command to be negligent, inappropriate or improper. Such actions include but are not limited to: **Failing to complete the activity quota, repeatedly ignoring an officer's warnings or orders, breaking CoE, acting against the interests of the department, going against departmental guidelines, negligence, misconduct and any other action an officer considers to be egregious.**

Alleged misconduct will be reported to High Command via a form the officers may fill out and send to High Command, whom will then review it and debate the circumstances, validity and decide a punishment.

Sub-Section 16 – Riot Control and Riot Certification Tier List.

Tier 1 - Newly qualified Security Officer, can use the Riot Control Unit uniform and the Sock gun, but cannot use the M32 Grenade Launcher.

Tier 2 - Fully qualified Security Officer, may use the M32 Grenade Launcher only when RCU Instructor+ grant authorization.

Tier 3 - Has acquired advanced qualification, may use the M32 Grenade Launcher without Instructor+ authorization.

Instructor - Instructing Officer for RCU, may issue qualifications to other Security Department personnel (Can only be obtained by Security Sergeants and above).

Director - Commanding Officer for RCU, implements new regulations and works alongside the Security Department High Command (May only be obtained by Lieutenant and above).

Equipment Listing:

Sock gun – Used to incapacitate individual Class-D personnel.

M32 Grenade Launcher - Used to disperse CDs from a clustered area.

Handcuffs	Tier 1+ Personnel
M32 Grenade Launcher	Tier 3+ Certified personnel

Sub-Section 17 – Patrolling the facility

Given the incredibly tedious and repetitive nature of your role within the Security Personnel, preventative measures must be taken to prevent you from dying of boredom standing at constant attention within the CDC. Security personnel may patrol the facility or stand guard at high traffic areas (not the checkpoint) as a means of relief to the high stress of the CDC. This is of course assuming that the CDC is secure and there is enough of a surplus of personnel to both fulfil their interdepartmental duties such as escorting tests and other requests. Independent responsibility is expected of you in this regard, you may perform rotations as you see fit among you, and if the need arises, you must return to your post within the CDC, which is your first priority. This subsection is of the least importance within this document, should any other subsection contradict the content within this subsection, it is to be assumed that the other one is the correct one.

**Authored and illustrated by the standing Overseer of the Security
Department as of 12/05/20**

iiiAnzac

