UNRESTRICTED

Explanations on
Key Issues Regarding the Implementation
of
The Standard Protocol of Sector 3 Checkpoint

Site-Virtus
Administrative Department

1. General Provisions

In order to standardize the operation of the Sector 3 Checkpoint, the administrative department has issued the Standard Protocol of Sector 3 Checkpoint, aiming to ensure the checkpoint functions properly. However, recent implementation practices have revealed that some personnel have insufficient understanding of the regulations, certain provisions are subject to dispute, and there is a lack of effective coverage for some individuals. Consequently, this document has been drafted to provide supplementary clarification.

2.Explanations

2.1 Explanations for Section 2

2.1.1 Regarding Section 2.1.1:

Personnel submitting entry applications must do so via the radio communication system. The application shall include the following contents:

- Codename
- Purpose of Entry
- Current Location
- Estimated Duration

Patrol requests must be submitted at least 5 minutes in advance

Emergency tasks (e.g., containment breach response) may be submitted in real-time but require authorization from the Site Director.

Examples:

A researcher planning to test SCP-049 in Sector 3 send the entry applications via radio, includes:

1. Codename: ██
2. Purpose of Entry: Test on SCP-049
3. Current Location: CDC(Central D-class Cell)
4. Estimated Duration of test: 10mins

Which should be send in radio like this:

"Codename:██. Test on SCP-049. Current At CDC. Estimated Test Duration: 10mins."

Failed to Following this will result in a Denied entry request.

2.1.2 Regarding Section 2.2.1:

Access to Sector 3 (S3):
    The keycard is a mandatory credential for entry. Personnel may enter under the following circumstances only after contacting their department supervisor through radio for identity verification:
- Damaged keycards
- Stolen keycards
- Lost keycards

Personnel in the following situations shall be denied entry:
- Failure to present a keycard;
- Presentation of a keycard not registered to the individual.

Exceptions for Insufficient Clearance:
    Personnel with keycards below the minimum clearance level(CL 3) may enter Sector 3 if accompanied by a senior personnel(CL 3 or above) from their department.

    In special circumstances, The Section 2.1.1, 2.1.2 may be disregarded.(Detailed Information In Section 2.2 of this file)

2.1.3 Regarding Section 2.2.2:
    Under the following circumstances, the application process may be bypassed:
1. Direct authorization by the Site Director or higher-ranking personnel (proof of authorization must be provided).
2. SCP containment breach requiring immediate assistance from the Scientific Department.
3. Other necessary circumstances as determined by the Administrative or Security Departments.

    Besides, Medical Department personnel may bypass Section 2 for sending SCP-008 Vaccine to the Vent system.

2.2 Explanations for Section 3

2.2.1 Regarding Section 3.1:

During a containment breach, non-combatant are prohibited from entering Sector-3 (S3). Combatants may disregard the relevant provisions in Section 2.1 and 2.2 and enter S3 directly.

A containment breach is defined as meeting any of the following criteria:
1. One or more Euclid-class SCPs have breached containment.
2. One or more Keter-class SCPs have breached containment.
3. Multiple Safe-class SCPs have breached containment.
4. The containment zone has come under attack by hostile forces and is at imminent risk of/or has already lost control.

Addition Notes:

During a containment breach, combatants may enter Sector-3 (S3) without presenting any Keycards. This also means that, under such circumstances, personnel with Clearance Level 2 (CL2) or below are permitted access to S3.

However, as they still do not meet the required clearance level, all CL2 and below personnel must immediately evacuate from S3 once the containment breach is resolved. CL3 and above personnel, on the other hand, shall remain within S3 and undergo comprehensive inspection procedures.

A containment breach may be declared over upon meeting at least two of the following conditions:
1. All escaped SCPs have been successfully recontained;
2. Hostile forces within the containment zone have been fully neutralized;
3. Inspection reports confirm normal operational status;
4. A direct order has been issued by senior personnel to lift the breach status.

2.2.2 Regarding Section 3.2:

The regulations for this scenario are fundamentally consistent with the provisions outlined in Section 3.1.

A hostile force assault event shall be announced when at least one of the following conditions is met:
1. Three or more armed hostile personnel infiltrate Sector-3 (S3);
2. The S3 checkpoint is compromised and rendered operationally disabled due to hostile assault;
3. S3 security forces lose control over the containment zone;
4. At least one SCP within the containment zone is breached by hostile forces;
5. The situation is officially declared as a hostile force assault event by authorized personnel.

During this event. Non-combatants are prohibited from entering Sector-3 (S3). Combatants may enter S3 directly.

2.2.3 Regarding Section 3.3:

Any D-Class personnel meeting one or more of the following criteria shall be designated as "Rogue Class-D" and are subject to immediate termination:
1. Possession of a weapon (regardless of intent to use).
2. Failure to comply with Foundation personnel commands.
3. Unauthorized deviation from designated activity zones.
4. Attempted harm against Foundation personnel.

2.2.4 Regarding Section 3.4:

Under the nuclear warhead detonation/Day break event:
1. All non-combatants must immediately evacuate Sector-3 (S3).
2. Combatants shall:
   - Deploy a 2-3 member tactical unit to conduct a rapid full-sector sweep of S3.
   - Only after confirming zero remaining personnel may the unit withdraw to designated rally points or evacuation shelter.

After Event:
1. Combatants must conduct a full-facility security sweep.
2. Non-combatants are to remain in designated safe zones until exiting the safe zone is granted.
3. After combatants confirm all sectors secure, non-combatants may leave the safe zone.
4. Facility reactivation may commence only after:
   - Combatants confirm all sectors secure
   - Threat elimination is verified by combatants.
   - Approval is given by Site Director or Higher clearance personnel.

Besides, During a blackout event(Sector 3 Standard Protocol, Section 3.5), All personnel in Sector 3 must:
1. Activate night-vision equipment and maintain Code Red alert status to counter potential hostile incursions.
2. Prohibit all non-combatants from entering S3 until full power restoration is achieved.

Also:
3. Pending tests in S3 are to be postponed until transformer repairs are completed.
4. Ongoing tests must be immediately suspended, with continuation permitted only upon explicit authorization from CL4+ AD personnel.

2.3 Explanations for Section 4

2.3.1 Regarding Section 4.1:
All security patrols within Sector-3 (S3) must follow to the following protocols:
1. Team Composition:
   - Maximum of 4 personnel per patrol unit.
2. Deployment Limits:
   - No more than 2 patrol teams (8 combatants total) may operate in S3 at the same time.
3. Operational Duration:
   - Each patrol must conclude within 10 minutes after entering S3.
4. Post-Patrol Procedure:
   - Patrol team must submit a patrol report to the Administrative Department through radio after patrol completion.

Version: 1.0

Date of Written:29/3/25