



Escalation Policy and Procedure

Policy Statement:

CAPITAL SHIELD SECURITY LTD is committed to providing effective and efficient security services. This escalation policy is designed to ensure the safety and security of all personnel and assets under our protection. It outlines the steps and procedures to be followed in the event of a security incident or emergency, defining the roles and responsibilities of our security personnel.

Scope:

This policy applies to all security personnel employed by CAPITAL SHIELD SECURITY LTD and to all sites where our security services are provided.

Definitions:

Security Incident: Any event that threatens the safety or security of personnel or assets.

Emergency: A situation that poses an immediate threat to life, safety, or property.

Policy Elements:

1. Primary Response:

Upon identifying a security incident, security personnel should immediately assess the situation and take appropriate initial action to mitigate the threat.

If possible, call for assistance from other on-site security personnel to control the situation.

Notify on-site management or supervisors about the incident.

2. Communication:

Use the provided communication devices (two-way radios, phones, etc.) to report the incident to the central security control room.

Clearly and concisely describe the situation, providing details such as location, nature of the incident, and any injuries if applicable.

3. Central Security Control Room:

The central security control room will act as the command center for coordinating the response.

The control room operator will immediately dispatch additional security personnel to the scene if required.

If the situation escalates to an emergency, the control room operator will notify local authorities (police, fire, or medical services) as necessary.

4. On-Site Management and Client Notification:

If the situation is not under control, the on-site manager or supervisor will be informed by security personnel.

On-site management will communicate with the client's designated contact person to keep them informed about the incident's status.

5. Incident Documentation:

Security personnel involved in the incident must maintain accurate records, including written reports, photographs, and witness statements if applicable.

The central security control room should also maintain a log of all actions taken during the incident.



Escalation Policy and Procedure

6. Post-Incident Review:

After the incident has been resolved, a debriefing session should be conducted with all involved security personnel to assess the response and identify areas for improvement.

Recommendations for procedural changes or additional training should be documented.

7. Incident Report and Documentation:

A comprehensive incident report should be generated within a specified timeframe (e.g., 24 hours) after the incident.

This report should include a summary of the incident, actions taken, and recommendations for further action.

8. Client Communication:

The client should be provided with the incident report as soon as possible, along with any recommendations for improving security measures.

9. Continuous Improvement:

Periodic reviews of the escalation policy should be conducted to ensure its effectiveness in handling security incidents and emergencies.

10. Compliance:

All security personnel are expected to adhere to this escalation policy as part of their duties.

Conclusion:

This Security Guarding Services Escalation Policy is designed to ensure the safety and security of all personnel and assets under our protection. Regular training and drills should be conducted to ensure that all security personnel are familiar with this policy and can respond effectively in the event of a security incident or emergency.



Escalation Policy and Procedure

Escalation Procedure

Objective:

This procedure outlines the steps to be followed in the event of a security incident or emergency, ensuring the safety and security of all personnel and assets under our protection.

Scope:

This procedure applies to all security personnel employed by [Your Company Name] and to all sites where our security services are provided.

Definitions:

Security Incident: Any event that threatens the safety or security of personnel or assets.

Emergency: A situation that poses an immediate threat to life, safety, or property.

Procedure:

1. Primary Response:

Upon identifying a security incident, security personnel should immediately assess the situation and take appropriate initial action to mitigate the threat.

If possible, call for assistance from other on-site security personnel to control the situation.

Notify on-site management or supervisors about the incident.

2. Communication:

Use the two-way radio, phone, or other communication devices to report the incident to the central security control room.

Clearly and concisely describe the situation, providing details such as location, nature of the incident, and any injuries if applicable.

3. Central Security Control Room:

The central security control room will act as the command center for coordinating the response.

The control room operator will immediately dispatch additional security personnel to the scene if required.

If the situation escalates to an emergency, the control room operator will notify local authorities (police, fire, or medical services) as necessary.

4. On-Site Management and Client Notification:

If the situation is not under control, the on-site manager or supervisor will be informed by security personnel.

On-site management will communicate with the client's designated contact person to keep them informed about the incident's status.

5. Incident Documentation:

CSS-POL-39

Revision-01

Issuance Date: 01-01-2026



Escalation Policy and Procedure

Security personnel involved in the incident must maintain accurate records, including written reports, photographs, and witness statements if applicable.

The central security control room should also maintain a log of all actions taken during the incident.

6. Post-Incident Review:

After the incident has been resolved, a debriefing session should be conducted with all involved security personnel to assess the response and identify areas for improvement.

Recommendations for procedural changes or additional training should be documented.

7. Incident Report and Documentation:

A comprehensive incident report should be generated within a specified timeframe (e.g., 24 hours) after the incident.

This report should include a summary of the incident, actions taken, and recommendations for further action.

8. Client Communication:

The client should be provided with the incident report as soon as possible, along with any recommendations for improving security measures.

9. Continuous Improvement:

Periodic reviews of the escalation procedure should be conducted to ensure its effectiveness in handling security incidents and emergencies.

10. Compliance:

All security personnel are expected to adhere to this escalation procedure as part of their duties.

Conclusion:

This Security Guarding Services Escalation Procedure is designed to ensure the safety and security of all personnel and assets under our protection. Regular training and drills should be conducted to ensure that all security personnel are familiar with this procedure and can respond effectively in the event of a security incident or emergency.

Approved

Managing Director

A handwritten signature in black ink, appearing to be "J. Smith", is written over a horizontal line.

CAPITAL SHIELD SECURITY LTD

This policy is reviewed on 01 01 2026