Media Talk Policy

1. Purpose

This Media Talk Policy establishes clear guidelines for communication with the media to safeguard the organization's operational security, protect client confidentiality, and ensure accurate and consistent public messaging.

2. Scope

This policy applies to all employees, contractors, temporary staff, and representatives of the organization who may interact with journalists, news outlets, bloggers, or any external media platforms.

3. Policy Statement

Only authorized spokespersons may speak on behalf of the organization. All employees must refrain from providing statements, opinions, or information to members of the media without explicit approval.

4. Authorized Spokespersons

The following positions are authorized to communicate with the media:

- Managing Director Lloyds Security Services (Hamid Mahmood)

Unauthorized individuals must direct all media inquiries to the Communications Office.

5. Prohibited Disclosures

Employees are strictly prohibited from sharing the following information:

- Details of security procedures, technologies, patrol methods, or system vulnerabilities
- Client identities, locations, contract details, or confidential information
- Incident details before they are officially verified and released
- Internal investigations, personnel matters, or legal proceedings
- Sensitive photos, video footage, or written materials

6. Handling Media Inquiries

When approached by the media, employees must:

1. Remain professional and courteous.
2. Avoid answering any questions or providing commentary.
3. Redirect the journalist to the designated spokesperson.

4. Report the interaction to their supervisor immediately.

Approved Response Script: "I'm not authorized to speak on behalf of the organization, but I can connect you with our Communications Office."

7. Crisis Communication

During emergencies or significant incidents:

- All public statements must be coordinated through the Crisis Communications Team (Managing Director)
- Information released must be factual, verified, and cleared by leadership.
- No employee may share unapproved updates, photos, or comments on any platform.

8. Social Media Restrictions

Employees may not:

- Discuss work activities, clients, or incidents online
- Post pictures or videos taken at client sites or during operations
- Share internal documents, schedules, or sensitive security details
- Engage with the media through personal social accounts regarding work matters

9. Legal and Compliance Requirements

All communications must comply with:

- Applicable privacy and data protection laws
- Client confidentiality agreements
- Law enforcement and regulatory protocols
- Contractual obligations and non-disclosure agreements

10. Training and Awareness

Employees will receive periodic training on this policy, including:

- Media interaction protocols
- Operational security (OPSEC) practices
- Social media guidelines

11. Violations and Consequences

Non-compliance with this policy may result in disciplinary actions, up to and including termination. Legal action may be taken if disclosures breach confidentiality or contractual obligations.

12. Policy Review and Updates

This policy will be reviewed annually or as needed to remain aligned with operational, legal, and industry standards.