Confidentiality Policy

1. Introduction

The Institute of Industrial Engineers & Safety Management Systems (IIESMS) is committed to maintaining the highest standards of confidentiality regarding the information it handles. This Confidentiality Policy outlines the principles and procedures for protecting confidential information and ensuring that it is handled appropriately.

2. Policy Statement

IIESMS is dedicated to:

- Protecting the confidentiality of all personal, professional, and sensitive information.
- Complying with all relevant laws and regulations regarding confidentiality.
- Ensuring that all employees, members, contractors, and stakeholders understand their responsibilities regarding confidentiality.

3. Scope

This policy applies to all IIESMS employees, members, contractors, volunteers, and other stakeholders who may have access to confidential information.

4. Definition of Confidential Information

Confidential information includes, but is not limited to:

- Personal information about employees, members, contractors, and other stakeholders.
- Business information, including financial records, strategic plans, and proprietary processes.
- Information about IIESMS's projects, research, and development activities.
- Any other information designated as confidential by IIESMS.

5. Responsibilities

5.1 Management

- Ensure that adequate measures are in place to protect confidential information.

- Provide training and resources to employees and members to understand their confidentiality obligations.

5.2 Employees and Members

- Adhere to this Confidentiality Policy and related procedures.
- Ensure that confidential information is accessed, used, and disclosed only as authorised.
- Report any breaches of confidentiality to the appropriate authority immediately.

6. Handling Confidential Information

6.1 Access

- Access to confidential information is restricted to authorised individuals who require it for their roles.
- Unauthorized access or disclosure of confidential information is strictly prohibited.

6.2 Storage

- Confidential information must be stored securely, whether in physical or electronic form.
- Physical documents should be kept in locked cabinets or secure areas.
- Electronic information should be protected by strong passwords, encryption, and other security measures.

6.3 Transmission

- Confidential information should be transmitted securely using encrypted email or secure file transfer methods.
- Avoid sharing confidential information through unsecured channels or public networks.

6.4 Disposal

- Confidential information should be disposed of securely when no longer needed.
- Shred physical documents and use secure deletion methods for electronic files.

7. Breach of Confidentiality

- Any suspected or actual breaches of confidentiality must be reported immediately to the designated authority.
- An investigation will be conducted to determine the cause and extent of the breach.
- Appropriate corrective actions will be taken, including disciplinary measures if necessary.

8. Training and Awareness

- Provide regular training on confidentiality policies and procedures to all employees, members, and relevant stakeholders.
- Ensure that all individuals understand their responsibilities and the importance of maintaining confidentiality.

9. Review and Updates

This Confidentiality Policy will be reviewed regularly and updated as necessary to ensure it remains relevant and effective.

10. Contact

For questions or concerns about this Confidentiality Policy, please contact the **Institute of Industrial Engineers & Safety Management Systems (IIESMS)**
Email: info@iiesms.ie
Phone: +353 (0)51 311134