Cybersecurity Policy

1. Introduction

The Institute of Industrial Engineers & Safety Management Systems (IIESMS) is committed to safeguarding its information systems and data against cybersecurity threats. This Cybersecurity Policy outlines the principles and procedures for protecting our digital infrastructure and ensuring the confidentiality, integrity, and availability of information.

2. Policy Statement

IIESMS aims to:

- Protect information systems and data from unauthorised access, use, disclosure, disruption, modification, or destruction.
- Comply with all relevant cybersecurity laws, regulations, and best practices.
- Promote a culture of cybersecurity awareness and responsibility among employees, members, and stakeholders.

3. Scope

This policy applies to all employees, members, contractors, volunteers, and other stakeholders who have access to IIESMS's information systems and data.

4. Cybersecurity Principles

IIESMS adheres to the following cybersecurity principles:

- **Confidentiality:** Ensuring that information is accessible only to those authorised to have access.
- **Integrity:** Safeguarding the accuracy and completeness of information and processing methods.
- **Availability:** Ensuring authorised users can access information and associated assets when required.

5. Responsibilities

5.1 Management

- Provide leadership and oversight of cybersecurity practices.
- Ensure that adequate resources are allocated for cybersecurity management.
- Monitor and review cybersecurity performance regularly.

5.2 Cybersecurity Officer

- Implement and maintain the cybersecurity management system.
- Conduct regular risk assessments and security audits.
- Provide cybersecurity training and information to employees and members.
- Respond to cybersecurity incidents and implement corrective actions.

5.3 Employees and Members

- Adhere to this Cybersecurity Policy and related procedures.
- Use information systems and data responsibly and securely.
- Report any cybersecurity incidents or concerns to the Cybersecurity Officer immediately.

6. Risk Management

- Conduct regular risk assessments to identify potential cybersecurity threats and vulnerabilities.
- Implement measures to mitigate identified risks, including technical controls, policies, and procedures.
- Review and update risk assessments periodically or when significant changes occur in the IT environment.

7. Access Control

- Restrict access to information systems and data to authorised individuals based on their roles and responsibilities.
- Implement strong authentication and authorisation mechanisms, including multi-factor authentication where appropriate.
- Regularly review and update access permissions to ensure they remain appropriate.

8. Data Protection

- Encrypt sensitive data in transit and at rest to protect it from unauthorised access.
- Implement data backup and recovery procedures to ensure data integrity and availability.
- Regularly test backup and recovery procedures to ensure they are effective.

9. Network Security

- Implement network security measures, including firewalls, intrusion detection/prevention systems, and secure network configurations.
- Monitor network traffic for suspicious activity and respond to potential threats promptly.
- Ensure that wireless networks are secured using strong encryption and authentication methods.

10. Endpoint Security

- Ensure that antivirus software, firewalls, and other security measures protect all devices accessing IIESMS's information systems.
- Regularly update and patch software and operating systems to protect against known vulnerabilities.
- Implement device management policies to control the use of personal devices (BYOD).

11. Incident Response

- Develop and maintain an incident response plan to address cybersecurity incidents effectively.
- Train employees and members on how to recognise and report cybersecurity incidents.
- Investigate and respond to incidents promptly, including notifying affected parties and regulatory authorities as required.

12. Training and Awareness

- Provide regular cybersecurity training to all employees, members, and relevant stakeholders to raise awareness and promote secure behaviour.
- Ensure that all individuals understand their responsibilities and the importance of cybersecurity.

13. Monitoring and Review

- Regularly monitor and review cybersecurity performance to ensure compliance with this policy and identify areas for improvement.
- Conduct periodic audits of the cybersecurity management system to ensure its effectiveness.

14. Continuous Improvement

- Set and review cybersecurity objectives and targets to drive continuous improvement.
- Encourage innovation and the adoption of new technologies and practices that enhance cybersecurity.

15. Review and Updates

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

16. Contact

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