

## Standard Operating Procedure (SOP)

Cybersecurity Head

Institution's Innovation Council (IIC)

### 1. Purpose

The Cybersecurity Head is responsible for ensuring the security, privacy, and protection of digital assets, data, and online infrastructure of IIC. This role focuses on preventing unauthorized access, data breaches, and cyber threats, while promoting awareness about cybersecurity among members.

### 2. Scope

This SOP applies to all cybersecurity-related activities of the IIC, including:

- Protection of official IIC systems, websites, and online platforms.
- Security of sensitive documents, credentials, and member data.
- Conducting cybersecurity awareness and training programs.
- Managing cyber hygiene during online events, webinars, and competitions.

### 3. Responsibilities

The Cybersecurity Head shall:

#### 1. Digital Protection

- Monitor and secure all IIC digital platforms (website, email, cloud drives, etc.).
- Implement password management and multi-factor authentication practices.
- Regularly audit access permissions and ensure secure storage of credentials.

#### 2. Incident Response

- Respond immediately to any suspected or confirmed cyber incidents.
- Coordinate with Technical and Web Development Heads for system recovery.
- Maintain a detailed log of security incidents and resolutions.

### **3. Awareness and Training**

- Conduct sessions, workshops, or webinars on cybersecurity and ethical hacking.
- Promote responsible online behavior among IIC members.
- Share monthly cybersecurity tips or updates with all teams.

### **4. Policy & Compliance**

- Establish basic cybersecurity guidelines and ensure all teams follow them.
- Work with the Documentation Head to maintain a record of security audits and reports.
- Ensure all digital tools used by IIC comply with institutional IT policies.

### **5. Collaboration & Innovation**

- Collaborate with the R&D and Technical Heads for cybersecurity-related projects.
- Encourage members to work on innovative cybersecurity solutions and competitions.

### **4. Authority**

- The Cybersecurity Head has the authority to restrict access, request password resets, or recommend technical actions for data protection.
- All major cybersecurity decisions must be communicated to the Student President and Board.
- Board Members of IIC reserve the right to remove the Cybersecurity Head from the position at any time if found underperforming or violating organizational standards.

### **5. Review**

This SOP shall be reviewed annually or as required by the IIC Board to ensure it remains aligned with emerging cybersecurity practices and institutional needs.