SINHGAD TECHNICAL EDUCATION SOCIETY'S

SINHGAD INSTITUTE OF TECHNOLOGY, LONAVALA

INSTITUTION'S INNOVATION COUNCIL (IIC)

CYBER SECURITY CONSTITUTION 2026 – 2036

Master SOP for Digital Defense, Threat Intelligence, and Forensic Accountability

The Definitive Spoon-Feeding Manual for the Council's Shield: Managing Peak Threats, Forensic Investigations, and the Absolute Integrity of the IIC Digital Ecosystem.

Custodians:	**Approving Authority:**
Cyber Security Head	Dr. M.S. Chaudhari
IIC SIT Lonavala	Dean R&D and President IIC

Classification: Restricted/Top-Secret

January 2, 2026

Contents

1 ARTICLE I: FOUNDATIONAL MISSION AND SCOPE

1.1 The ”Sovereign Shield” Mandate

The Cyber Security Department is established as the primary intelligence and defense wing of the Council. Their mission is to maintain the **Peak Security Integrity** of every digital asset, physical lab access point, and research prototype. They are the ”Internal Affairs” of the tech ecosystem, responsible for identifying vulnerabilities before they are exploited and investigating any breach—whether it occurs within the club or involves institutional interests externally.

1.2 The ”Trust-but-Verify” Rule

In the IIC, technical innovation cannot exist without security. No system (Web, IoT, or Network) is considered ”Live” until it carries a **Cyber Security Certification** issued by the Head. The team must operate with absolute neutrality, investigating cases with data-driven forensic accuracy.

2 ARTICLE II: DETAILED ROLES AND INTELLIGENCE COMMAND

2.1 The Cyber Security Head (Chief Information Security Officer)

- **Supreme Auditor:** Holds the power to halt any event or system deployment if a critical security flaw is identified.
- **Lead Investigator:** Personally leads all digital forensic investigations and drafts the ”Final Threat Report” for the Faculty President.
- **Certification Authority:** Signs off on the ”Security Clearance” for new hardware and software integrations.

2.2 The Security Co-Head (Red-Team Lead)

- **Vulnerability Hunter:** Leads the penetration testing of the IIC Portal and internal networks.
- **Incident Responder:** First point of contact during a live attack (DDOS, SQL Injection, or Data Leak).
- **Asset Protection:** Manages the encryption standards for the ”Legacy HDD” and R&D code repositories.

3 ARTICLE III: THREAT IDENTIFICATION & INVESTIGATION

3.1 Peak Threat Monitoring

The team must maintain a 24/7 ”Threat Radar.”

- **Internal Threats:** Monitoring for unauthorized credential sharing, ”shadowing” in the lab, or data exfiltration by members.
- **External Threats:** Tracking institutional mentions on the deep-web or identifying phishing attempts targeting IIC leadership.

3.2 Investigative Authority

The Head is empowered to investigate any ”Cyber Case” affecting the Council:

1. **Case Initiation:** When an anomaly is detected, the Head opens a ”Formal Investigation Log.”
2. **Evidence Collection:** Forensic imaging of logs from the iicsit.in portal or lab biometric systems.
3. **The Investigative Report:** A detailed dossier containing ”Point of Entry,” ”Impact Analysis,” and ”Recommended Disciplinary Action.”

4 ARTICLE IV: CROSS-DEPARTMENTAL SECURITY AUDITS

4.1 Collaboration with WebDev Team

- **Code Audit:** Every major update to the portal must undergo a ”Static Analysis” by Cyber Security.
- **Vulnerability Assessment:** Monthly automated scans for XSS, SQLi, and outdated server dependencies.

4.2 Collaboration with R&D and Technical Teams

- **IoT Inspection:** R&D prototypes involving wireless communication (ESP32, Drones, Rovers) must be inspected for ”Hijack Vulnerabilities.”
- **Firmware Testing:** Verification that no hardcoded credentials exist in R&D firmware.
- **Lab Security:** Digital management of biometric logs. Any ”Unrecognized Entry” must be flagged within 12 hours.

5 ARTICLE V: EVENT AND LIVE-STREAMING SECURITY

5.1 Broadcast Integrity

The Technical Team sets up the stream; Cyber Security **guards** it.

- **Streaming Security:** Preventing ”Stream Sniping” or unauthorized access to Zoom/YouTube backend keys.

- **Admittance Scrutiny:** Verifying that participants in private webinars match the PR Team's registration database.
- **Data Logs:** Maintaining a clean record of all IP addresses accessing IIC-hosted digital events for post-event audit.

6 ARTICLE VI: MANDATORY CERTIFICATION & APPROVALS

6.1 New System Integration (NSI) Protocol

No new software or hardware (e.g., a new lab router or a custom-built ERP) can be used without:

- **The Pen-Test Phase:** 48 hours of stress-testing by the Security Team.
- **Approval Document:** A signed "Security Clearance Certificate" from the Head. Use of uncertified systems is grounds for "Termination of Membership" for the lead of that specific project.

7 ARTICLE VII: ACCOUNTABILITY, LOGS & ATTENDANCE

7.1 Strict Professional Discipline

- **Compulsory Attendance:** Cyber Security members must be present for every system integration meeting. Absence results in an immediate "Red Slip" due to the high-risk nature of the role.
- **Confidentiality (NDA):** Members have access to sensitive logs. Leaking an investigation detail results in permanent blacklisting and a formal report to the College Administration.
- **The "Busy" Rule:** During an "Active Incident," the Security Team is exempt from general council duties to focus 100% on threat mitigation.

8 ARTICLE VIII: STEWARDSHIP AND MULTI-CAMPUS LEGACY

8.1 Dual-Campus Defense Synchronization

- **Standardized Security:** Both colleges must use the same encryption standards for data storage.
- **Joint Threat Intelligence:** If a vulnerability is found in College A's network, a "Security Bulletin" must be issued to College B within 4 hours.
- **The Security Heritage HDD:** A physical drive containing all previous vulnerability reports, patch histories, and forensic tools for future leads.

9 ARTICLE IX: REAL-WORLD SCENARIO MITIGATION

9.1 Scenario A: The Portal Defacement

If the official website is hacked and shows unauthorized content:

- **Action:** Cyber Security Head issues an ”Emergency Lockdown” to the Web Team.
- **Investigation:** Identifying the compromised credential or unpatched plugin.
- **Recovery:** Only after the ”Security Patch” is certified by the Head can the site go live again.

9.2 Scenario B: The Hardware Breach

If an R&D Drone is found to be responding to an external unauthorized controller:

- **Action:** Security Lead performs a ”Wireless Packet Capture” to identify the intrusion frequency.
- **Prevention:** Implementing a mandatory rolling-code encryption for all future R&D communications.

SIGNATORIES OF THE 2026 SECURITY CONSTITUTION

Cyber Security Head (Guardian)	*Student President*	*Dean R&D (STES)*