Standard Operating Procedure (SOP) for Corporate Cyber Protection

(Prepared by CAPSI AI & Cyber Task Force)

Objective

To establish a structured and proactive framework for protecting corporate digital assets from cyber threats and ensuring a resilient cybersecurity posture.

1. Governance and Leadership

- Appoint a CISO: Designate a Chief Information Security Officer (CISO) or Virtual CISO responsible for cyber risk management.
- Cybersecurity Governance Committee: Establish a committee including IT, Legal, HR, and Operations to oversee cybersecurity efforts.
- Cybersecurity Policy: Define a policy aligned with ISO 27001/NIST CSF standards.

2. Risk Assessment and Asset Inventory

- Cyber Risk Assessment: Conduct a risk assessment every 6 months to identify potential threats.
- Asset Inventory: Maintain a detailed inventory of IT assets, including servers, endpoints, IoT devices, and cloud services.
- Asset Classification: Classify assets based on criticality and data sensitivity.

3. Network & Endpoint Security

- Firewalls and IPS: Implement firewalls and intrusion prevention systems (IPS) to protect the network.
- EDR Solutions: Use endpoint detection and response (EDR) solutions on all devices.
- Network Segmentation: Segment networks to isolate critical systems and prevent lateral movement.

4. Identity & Access Management (IAM)

- Multi-Factor Authentication: Enforce MFA for all user logins.
- Least Privilege Access: Apply least privilege access principles to limit user access.
- Access Rights Review: Review and update user access rights quarterly.

5. Data Protection & Backup

- Data Encryption: Encrypt sensitive data at rest and in transit.
- Regular Backups: Establish regular backups (3-2-1 strategy) with air-gapped storage.
- Data Restoration: Test data restoration capabilities monthly.

6. Email & Phishing Protection

- Anti-Phishing Gateways: Use anti-phishing gateways and SPF, DKIM, and DMARC protocols.
- Employee Training: Train employees on phishing awareness and conduct mock phishing tests quarterly.

7. Application and Cloud Security

- Secure Applications: Secure all applications with code reviews, WAFs, and DevSecOps practices.
- Vulnerability Scans: Conduct regular vulnerability scans and penetration testing.
- Cloud Security: Monitor cloud platforms for misconfigurations and anomalies using CSPM tools.

8. Incident Response & Forensics

- Incident Response Plan: Maintain a Cybersecurity Incident Response Plan (CSIRP).
- 24/7 SOC: Set up a 24/7 Security Operations Center (SOC) or outsource to an MSSP.
- Incident Logging: Log all incidents and conduct Root Cause Analysis (RCA) within 72 hours.

9. Legal Compliance & Reporting

- Compliance: Ensure compliance with IT Act 2000, CERT-IN directives, and GDPR/DPDP if applicable.
- Breach Reporting: Report major breaches to authorities (CERT-IN) within the stipulated time frame.
- Breach Register: Maintain a breach register with resolution status.

10. Training & Continuous Awareness

- Monthly Awareness Programs: Conduct monthly cybersecurity awareness programs for all staff.
- Cyber Attack Drills: Simulate cyber attack drills bi-annually.
- Security Personnel Certification: Certify all security personnel through recognized programs.

11. Vendor Risk Management

- Vendor Audit: Audit all third-party vendors for cyber compliance.
- Security Clauses: Ensure NDAs and security clauses in vendor contracts.
- Vendor Access Monitoring: Monitor third-party access and integrations regularly.

12. Cyber Insurance

- Cyber Liability Insurance: Evaluate and subscribe to a Cyber Liability Insurance plan.
- Coverage: Ensure coverage includes data breaches, business interruption, and ransomware payouts.

13. Board-Level Reporting

- Quarterly Reporting: Present cybersecurity posture, incident reports, and risk metrics to the Board quarterly.
- Cyber Resilience Planning: Include cyber resilience plans in overall business continuity planning.

14. Device Security

1. Use Strong, Unique Passwords
   - Avoid reuse; consider using a password manager.
2. Enable Multi-Factor Authentication (MFA)
   - Especially for email, cloud apps, VPNs, and critical systems.
3. Keep Software and Operating Systems Updated
   - Install patches promptly for OS, browsers, and apps.
4. Use Authorized Antivirus and Security Tools
   - Keep them enabled and updated at all times.
5. Avoid Rooting/Jailbreaking Mobile Devices
   - It weakens built-in security controls.

15. Network Safety

1. Avoid Using Public Wi-Fi Without a VPN
   - Use company-approved VPNs when working remotely.
2. Connect Only to Secure Networks
   - Never use unknown or unsecured hotspots for work.
3. Disable Bluetooth and Auto-Connect Features When Not Needed
   - Prevents unwanted device pairing.

16. Email and Communication

1. Beware of Phishing Emails and Messages
   - Don’t click on suspicious links or attachments; verify sender identity.
2. Don’t Share Confidential Info via Unsecured Channels
   - Use encrypted platforms approved by your organization.

17. Data Handling

1. Avoid Installing Unauthorized Software or Apps - Only use tools vetted by IT.
2. Do Not Store Work Files on Personal Devices or Drives - Use company-managed cloud storage or secured drives.
3. Encrypt Sensitive Data When Storing or Sharing - Follow data classification and handling policies.

18. Behavioral Practices

1. Lock Your Screen When Away - Even for short breaks—especially in public or shared spaces.
2. Report Suspicious Activity Immediately - Notify IT/security teams of any unusual activity or potential breaches.

Recommended Tools

- SIEM: Splunk, QRadar
- EDR: CrowdStrike, SentinelOne
- IAM: Okta, Azure AD
- CSPM: Wiz, Prisma Cloud
- Email Security: Proofpoint, Mimecast

DO NOT CLICK ANY NEWS LINK OR IMAGE ETC, ORIGINATING FROM PAK MEDIA, PAK NEWS CHANNEL OR PAK SOCIAL MEDIA HANDLES … BEST TIME FOR PAK STATE ACTORS TO EXPLOIT INNOCENT LOTS FOR THEIR NEFARIOUS GOALS

By following this SOP, organizations can establish a robust cybersecurity framework to protect their digital assets and ensure business continuity.

Kunwar Vikram Singh
Chairman
Central Association of Private Security Industry
www.capsi.in