# Cybersecurity Breach IP Checklist (India)

Step-by-step IP protection and legal compliance checklist for cybersecurity incidents

| HOW TO USE THIS TEMPLATE | |
|---|---|
| 1. | Use this checklist immediately upon discovering or suspecting a cybersecurity incident. |
| 2. | Preserve all logs, evidence, and records — do not wipe or reset systems without IP team approval. |
| 3. | Notify the IP team within 1 hour of discovering any breach involving Company IP or source code. |
| 4. | Under the DPDP Act 2023 and IT Act 2000, certain breaches may require regulatory notification. |
| 5. | Document every action taken — this record is critical for legal proceedings and insurance claims. |

## INCIDENT DETAILS

| | |
|---|---|
| **Incident Reference Number** | [INC-YYYY-NNN — assigned by IT team] |
| **Date and Time Incident Detected** | [DD/MM/YYYY HH:MM] |
| **Date and Time Incident Reported to IT** | [DD/MM/YYYY HH:MM] |
| **Person Who Detected the Incident** | [Name, designation, and contact] |
| **IT/Security Lead Handling Incident** | [Name and contact] |
| **IP Manager / Legal Notified** | [Name and time of notification] |
| **CEO / MD Notified** | [Name and time of notification] |
| **Type of Incident (initial assessment)** | [Ransomware / Data breach / Unauthorised access / Phishing / Insider threat / Source code theft / Other] |
| **Systems / Data Affected (initial assessment)** | [List affected systems, repositories, databases] |
| **Is this incident ongoing?** | [Yes — containment in progress / No — incident appears contained] |

## PHASE 1 — IMMEDIATE CONTAINMENT (0–1 HOUR)

| Action | Detail | Responsible | Done? | Time |
|---|---|---|---|---|
| Isolate affected systems from network | Disconnect compromised devices from company network and internet. Do NOT power off — preserve volatile memory and logs. | IT Security | ■ | ___:___ |
| Revoke compromised access credentials | Immediately reset passwords and revoke API keys, SSH keys, or tokens associated with compromised accounts. | IT Security | ■ | ___:___ |
| Preserve forensic evidence | Take memory dumps and disk images before any remediation. Preserve all logs in read-only format. Document chain of custody. | IT Security + Legal | ■ | ___:___ |

| | | | | |
|---|---|---|---|---|
| Identify what IP may be affected | Conduct initial triage: source code repos, design files, customer databases, trade secret documents, patent-pending information. | IP Manager | ■ | ___:___ |
| Notify IP Manager and Legal team | Brief the IP Manager and Legal on what IP may have been accessed, copied, or exfiltrated. | CEO / CTO | ■ | ___:___ |
| Activate incident response team | Convene emergency meeting with CTO, IP Manager, Legal, and HR (if insider threat). | CEO | ■ | ___:___ |

## PHASE 2 — IP IMPACT ASSESSMENT (1–24 HOURS)

**2.1 Source Code and Technical IP Assessment.** Determine specifically what source code, algorithms, technical specifications, or other technical IP may have been accessed or exfiltrated:

| | |
|---|---|
| **Git repositories accessed or cloned** | [List affected repos — include branch and commit hash of last known clean state] |
| **Design files / CAD files accessed** | [List affected files] |
| **Patent-pending or trade secret technical data accessed** | [Reference TS Register entries — specify TS reference numbers] |
| **Development environment credentials exposed** | [API keys, SSH keys, cloud service credentials, database passwords] |
| **Extent of exfiltration (if known)** | [Estimated volume of data — files, records, or lines of code] |

**2.2 Commercial and Customer IP Assessment.** Determine what commercial and customer data may have been accessed:

| | |
|---|---|
| **Customer database records accessed** | [Estimated number of records — customer names, contacts, commercial terms] |
| **Pricing and commercial strategy documents accessed** | [List documents] |
| **Investor information or financial data accessed** | [Describe] |
| **Employee personal data accessed** | [Estimated number of records — may trigger DPDP notification obligations] |
| **Third-party IP (licensed software, customer data) affected** | [Describe — may trigger third-party notification obligations] |

## PHASE 3 — LEGAL AND REGULATORY OBLIGATIONS (24–72 HOURS)

| Action | Detail | Responsible | Done? |
|---|---|---|---|
| Assess DPDP Act 2023 notification obligation | If personal data of customers or employees was breached, assess whether notification to the Data Protection Board is required under the Digital Personal Data Protection Act 2023. | Legal / DPO | ■ |
| Assess IT Act 2000 obligations | Section 43A of the IT Act 2000 imposes liability for negligent handling of sensitive personal data. Assess whether the breach triggers liability. | Legal | ■ |
| Notify cyber insurance carrier | If the Company has cyber insurance, notify the insurer within the time limit specified in the policy — typically 24–72 hours of discovery. | CFO / Legal | ■ |

| | | | |
|---|---|---|---|
| Consider FIR / police complaint | For significant breaches involving source code theft, insider threat, or ransomware, consider filing a complaint with the Cyber Crime Cell under the IT Act 2000. | Legal + CEO | ■ |
| Notify affected third parties | If customer data, partner data, or investor data was breached, assess contractual and legal obligations to notify affected parties. | Legal + CEO | ■ |
| Assess patent filing urgency | If patent-pending or patentable trade secrets were exposed, immediately assess whether emergency patent filings are required to preserve patent rights. | IP Manager + Patent Attorney | ■ |

## PHASE 4 — REMEDIATION AND RECOVERY

| | |
|---|---|
| **Systems fully remediated and restored** | [Date and description of remediation steps] |
| **All compromised credentials rotated** | [Date completed — list all systems where credentials were rotated] |
| **Security patches applied** | [List patches applied and systems affected] |
| **New access controls implemented** | [Describe any new access restrictions, MFA requirements, or monitoring tools deployed] |
| **Employee security briefing conducted** | [Date and scope of briefing] |
| **Penetration test or security audit commissioned** | [Date commissioned — firm engaged] |

## PHASE 5 — POST-INCIDENT REVIEW

| | |
|---|---|
| **Root cause identified** | [Describe root cause — phishing, unpatched system, insider, weak credential, third-party vendor, etc.] |
| **IP ultimately compromised — final assessment** | [List all IP confirmed to have been accessed or exfiltrated] |
| **Financial impact estimate** | [Estimated cost of breach — remediation, legal, business disruption, potential liability] |
| **Lessons learned and policy improvements** | [Describe changes to policies, systems, or processes being implemented] |
| **Board / investor notification required?** | [Yes / No — if Yes, date of notification and persons notified] |
| **Date of post-incident report** | [DD/MM/YYYY] |
| **Post-incident report prepared by** | [Name and designation] |

## INCIDENT COMMANDER SIGN-OFF

| IT SECURITY LEAD | IP MANAGER / LEGAL | CEO / MD |
|---|---|---|
| Signature: _____ | Signature: _____ | Signature: _____ |
| Name: _____ | Name: _____ | Name: _____ |
| Date: _____ | Date: _____ | Date: _____ |

**IMPORTANT NOTE**

TIME-CRITICAL: The Digital Personal Data Protection Act 2023 and IT Act 2000 impose notification and compliance obligations with specific timeframes. Failure to notify within required periods may result in regulatory penalties. Engage legal counsel within 24 hours of any significant breach. Template only — not legal advice.

## REGULATORY FRAMEWORK AND LEGAL OBLIGATIONS

**6.1 DPDP Act 2023 — Data Breach Obligations.** Under the Digital Personal Data Protection Act 2023 and its implementing rules, the Company as a Data Fiduciary must notify the Data Protection Board of India and affected Data Principals (individuals) of any personal data breach that is likely to cause significant harm. The notification timelines and format will be specified in the implementing rules. In the absence of notified rules, the Company should adopt best practice: notify the DPB within 72 hours of becoming aware of a significant breach, and notify affected individuals without undue delay.

**6.2 CERT-In Reporting Obligations.** Under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013, certain cybersecurity incidents must be reported to CERT-In (the Indian Computer Emergency Response Team) within specified timeframes. Reportable incidents include: data breaches involving sensitive personal data; ransomware attacks; attacks on critical information infrastructure; and unauthorised access to IT systems. The Company should verify the current reporting obligations with the CERT-In website (cert-in.org.in) and report applicable incidents within the prescribed 6-hour window for the most serious incidents.

**6.3 Insurance Claim Documentation.** If the Company carries cyber insurance, the quality of incident documentation under this Checklist directly affects the insurance claim. Insurers typically require: a detailed timeline of events from discovery to remediation; evidence of the root cause; documentation of all costs incurred (IT forensics, legal fees, regulatory fines, business interruption, customer notification costs); and evidence that reasonable security measures were in place before the breach. Maintaining this Checklist as a contemporaneous record — completing it in real time during the incident — creates the strongest evidentiary foundation for an insurance claim.

**6.4 IP-Specific Incident Response — Source Code Theft.** Where the breach involves potential theft of source code, algorithms, or other technical trade secrets, additional IP-specific steps are required: (a) engage an IP litigation attorney immediately — do not wait for the full incident report; (b) assess whether any patent-pending inventions may have been exposed — this may trigger urgency for provisional patent filing; (c) document the exact state of the source code at the time of breach (commit hashes, version numbers) to establish what was owned by the Company at the relevant time; and (d) if there is reason to believe a specific individual (e.g. a departing employee or competitor) is responsible, preserve evidence for potential civil proceedings under the IT Act 2000 and common law misappropriation.