Remote Work / WFH IP Policy (India)

IP creation, device security, data handling, and AI tool rules for remote and hybrid employees

HOW TO USE THIS TEMPLATE	
1.	Applies to ALL employees working remotely — fully remote, hybrid, or occasional WFH.
2.	Distribute to all employees and require signed acknowledgement before any remote work begins.
3.	Review and update annually — remote work technology and risks evolve rapidly.
4.	Specific device, network, and data-handling rules must be read alongside your Cybersecurity Policy.
5.	IP ownership rules apply the same way whether the employee is in the office or working remotely.

1. PURPOSE AND SCOPE

1.1 This Remote Work and Work-From-Home Intellectual Property Policy (this **"Policy"**) establishes the Company's rules regarding the creation, protection, and handling of intellectual property and confidential information when employees work from home, from co-working spaces, or from any location other than the Company's designated office premises.

1.2 This Policy applies to all employees, including full-time employees, part-time employees, contractual employees, and interns who are authorised to work remotely on a full-time, hybrid, or occasional basis.

1.3 Why This Policy Is Needed. Remote work creates specific IP and confidentiality risks that do not arise in a controlled office environment: work product may be created on personal devices; confidential information may be transmitted over insecure networks; physical documents may be left in non-secure locations; and the boundary between personal and Company work may become blurred. This Policy addresses each of these risks.

2. IP OWNERSHIP — NO CHANGE IN REMOTE WORK

2.1 The employee's IP assignment obligations under their Employment Agreement apply in exactly the same way when working remotely as when working in the office. All work product, inventions, software, designs, content, and other intellectual property created by the employee in the course of their employment — whether created at home, in a café, or in a co-working space — belongs to the Company if it relates to the Company's business.

2.2 Personal Device Usage. If the employee uses a personal device for Company work (whether approved or not), any Company IP created on that device remains the Company's property. The employee must: (a) promptly transfer all such IP to Company systems (repositories, cloud drives, or email); (b) not retain copies on personal devices beyond what is temporarily necessary; and (c) delete all Company IP from personal devices when no longer needed for the immediate work task.

2.3 Blending Personal and Company Work. Employees must maintain clear separation between personal projects and Company work. Any work created using Company Confidential Information, Company systems, or during Company working hours shall be treated as Company IP regardless of the device or location used for its creation.

3. APPROVED DEVICES AND SYSTEMS

3.1 Company-Issued Devices (Preferred). Where possible, employees should use only Company-issued and Company-managed devices for all Company work. Company devices are configured with appropriate security

controls, encryption, and remote wipe capabilities.

3.2 Personal Devices — BYOD Rules. Where the Company permits use of personal devices (Bring Your Own Device), the following rules apply: (a) install and maintain the Company's mobile device management (MDM) profile if required; (b) use only Company-approved applications for work tasks — do not use personal messaging apps, personal cloud drives, or personal email for Company work; (c) enable device encryption and strong PIN/biometric lock; (d) install operating system and security updates promptly; and (e) agree to the Company's right to remotely wipe Company data from the device in the event of loss, theft, or departure from the Company.

3.3 Prohibited Systems. Employees shall not use any of the following for handling Company IP or Confidential Information without prior written approval from IT: personal cloud storage (personal Google Drive, Dropbox, iCloud, or similar); AI tools and services that train on user inputs (unless the Company has a specific enterprise agreement that prevents training); personal email accounts; or any third-party collaboration tools not approved by the IT team.

4. NETWORK SECURITY AND CONFIDENTIAL INFORMATION HANDLING

4.1 VPN Requirement. When accessing Company systems remotely, employees must connect through the Company's VPN at all times. Employees shall not access Company systems, repositories, databases, or confidential files over public WiFi or unsecured networks without an active VPN connection.

4.2 Home Network Security. Employees working from home should ensure: (a) home router firmware is up to date; (b) WiFi network uses WPA2 or WPA3 encryption; (c) the default router admin password has been changed; and (d) IoT devices are on a separate network from the work device where possible.

4.3 Physical Security of Confidential Information. When working remotely, employees must: (a) ensure their screen is not visible to household members, neighbours, or others in shared spaces while viewing confidential data; (b) not leave confidential documents, notebooks, or printed materials in shared or accessible locations in the home; (c) shred printed confidential documents before disposal rather than placing them in general waste; and (d) lock their screen whenever leaving the device unattended, even briefly.

4.4 Video Calls and Screen Sharing. During video calls and screen shares: (a) be aware of what is visible in the background — whiteboards, sticky notes, or other screens displaying confidential information must not be visible; (b) use a virtual background if working in an area where confidential information is visible; and (c) verify all participants on a call are authorised before sharing screens containing confidential data.

5. AI TOOLS AND GENERATIVE AI

5.1 The use of generative AI tools (including large language models, code generation tools, image generation tools, and similar AI services) for Company work is subject to the following rules: (a) do not enter any Confidential Information, source code, customer data, financial data, or other non-public Company information into any AI tool that does not have an enterprise agreement prohibiting training on user inputs; (b) all content generated using AI tools in the course of employment is Company IP; (c) employees must review and verify all AI-generated work product before incorporating it into Company deliverables; and (d) employees must disclose to their manager if they are using AI tools for significant work tasks.

6. SOURCE CODE AND DEVELOPMENT WORK

6.1 All source code, scripts, configurations, and other technical work product created remotely must be: (a) committed to the Company's official version control repository at regular intervals — never left only on local devices for extended periods; (b) not stored in personal GitHub, GitLab, or Bitbucket accounts in any public or private repository; (c) not shared with external parties via personal accounts, email, or messaging apps; and (d) created using only Company-approved development environments and toolchains.

7. INCIDENT REPORTING

7.1 Employees must report immediately to IT and their manager: (a) loss or theft of any device containing Company data; (b) any suspected malware, ransomware, or phishing attack on a device used for Company work; (c) any accidental disclosure of Confidential Information — including sending to the wrong recipient; (d) any unauthorised access to Company systems or data; and (e) any situation where Company data may have been exposed to an unauthorised person.

8. POLICY ADMINISTRATION

Policy Owner	[IT Manager / CISO / HR Head]
Policy Effective Date	[DD Month YYYY]
Review Cycle	Annual or on significant change in remote work arrangements
Approved Remote Work Tools	[List — e.g. Google Workspace / Microsoft 365 / Slack / Zoom / GitHub Enterprise]
VPN Solution	[Name of VPN used by Company]
MDM Solution (if applicable)	[Name of MDM platform]
IT Helpdesk Contact	[Email / phone for IT security queries]

EMPLOYEE ACKNOWLEDGEMENT

I confirm that I have read and understood this Remote Work IP Policy and agree to comply with all its provisions. I understand that my IP obligations to the Company are unchanged by remote work arrangements, and that violations of this Policy may result in disciplinary action.

EMPLOYEE	IT / HR REPRESENTATIVE
[Employee Full Name]	[Name and Designation]
Signature: _____	Signature: _____
Employee ID: _____	Date: _____
Date: _____	

IMPORTANT NOTE

The use of AI tools by employees for Company work raises emerging IP ownership questions under Indian law, as copyright in AI-generated works is not yet settled. This Policy treats AI-generated work product created in the course of employment as Company property. Seek legal advice on AI and IP ownership as this area evolves. Template only — not legal advice.

EMERGING TECHNOLOGIES AND FUTURE WORK ARRANGEMENTS

9.1 Generative AI Tools — Detailed Guidance. The rapid adoption of generative AI tools creates specific IP risks that this Policy addresses directly. When using any AI-powered writing, coding, image generation, or analysis tool for Company work, the employee must: (a) never input proprietary source code, customer data, financial projections, trade secret details, or any other Confidential Information into any AI tool that processes user inputs for model training; (b) treat all AI-generated outputs created in the course of employment as Company property; (c) review AI-generated code for security vulnerabilities, licence compatibility, and accuracy before incorporating into any Company product; (d) disclose to the manager if a significant deliverable was produced primarily by AI tools; and (e) check whether the AI tool's terms of service grant the tool provider any rights over the inputs or outputs.

9.2 Bring Your Own Device (BYOD) — Security Requirements. Employees approved to use personal devices for Company work must ensure their device meets minimum security standards: device encryption enabled (full-disk encryption on laptops, hardware encryption on phones); screen lock activated with PIN, password, or biometrics; automatic lock triggered after no more than [5] minutes of inactivity; remote wipe capability enabled; and up-to-date operating system and security patches. Devices that do not meet these standards must not be used for Company work until compliant. The Company's IT team may conduct periodic security compliance checks on personal devices used for Company work.

9.3 Co-Working Spaces. Employees working from co-working spaces face additional risks: shared printers, shared networks, and shared spaces where screens may be visible. Additional precautions required in co-working spaces include: always using the Company VPN even if the co-working space offers its own WiFi; using a privacy screen filter on laptops; not printing or leaving physical documents at shared printers; and using headphones for all confidential calls. Employees must never discuss confidential business matters in open shared spaces where others can hear.

9.4 International Remote Work. Employees who wish to work remotely from a country other than India for an extended period must obtain prior HR and Legal approval. Extended international remote work may have tax implications (permanent establishment risk, withholding tax obligations), visa and immigration implications, and may affect IP ownership under local law. The Company will assess each such request on a case-by-case basis.