

Tecknuovo Concurrent Engagement & Device Use Policy

Version: 1.0

Effective: June 2026

1. Definitions

BYOD: “Bring Your Own Device”; use of a personally owned device for Tecknuovo work, subject to policy requirements.

Concurrent Engagement: Any situation where a Supplier or Supplier Personnel is engaged in work for Tecknuovo and one or more other customers at the same time.

Device: Any laptop, desktop, tablet, smartphone, or other hardware used to access, process, or store Tecknuovo Information.

General Terms: The General Terms and Conditions for the Supply of Services between Tecknuovo and the Supplier.

Personal Data: Information relating to an identified or identifiable individual, as defined under the UK GDPR and Data Protection Act 2018.

Supplier: Any company, partnership, or individual (including sub-contractors) providing services to Tecknuovo.

Supplier Personnel: Employees, agents, or sub-contractors of the Supplier engaged in Tecknuovo work.

Tecknuovo Information: All data, documents, code, materials, and communications belonging to or provided by Tecknuovo, including confidential and Personal Data.

Tecknuovo-Issued Device: Any Device provided by Tecknuovo for use in delivering services.

2. Introduction & Scope

This Policy applies to all Suppliers and Supplier Personnel (including sub-contractors) performing services for Tecknuovo Ltd (“Tecknuovo”). It sets out mandatory standards for conduct, Device use, and information security, especially for suppliers engaged in multiple customer assignments concurrently. This Policy must be read in conjunction with the Tecknuovo Supplier IT Security Policy, Supplier Use of Device Policy, Privacy Policy, the General Terms and all other relevant contractual terms.

3. Core Principles

- **No Conflict of Interest:** Suppliers must avoid actual, potential, or perceived conflicts that could compromise independence or confidentiality.
- **Performance First:** Concurrent Engagements must not impair the quality, timeliness, or availability of services to Tecknuovo.
- **Strict Segregation:** Work for other customers must be logically and operationally separated from Tecknuovo work (accounts, tools, Devices, sessions, storage).
- **Confidentiality & Data Minimisation:** Access, use, storage, and transmission of Tecknuovo Information must be limited to what is necessary and protected by appropriate controls.
- **Transparency:** Suppliers must disclose all Concurrent Engagements and attest compliance on onboarding and at defined intervals (see attached declaration).

4. Acceptable and Prohibited Conduct

Acceptable Conduct

- Using a dedicated Device for Tecknuovo work, or, if BYOD is permitted, ensuring strict segregation via separate user profiles or approved virtual environments.
- During Tecknuovo meetings or scheduled work, ensuring that no other client meetings, sessions, or collaboration tools are open or running on the same Device or screen.
- Using a private, secure environment for all Tecknuovo work; avoiding public spaces where screen or audio may be exposed.
- Recording Tecknuovo meetings or content is prohibited unless expressly authorised in writing by Tecknuovo.
- Recording time for Tecknuovo only where that time is specifically allocated to Tecknuovo services and is not also being billed or committed to a Concurrent Engagement.

Prohibited Conduct

- Using Tecknuovo-issued Devices for any non-Tecknuovo engagement, project, or personal activity.
- Accessing or referencing other customers' materials while performing Tecknuovo work.
- Cross-pollination of code, architectures, templates, or documentation unless pre-approved and scrubbed of confidential elements.
- Dual screen sharing (Tecknuovo + other client) or having other client meetings/apps active during Tecknuovo meetings.

- Use of personal email, consumer cloud storage, or unapproved tools for Tecknuovo Information.
- Capturing screenshots, notes, or recordings that include other clients' content or identifiers.
- Recording or charging time to Tecknuovo where the same period is also allocated to work, meetings or deliverables for a Concurrent Engagement.

5. Device & Account Controls

- **Tecknuovo-Issued Devices:** Must be used exclusively for Tecknuovo engagements in accordance with the policies referenced in Clause 2. No concurrent sessions or use for other customers.
- **BYOD (if permitted):**
 - Use separate OS user profiles or approved containerisation/virtual desktop.
 - Use distinct Tecknuovo-issued credentials and collaboration tenants.
 - Store Tecknuovo data only in approved locations; no local commingling with other clients' files.
 - Maintain current OS patches, full-disk encryption, endpoint protection, and screen lock ($\leq$ 5 minutes).
 - Use secure networks; VPN when required; prohibit public/open Wi-Fi without secure tunnelling.
 - Comply with Tecknuovo DLP; do not copy/paste or transfer materials between tenants/tools.
 - Removable media is prohibited unless expressly authorised and encrypted.Do not disable Tecknuovo logging/monitoring on Tecknuovo apps and VDI.

6. Disclosure, Reporting & Sanctions

- **Disclosure:** Suppliers must disclose Concurrent Engagements prior to onboarding and update disclosures within 5 business days of any change that could create conflicts or confidentiality risks. Tecknuovo may require mitigations or refuse Concurrent Engagements that create unacceptable risk.
- **Incident Reporting:** Immediate reporting (within 24 hours) of suspected or actual confidentiality breach, cross-tenant data movement, misdirected emails, or observed concurrent-session violations is required. Tecknuovo may require a fact-finding review, temporary suspension of access, Device inspection (subject to privacy laws), and corrective actions.

- **Sanctions:** Any breach of this policy may lead to immediate removal, contract termination, and potential indemnity claims under the General Terms.

7. Data Protection & Legal Compliance

- Suppliers must comply with all contractual confidentiality clauses, relevant legislation including the UK GDPR and Data Protection Act 2018, and applicable sector regulations.
- Suppliers must not transfer Personal Data outside approved locations or processors and must follow Tecknuovo DPIA and security instructions.
- For all data protection and IT security requirements, refer to the Tecknuovo Supplier IT Security Policy and

8. Governance & Attestation

- This Policy forms part of Tecknuovo's onboarding due diligence and ongoing compliance requirements.
- Suppliers must sign the Concurrent Engagement Declaration on onboarding or upon material change (attached).