PARTNERSHIP POLICY & STRATEGIC ALLIANCE GOVERNANCE FRAMEWORK

Place: Kolkata, West Bengal, India
Last Updated: Saturday, 20 December 2025

Legal Nature and Electronic Execution

This Partnership Policy & Strategic Alliance Governance Framework **("Policy")** establishes the enterprise-wide governance architecture governing the identification, evaluation, onboarding, management, monitoring, renewal, suspension, termination, and post-termination oversight of all partnerships entered into by IVY Nest Apartments **("IVY Nest", "Company", "Platform", "Organization").**

This Policy shall be read in conjunction with the Terms of Use, Customer Service and Support Policy, Grievance Redressal Policy, Privacy Policy, Booking and Cancellation Policy, and other applicable IVY Nest Apartments policies. In case of any inconsistency, the Terms of Use shall prevail.

By clicking on the **"I ACCEPT"** or **"ACCEPT & CONTINUE"** button on the electronic interface of the Platform, the User expressly **consents to, acknowledges, and agrees** to be legally bound by the terms of this Policy.

This **Policy is generated by a computer system** and, in accordance with applicable law, **does not require any physical, electronic, or digital signature for validity, binding effect, or enforceability**.

By accessing, browsing, registering on, booking through, or otherwise using the IVY NEST platform, website, mobile application, or services, and by clicking the **"I ACCEPT" / "ACCEPT & CONTINUE"** button, the user expressly **consents to be bound by this Policy**, along with all other applicable platform policies.

Users are advised to carefully read and fully understand all provisions of this Policy before participating. Any continued use of the **IVY NEST digital platform** or availing of any services after accepting this **Policy shall constitute valid, informed, and legally** enforceable consent under applicable law.

If this Policy is **not in a language that the user understands**, the user is required to contact IVY NEST at **grievance@ivynestapartments.com** within **24 (Twenty-Four) hours** of receipt. Failure to do so, coupled with acceptance of this Policy, shall be deemed to constitute **full understanding and informed consent**.

If the User does not agree to any provision contained herein, the User must **immediately discontinue** access to and use of the Platform and refrain from availing any services offered thereunder.

The digital platform is owned by **Ivy Nest Apartments**, operating under the brand name **"IVY NEST"** ("Company", "IVY NEST", "Platform", "we", "us", or "our").
IVY NEST Apartments **operates, controls, and manages** the Platform and the services offered thereon, as defined under applicable policies, terms, and agreements.

IVY Nest Apartments is engaged in the business of providing **residential accommodation and rental solutions** through a **technology-enabled digital platform / online portal** to intending occupiers and/or licensees.

The services offered through the Platform cater to a diverse range of users, including but not limited to:

- Digital nomads
- Remote workers
- Students
- Working professionals
- Community-oriented residents
- Short-term and long-term occupiers

The Platform facilitates access to multiple categories of living and working spaces, including:

- Paying Guest (PG) accommodations
- Rental flats and apartments
- Room-sharing residences
- Hostels
- Co-living spaces
- Co-working spaces
- Workcation stays
- Vacation homes and short-term stays

In addition to accommodation services, IVY NEST operates as a technology-enabled Online Travel Agency (OTA), facilitating access to a wide range of travel and mobility services through authorised third-party service providers and integrated digital platforms.

Subject to availability and applicable terms, the Platform may facilitate:

- Hotel, resort, homestay, vacation home, serviced apartment, hostel, PG, co-living, and rental accommodation bookings.
- Domestic and international flight bookings, including fare comparison and reservation assistance.

- Railway ticket bookings, train search, journey planning, and reservation support.
- Bus bookings across public and private operators.
- Cab, taxi, airport transfer, ride-hailing, and local transportation services.
- ravel-related services such as itinerary planning, business and student travel, workcation solutions, corporate accommodation, holiday packages, destination discovery, and travel assistance.

All travel-related services are facilitated through authorised third-party service providers and remain subject to their respective terms, conditions, availability, and applicable laws.

The Platform acts strictly as a **technology intermediary and facilitator**, and **does not act as a landlord, property owner, broker, or agent**, unless expressly stated otherwise.

The business operates **entirely through electronic and digital means**, ensuring convenience, transparency, and scalability for both short-term and long-term stays.

For the purposes of this Policy, unless the context otherwise requires:

"Platform" means the IVY Nest Apartments website, mobile applications, and all related digital interfaces, collectively.

"User" means any individual, firm, entity, occupier, guest, licensee, or customer registered as an end user/client on the IVY Nest platform.

"Password" means any secret word, phrase, code, passphrase, encryption or decryption key, socket, or authentication credential used to access the Platform or its services.

"Affiliate(s)" means any person, company, corporation, association, or entity that directly or indirectly controls, is controlled by, or is under common control with a Party.
"Control" includes the power to direct management or policies, whether through ownership, contract, or otherwise.

"Applicable Laws" or **"Laws"** include all statutes, enactments, rules, regulations, notifications, guidelines, policies, directions, and orders issued by any competent governmental, statutory, judicial, or regulatory authority, including municipal and local authorities.

"Authorized User" means employees, agents, or permitted individuals of a Customer or Affiliate expressly authorized to access and use the Platform.

"Confidential Information" means all non-public, proprietary, or sensitive information of the Company or its users, including business plans, financial data, software, trade secrets, customer data, marketing strategies, and technical information disclosed in any form.

“Data” includes Personal Data, usage data, images, records, IP addresses, transaction details, user information, supplier information, and all data generated through the execution of this Policy or use of the Platform.

“Effective Date” means the date on which the User accepts this Policy electronically.

“Force Majeure” means any event beyond reasonable control, including acts of God, natural disasters, epidemics, governmental actions, riots, wars, strikes, regulatory changes, or any circumstance rendering performance impracticable.

“Intellectual Property” includes all copyrights, patents, trade secrets, software, designs, business formats, and other proprietary rights developed, used, or licensed in connection with the Platform or services.

“Term” means the duration for which this Policy remains applicable, as defined under the relevant clauses.

“Independent Property” means a self-contained residential unit occupied exclusively by one Licensee or household.

“Visitor” means any person entering the premises upon invitation, permission, or accompaniment of a Resident, including social guests, relatives, friends, or professional visitors.

“Shared Accommodation” means premises where multiple unrelated occupants share common facilities, including hostels, PGs, and co-living spaces.

“Authorized Personnel” means employees, representatives, security staff, or agents appointed by the Licensor or property owner.

The purpose of this Policy is to ensure a **lawful, transparent, fair, and secure tenant induction process** that protects:

- Property owners and licensors
- Existing occupants and community safety
- Platform integrity and compliance obligations
- Public order, safety, and statutory requirements

This Policy aims to balance **risk mitigation**, **legal compliance**, and **non-discriminatory access** while preserving the Platform’s right to **accept, conditionally accept, or reject** any Applicant.

This Policy is drafted and implemented in compliance with:

- **Information Technology Act, 2000** – electronic contracts, records, and intermediary protection
- **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**
- **Digital Personal Data Protection Act, 2025**
    - Lawful purpose and consent
    - Data minimization and security safeguards
    - User rights and grievance redressal
- **Consumer Protection Act, 2019**
- **Consumer Protection (E-Commerce) Rules, 2020 (as amended)**
    - Transparency and disclosure obligations
    - Refunds, cancellations, and grievance handling
- **Indian Contract Act, 1872** – enforceability of electronic agreements
- **Applicable State Rent Control Laws / Model Tenancy Act / Applicable Central, State or Local tenancy, rent control, housing and accommodation laws, as amended from time to time**
- **Local municipal and real estate regulations**, where applicable

This Policy forms a **legally binding and enforceable contract** between Ivy Nest Apartments and the User upon electronic acceptance. The terms herein shall be read harmoniously with the Platform's:

- Terms of Use
- Privacy Policy
- Booking, Cancellation & Refund Policy
- Lease / License Agreements
- Any additional policies published on the Platform

In the event of any conflict, **the more specific policy shall prevail**, subject to Applicable Law.

The primary objectives of this Policy are to:
a. Establish a transparent, accountable, legally compliant, and risk-based partnership ecosystem.
b. Protect the interests of customers, guests, residents, property owners, investors, employees, regulators, and stakeholders.
c. Ensure operational, financial, legal, ethical, cybersecurity, and reputational integrity across all partnership relationships.
d. Create a standardized enterprise governance mechanism for strategic alliances and commercial collaborations.
e. Reduce regulatory, operational, litigation, cyber, fraud, and reputational risks.
f. Promote sustainable, ethical, transparent, and compliant business practices.
g. Strengthen investor confidence and governance maturity.
h. Support scalable expansion across multiple jurisdictions and operational verticals.

i. Enable regulatory readiness and audit preparedness.
j. Preserve brand integrity, customer trust, and platform reliability.
IVY Nest adopts a "Trust Through Verification" model whereby all partnerships shall be established, monitored, and governed through documented due diligence, risk assessment, contractual safeguards, continuous compliance oversight, and periodic review mechanisms.

1. SCOPE

1.1 Coverage

This Policy applies to all commercial, operational, strategic, technology, marketing, distribution, franchise, affiliate, vendor, property-owner, mobility, hospitality, real-estate, workforce-related and ecosystem partnerships.

1.2 Business Activities Covered

The Policy governs partnerships relating to:

a. Residential property management.

b. Paying guest accommodations.

c. Hostels and student housing.

d. Co-living operations.

e. Co-working operations.

f. Vacation rentals.

g. Workation facilities.

h. Managed properties.

i. Hospitality services.

j. OTA distribution.

k. Accommodation aggregation.

l. Property marketplace operations.

m. Corporate housing.

n. Travel and tourism operations.

o. Transportation booking facilitation.

p. Airline partnerships.

q. Rail booking integrations.

r. Cab and mobility integrations.

s. Technology integrations.

t. SaaS partnerships.

u. API integrations.

v. Strategic alliances.

w. Franchise systems.

x. Affiliate marketing.

y. Referral programs.

z. International collaborations.

1.3 Lifecycle Coverage

The Policy applies throughout the entire partnership lifecycle, including:

a. Identification.

b. Screening.

c. Due diligence.

d. Approval.

e. Contracting.

f. Onboarding.

g. Monitoring.

h. Audit.

i. Renewal.

j. Suspension.

k. Termination.

l. Post-termination obligations.

2. APPLICABILITY

2.1 Internal Applicability

This Policy applies to:

a. Board of Directors, Designated Partners, Managing Partners, Governing Body, or equivalent governing authority, as applicable.

b. Compliance Committee.

c. Executive Management.

d. Legal Department.

e. Finance Department.

f. HR Department.

g. Operations Department.

h. Procurement Teams.

i. Technology Teams.

j. Cybersecurity Teams.

k. Business Development Teams.

l. Franchise Management Teams.

m. Property Acquisition Teams.

n. Regional and State Management Teams.

o. Consultants acting on behalf of IVY Nest.

2.2 External Applicability

This Policy applies to:

a. Property owners.

b. Franchisees.

c. Vendors.

d. Contractors.

e. Subcontractors.

f. Referral partners.

g. Strategic alliance partners.

h. Technology partners.

i. API partners.

j. SaaS providers.

k. Marketing agencies.

l. Influencers.

m. Corporate clients.

n. Travel partners.

o. Mobility providers.

p. Hospitality operators.

q. Channel distribution partners.

r. Any third party representing IVY Nest.

3. LEGAL & REGULATORY BASIS

3.1 Foundational Laws

This Policy shall be interpreted and implemented in accordance with applicable laws including but not limited to:

a. Companies Act, 2013.

b. Indian Contract Act, 1872.

c. Specific Relief Act, 1963.

d. Limited Liability Partnership Act, 2008.

e. Partnership Act, 1932.

f. Consumer Protection Act, 2019.

g. Competition Act, 2002.

h. Information Technology Act, 2000.

i. Arbitration and Conciliation Act, 1996.

j. Bharatiya Nyaya Sanhita.

k. Bharatiya Nagarik Suraksha Sanhita.

l. Bharatiya Sakshya Adhiniyam.

3.2 Data & Cyber Governance

This Policy shall further align with:

a. Digital Personal Data Protection Act, 2025.

b. CERT-In Directions.

c. Information Technology Rules.

d. Applicable cybersecurity advisories.

e. Data localization requirements where applicable.

3.3 Labour & Workforce Governance

All partnership arrangements shall comply with:

a. Code on Wages, 2019.

b. Industrial Relations Code, 2020.

c. Code on Social Security, 2020.

d. Occupational Safety, Health and Working Conditions Code, 2020.

e. POSH Act, 2013.

f. Contract Labour (Regulation and Abolition) Act, 1970.

g. Inter-State Migrant Workmen Act, 1979.

h. Shops and Establishments legislation.

i. EPF and ESI laws.

3.4 Hospitality & Property Compliance

Applicable state and local requirements including:

a. Municipal licensing.

b. Fire safety compliance.

c. Tourism registrations.

d. Building occupancy requirements.

e. Public accommodation standards.

f. Local housing regulations.

4. DEFINITIONS

4.1 "Partner"

Means any external individual, natural person, legal entity, organization, body corporate, company, limited liability partnership, partnership firm, trust, society, association of persons, government or quasi-government entity, property owner, licensor, lessor, franchisee, franchise applicant, vendor, supplier, contractor, subcontractor, consultant, advisor, agent, intermediary, broker, channel partner, referral partner, affiliate, reseller, distributor, marketplace participant, accommodation provider, managed property operator, technology provider, cloud service provider, payment service provider, API provider, software provider, data processor, strategic alliance participant, joint venture participant, investor, lender, insurer, mobility provider, travel partner, hospitality operator, marketing agency, influencer, content creator, or any other third party that directly or indirectly provides goods, services, technology, infrastructure, data, funding, operational support, commercial collaboration, or otherwise enters into any contractual, commercial, operational, strategic, financial, technological, marketing, licensing, franchising, outsourcing, procurement, or business relationship with, or on behalf of, IVY Nest.

4.2 "Beneficial Owner"

Means the natural person(s) who ultimately owns, controls, or significantly influences a legal entity.

4.3 "Partnership"

Means any formal or informal commercial relationship involving exchange of services, revenue, technology, property, data, resources, branding, operational support, or strategic cooperation.

4.4 "High-Risk Partner"

Means a partner classified as high risk based upon legal, financial, regulatory, cybersecurity, reputational, operational, or geopolitical considerations.

4.5 "Sensitive Data"

Includes personal data, financial information, identity records, proprietary business information, operational intelligence, cybersecurity information, trade secrets, and confidential platform data.

4.6 "Compliance Event"

Means any actual or suspected breach of law, contract, regulation, policy, code of conduct, cybersecurity obligation, labour requirement, or ethical standard.

4.7 "Critical Incident"

Means an event causing significant legal, financial, operational, safety, cybersecurity, or reputational harm.

4.8 Material Breach

Material Breach means any act, omission, failure, misconduct, negligence, misrepresentation, non-compliance, or other circumstance that materially impairs or is reasonably likely to impair the rights, interests, assets, operations, security, reputation, regulatory compliance, contractual obligations, financial position, guests, customers, business continuity, or legitimate commercial interests of IVY Nest.

A Material Breach may include, without limitation:

a. Fraud, corruption, bribery, money laundering, financial crime, or other unlawful conduct.

b. Deliberate or repeated violation of applicable laws, regulations, contractual obligations, or this Policy.

c. Unauthorized disclosure, misuse, alteration, destruction, or compromise of confidential information, personal data, intellectual property, or proprietary business information.

d. Material cybersecurity incidents, unauthorized system access, ransomware attacks, malware infections, data breaches, or other information security failures.

e. Submission of false declarations, forged documents, misleading representations, concealment of material facts, or fraudulent certifications.

f. Repeated operational failures, serious service deficiencies, guest safety violations, or persistent non-performance.

g. Sanctions violations, export control violations, financial crime, regulatory enforcement actions, or significant compliance failures.

h. Any other act or omission which IVY Nest reasonably determines may materially expose the organization to legal, financial, operational, regulatory, reputational, cybersecurity, or strategic risk.

4.9 Material Non-Compliance

Material Non-Compliance means any significant failure to comply with applicable law, contractual obligations, internal policies, regulatory requirements, industry standards, or governance obligations that may expose IVY Nest to legal liability, regulatory enforcement, financial loss, reputational harm, operational disruption, or other significant adverse consequences.

Material Non-Compliance may arise from a single serious incident or repeated instances of non-compliance demonstrating a pattern of unacceptable conduct.

4.10 High-Risk Transaction

High-Risk Transaction means any proposed or existing transaction, arrangement, partnership, activity, or commercial relationship which, following a documented risk assessment, is reasonably determined to present elevated legal, regulatory, operational, financial, cybersecurity, data protection, fraud, sanctions, geopolitical, reputational, environmental, social, governance (ESG), or strategic risks requiring enhanced due diligence and higher-level approval.

Risk factors may include, without limitation:

a. High transaction value.

b. Cross-border or international operations.

c. Processing of sensitive personal data or confidential information.

d. Artificial Intelligence, cloud computing, cybersecurity, or critical technology services.

e. Government contracts or regulated industries.

f. Politically Exposed Persons (PEPs).

g. Jurisdictions presenting elevated corruption, sanctions, geopolitical, financial crime, or regulatory risks.

h. Significant public visibility or potential reputational impact.

4.11 Reputational Harm

Reputational Harm means any actual or reasonably foreseeable adverse effect on the credibility, goodwill, public confidence, commercial standing, stakeholder trust, market perception, investor confidence, customer relationships, regulatory relationships, or brand value of IVY Nest arising from acts, omissions, misconduct, regulatory action, adverse publicity, litigation, unethical conduct, operational failures, cybersecurity incidents, financial irregularities, or any other material event.

The determination of reputational harm shall be based upon objective evidence, documented risk assessments, publicly available information, regulatory findings, commercially recognized compliance intelligence, media reporting, or other reliable sources.

4.12 Related Party

Related Party means any individual or entity having a direct or indirect relationship with a Partner, employee, director, designated partner, key managerial personnel, shareholder, beneficial owner, consultant, contractor, or other person associated with IVY Nest, including:

a. Immediate family members.

b. Spouse or domestic partner.

c. Parents, children, siblings, or dependent relatives.

d. Entities under common ownership or common control.

e. Holding companies, subsidiaries, associates, joint ventures, affiliates, or controlled entities.

f. Persons exercising significant influence over management or financial decisions.

g. Beneficial owners or ultimate beneficial owners.

h. Any other relationship that may reasonably influence objective decision-making or create an actual, potential, or perceived conflict of interest.

4.13 Conflict of Interest

Conflict of Interest means any actual, potential, or perceived situation in which a person's personal, financial, professional, family, political, business, fiduciary, or other private interests may improperly influence, appear to influence, or reasonably be perceived as influencing the impartial, objective, or independent performance of their duties, responsibilities, or decision-making on behalf of IVY Nest.

4.14 Regulatory Action

Regulatory Action means any investigation, inspection, inquiry, audit, notice, direction, advisory, order, suspension, penalty, prosecution, enforcement proceeding, licence restriction, compliance review, or other action initiated by any competent governmental, statutory, judicial, regulatory, municipal, law enforcement, taxation, or administrative authority.

4.15 Regulatory Inspection

Regulatory Inspection means any announced or unannounced inspection, verification, audit, compliance review, examination, survey, evidence collection exercise, or other official inspection conducted by any competent governmental, statutory, judicial, regulatory, municipal, taxation, or law enforcement authority.

4.16 Controlled Technology

Controlled Technology means any technology, software, hardware, encryption product, artificial intelligence system, digital platform, technical information, source code, algorithm, technical data, design specification, or other technology that is subject to export control laws, strategic trade controls, licensing requirements, or other legal restrictions under applicable law.

4.17 Restricted Information

Restricted Information means information classified by IVY Nest as requiring the highest level of confidentiality and protection due to its strategic, legal, commercial, cybersecurity, regulatory, operational, or financial sensitivity, including but not limited to encryption keys, authentication credentials, source code, security architecture, vulnerability assessments, confidential investigations, merger and acquisition information, privileged legal communications, cryptographic materials, disaster recovery documentation, and other information designated as Restricted or Highly Restricted under IVY Nest's Information Classification Framework.

4.18 Critical Infrastructure

Critical Infrastructure means any physical or digital infrastructure, system, platform, application, cloud environment, network, communications system, payment infrastructure, identity management system, cybersecurity infrastructure, booking platform, property management system, API infrastructure, data processing environment, or other essential business asset whose compromise, disruption, or unavailability could materially affect IVY

Nest's business continuity, regulatory compliance, security, operations, financial stability, guest services, or public confidence.

4.19 Governing Authority

Governing Authority means the Board of Directors, Designated Partners, Managing Partners, Proprietor, Governing Body, Management Committee, Executive Committee, or any other duly authorized governing or decision-making authority of IVY Nest, as applicable to its legal structure and organizational form.

4.20 Approval Authority

Approval Authority means the individual, committee, governing authority, or other authorized person empowered to approve, reject, review, escalate, suspend, terminate, or otherwise decide matters under this Policy in accordance with the applicable Delegation of Authority Matrix, internal governance framework, contractual arrangements, or applicable law.

4.21 Enterprise Risk Appetite

Enterprise Risk Appetite means the level and type of legal, financial, operational, cybersecurity, regulatory, strategic, commercial, environmental, social, governance, and reputational risk that IVY Nest is willing to accept in pursuit of its legitimate business objectives, as determined by the applicable Governing Authority and documented enterprise risk management framework.

4.22 Force Majeure Event

Force Majeure Event means any event or circumstance beyond the reasonable control of the affected party, including natural disasters, epidemics, pandemics, war, terrorism, civil unrest, governmental restrictions, cyber warfare, widespread technology failures, utility disruptions, labour disturbances, or other events materially affecting the ability to perform contractual obligations, subject to applicable contractual provisions and governing law.

Interpretation of Definitions

Unless the context otherwise requires:

a. Definitions shall be interpreted broadly to promote effective corporate governance, regulatory compliance, enterprise risk management, business continuity, and protection of IVY Nest's legitimate commercial interests.

b. The use of the terms "including", "includes", "such as", or similar expressions shall be construed as illustrative and not exhaustive.

c. Where any defined term is not expressly addressed in this Policy, it shall be interpreted in accordance with applicable law, recognized industry practice, accepted corporate governance principles, and the legitimate business objectives of IVY Nest.

5. PARTNERSHIP GOVERNANCE PRINCIPLES

5.1 Core Governance Standards

All partnerships shall be governed by:

a. Legality.

b. Transparency.

c. Accountability.

d. Integrity.

e. Fair dealing.

f. Consumer protection.

g. Worker protection.

h. Data protection.

i. Cybersecurity resilience.

j. Ethical conduct.

k. Sustainability.

l. Risk management.

5.2 Zero-Tolerance Principles

IVY Nest maintains zero tolerance toward:

a. Fraud.

b. Corruption.

c. Bribery.

d. Money laundering.

e. Human trafficking.

f. Forced labour.

g. Child labour.

h. Wage theft.

i. Data misuse.

j. Cybercrime.

k. Identity fraud.

l. Brand misrepresentation.

m. Revenue concealment.

n. Regulatory evasion.

5.3 Enterprise Risk Appetite

The clause should state that IVY Nest ordinarily accepts only Low and Moderate Risk partnerships and that High or Critical Risk partnerships require enhanced due diligence and approval by the appropriate governing authority, with Critical Risk partnerships generally avoided unless justified by compelling strategic reasons and approved at the highest governance level.

5.4 Establishment of Governance Committees

IVY Nest may establish one or more Governance Committees, Compliance Committees, Risk Management Committees, Ethics Committees, Cybersecurity Committees, Data Protection Committees, or other oversight bodies, either on a permanent or ad hoc basis, to supervise implementation of this Policy. Such committees may exercise powers delegated by the applicable governing authority in accordance with internal governance requirements.

6. TYPES OF PARTNERSHIPS COVERED

6.1 Property Owner Partnerships

Owners listing or operating accommodations through IVY Nest.

6.2 Franchise Partnerships

Entities authorized to operate under IVY Nest branding.

6.3 Strategic Business Alliances

Commercial expansion, distribution, or growth partnerships.

6.4 OTA Distribution Partnerships

Distribution and inventory-sharing relationships.

6.5 Channel Partner Relationships

Third-party booking and distribution channels.

6.6 Referral Partnerships

Lead generation and customer acquisition arrangements.

6.7 Technology Integration Partnerships

Technology, software, API and infrastructure collaborations.

6.8 SaaS Partnerships

Software service providers and platform integrations.

6.9 Vendor Partnerships

Operational and support service providers.

6.10 Managed Property Partnerships

Properties operated under IVY Nest operational standards.

6.11 Corporate Housing Partnerships

Enterprise accommodation arrangements.

6.12 Travel & Tourism Alliances

Travel and hospitality ecosystem relationships.

6.13 Mobility Partnerships

Airlines, rail, bus, taxi and transportation facilitators.

6.14 Co-working & Co-living Alliances

Shared infrastructure and occupancy collaborations.

6.15 Affiliate & Influencer Partnerships

Marketing, promotional and brand engagement relationships.

6.16 Joint Venture Partnerships

Strategic growth and expansion structures.

6.17 International Partnerships

Cross-border strategic collaborations.

7. ELIGIBILITY & QUALIFICATION STANDARDS

7.1 General Eligibility

All prospective partners must:

a. Possess legal capacity.

b. Hold required registrations.

c. Maintain lawful operations.

d. Demonstrate financial stability.

e. Demonstrate ethical conduct.

f. Pass due diligence reviews.

g. Satisfy compliance screening.

7.2 Disqualification Grounds

IVY Nest may reject any partner that:

a. Has pending serious criminal proceedings.

b. Appears on sanctions lists.

c. Has been blacklisted.

d. Has history of consumer fraud.

e. Has repeated labour violations.

f. Has unresolved cybersecurity incidents.

g. Has material regulatory violations.

h. Has history of brand abuse.

i. Has materially misrepresented information.

j. Is associated with organized criminal activity.

8. PARTNER DUE DILIGENCE FRAMEWORK

8.1 Mandatory Due Diligence

No partnership shall commence without documented due diligence.

8.2 Due Diligence Components

The due diligence review shall include:

a. Legal verification.

b. Corporate verification.

c. Financial assessment.

d. Litigation screening.

e. Regulatory screening.

f. Beneficial ownership review.

g. GST verification.

h. Tax compliance verification.

i. Cybersecurity assessment.

j. Property verification.

k. Reputational review.

l. Workforce compliance assessment.

m. ESG assessment.

n. Sanctions screening.

8.3 Risk-Based Approach

The extent of due diligence shall be proportionate to:

a. Transaction value.

b. Data access level.

c. Geographic risk.

d. Regulatory exposure.

e. Brand impact.

f. Customer impact.

g. Operational dependency.

9. KYC & BENEFICIAL OWNERSHIP VERIFICATION

9.1 Mandatory Verification

All partners shall undergo KYC verification prior to onboarding.

9.2 Verification Requirements

Where applicable, IVY Nest may require:

a. PAN.

b. GST Registration.

c. TAN.

d. Certificate of Incorporation.

e. LLP Registration.

f. Partnership Deed.

g. Udyam Registration.

h. Trade License.

i. FSSAI License.

j. Professional Tax Registration.

k. Shop Establishment Registration.

l. Bank Verification.

m. Utility Address Verification.

9.3 Beneficial Ownership Disclosure

Partners shall disclose:

a. Ultimate beneficial owners.

b. Shareholding structure.

c. Control rights.

d. Voting rights.

e. Parent entities.

f. Related parties.

g. Politically exposed persons.

9.4 Ongoing Obligation

Partners shall notify IVY Nest within thirty (30) days of any material ownership or control change.

10. LITIGATION & REGULATORY SCREENING PROCEDURES

10.1 Screening Requirements

All prospective partners shall be screened for:

a. Civil litigation.

b. Criminal proceedings.

c. Regulatory actions.

d. Consumer disputes.

e. Insolvency proceedings.

f. Tax enforcement actions.

g. Labour disputes.

h. Environmental violations.

i. Cybersecurity enforcement actions.

10.2 Sources

IVY Nest may utilize:

a. Court databases.

b. Tribunal databases.

c. Regulatory records.

d. Public filings.

e. News reports.

f. Commercial intelligence providers.

g. Compliance screening platforms.

10.3 Enhanced Screening

Enhanced reviews shall be conducted for:

a. High-value partners.

b. Strategic alliances.

c. International partners.

d. Franchise partners.

e. Data-processing partners.

10.4 International Sanctions & Trade Compliance

10.4.1 Compliance Commitment

Where applicable to the nature, scope, location, value, counterparties, subject matter, or jurisdiction of a proposed or existing partnership, IVY Nest and its Partners shall comply with all applicable international sanctions regimes, export control laws, international trade restrictions, customs laws, economic embargoes, anti-boycott requirements, strategic trade controls, and other applicable cross-border legal and regulatory obligations imposed by competent governmental, statutory, judicial, regulatory, or intergovernmental authorities.

Compliance obligations shall extend to all international business activities, cross-border commercial relationships, technology transfers, digital services, financial transactions, logistics operations, procurement activities, licensing arrangements, strategic alliances, and any other activities that may be subject to applicable international trade or sanctions regulations.

10.4.2 Risk-Based Screening

Prior to onboarding, renewing, materially modifying, or expanding any international or cross-border partnership, IVY Nest may conduct sanctions, export control, and international trade compliance screening proportionate to the nature, value, strategic significance, regulatory exposure, geographic risk, operational dependency, data sensitivity, and reputational impact of the proposed relationship.

Such screening may include verification of the Partner, its beneficial owners, directors, key management personnel, affiliates, parent entities, subsidiaries, subcontractors, intermediaries, distributors, logistics providers, agents, and any other relevant counterparties participating in the proposed partnership.

10.4.3 Enhanced Due Diligence

Enhanced due diligence may be undertaken where a prospective or existing Partner:

a. Operates within, conducts business with, or maintains commercial relationships involving jurisdictions presenting elevated geopolitical, sanctions, regulatory, financial crime, cybersecurity, export control, or international trade risks.

b. Engages in cross-border transactions involving sensitive technologies, controlled software, encryption technologies, strategic infrastructure, financial services, cloud computing services, artificial intelligence systems, regulated digital platforms, or other regulated goods or services.

c. Is involved in international payments, cross-border financing, international procurement, technology licensing, data transfers, or strategic commercial alliances.

d. Has been subject to sanctions-related investigations, export control proceedings, customs enforcement actions, trade compliance investigations, regulatory proceedings, or material adverse compliance findings.

e. Is identified through risk assessments, publicly available governmental information, regulatory advisories, intergovernmental publications, or commercially recognized compliance intelligence sources as presenting elevated legal, financial, operational, reputational, or compliance risks.

10.4.4 Restricted Goods, Technologies and End-Use Controls

Where applicable, Partners shall not directly or indirectly involve IVY Nest in transactions concerning prohibited, restricted, or controlled goods, technologies, software, technical data, digital products, services, or intellectual property except in full compliance with applicable laws.

Partners shall exercise reasonable diligence regarding:

a. End-user verification.

b. End-use verification.

c. Destination verification.

d. Ultimate beneficial ownership.

e. Transshipment risks.

f. Diversion risks.

g. Strategic technology controls.

h. Controlled software and encryption technologies.

10.4.5 Supply Chain Compliance

Partners shall exercise reasonable due diligence over their subcontractors, suppliers, affiliates, distributors, logistics providers, intermediaries, consultants, agents, and other third parties participating in activities connected with the partnership.

Where appropriate, Partners shall implement reasonable measures to identify and mitigate indirect sanctions exposure, prohibited transactions, supply chain trade compliance risks, export control violations, or other material regulatory concerns arising through third-party relationships.

10.4.6 Ongoing Notification Obligations

Partners shall promptly notify IVY Nest of any circumstance that may materially affect their legal eligibility or compliance status, including but not limited to:

a. Sanctions designation.

b. Export control restrictions.

c. International trade investigations.

d. Customs enforcement proceedings.

e. Government-imposed restrictions.

f. Economic embargoes.

g. Material regulatory investigations.

h. Placement on prohibited, debarred, or restricted-party lists.

i. Material changes affecting international business operations.

10.4.7 Record Retention and Cooperation

Partners shall maintain complete and accurate records relating to sanctions screening, export control compliance, trade compliance assessments, declarations, certifications, customs documentation, licences, approvals, and related due diligence documentation for the period prescribed by applicable law, contract, regulatory requirement, or legal hold.

Partners shall fully cooperate with lawful regulatory inquiries, audits, investigations, voluntary disclosures where legally required, and other compliance activities relating to international trade or sanctions matters.

10.4.8 Cross-Border Financial Transactions

Where applicable, international payments, financial transfers, foreign exchange transactions, and cross-border commercial settlements relating to the partnership shall comply with applicable sanctions laws, anti-money laundering requirements, counter-terrorist financing obligations, export control requirements, international trade restrictions, and other applicable financial crime prevention laws.

10.4.9 Right to Suspend, Restrict or Terminate

Where IVY Nest reasonably believes, based upon documented risk assessment, governmental advisories, regulatory guidance, publicly available enforcement information, or commercially recognized compliance intelligence, that continuation of a partnership may expose IVY Nest to sanctions violations, export control breaches, international trade restrictions, financial crime risks, regulatory enforcement, or material legal, operational, cybersecurity, or reputational harm, IVY Nest may, subject to applicable law and contractual rights:

a. Conduct enhanced due diligence.

b. Require additional information or certifications.

c. Impose enhanced monitoring.

d. Suspend or restrict the partnership.

e. Refuse or delay proposed transactions.

f. Require corrective action plans.

g. Terminate the partnership.

h. Exercise any other contractual or legal remedy available under this Policy or applicable law.

11. FINANCIAL INTEGRITY & CREDITWORTHINESS ASSESSMENT

11.1 Assessment Criteria

Partners may be evaluated based upon:

a. Audited financial statements.

b. Bank references.

c. Credit history.

d. Cash flow stability.

e. Tax compliance.

f. Debt exposure.

g. Solvency indicators.

h. Business continuity capacity.

11.2 Financial Red Flags

The following may trigger enhanced review:

a. Repeated defaults.

b. Insolvency risks.

c. Significant tax liabilities.

d. Fraud allegations.

e. Revenue concealment indicators.

f. Regulatory penalties.

12. BACKGROUND VERIFICATION REQUIREMENTS

12.1 Verification Scope

IVY Nest may conduct:

a. Identity verification.

b. Address verification.

c. Corporate verification.

d. Director verification.

e. Key management verification.

f. Employment verification.

g. Criminal background checks.

h. Reference checks.

12.2 Continuous Monitoring

Verification may be repeated periodically throughout the relationship lifecycle.

13. ANTI-BRIBERY & ANTI-CORRUPTION OBLIGATIONS

13.1 Prohibition

Partners shall not directly or indirectly:

a. Offer bribes.

b. Solicit bribes.

c. Facilitate unlawful payments.

d. Provide kickbacks.

e. Offer improper gifts.

f. Influence officials unlawfully.

13.2 Books & Records

Partners shall maintain accurate records reflecting all transactions.

13.3 Cooperation

Partners shall fully cooperate with investigations relating to corruption concerns.

14. CONFLICT OF INTEREST DISCLOSURE OBLIGATIONS

14.1 Disclosure Duty

Partners shall disclose actual, potential, or perceived conflicts of interest.

14.2 Examples

Conflicts may include:

a. Family relationships.

b. Ownership interests.

c. Vendor influence.

d. Employment relationships.

e. Competitive affiliations.

f. Undisclosed commissions.

14.3 Ongoing Obligation

Conflicts shall be disclosed immediately upon becoming known.

14.4 Conflict of Interest Register

14.4.1 Establishment of Register

IVY Nest may establish and maintain a formal Conflict of Interest Register to identify, record, monitor, review, manage, and resolve all disclosed, identified, potential, perceived, and actual conflicts of interest arising in connection with partnerships, strategic alliances, procurement activities, commercial transactions, governance matters, regulatory interactions, or any other business activities governed by this Policy.

The Register shall support transparency, accountability, ethical decision-making, enterprise risk management, regulatory compliance, and protection of IVY Nest's legitimate commercial interests.

14.4.2 Persons Required to Disclose

The obligation to disclose conflicts shall apply, where applicable, to:

a. Partners.

b. Strategic alliance participants.

c. Vendors and service providers.

d. Directors, Designated Partners, Managing Partners, Proprietor, or other members of the Governing Authority.

e. Employees.

f. Consultants and advisors.

g. Contractors.

h. Agents, representatives, intermediaries, and distributors.

i. Any other individual or entity participating in activities governed by this Policy.

14.4.3 Register Contents

The Conflict of Interest Register may include, without limitation:

a. Name of the individual or entity making the disclosure.

b. Date of disclosure.

c. Nature and description of the conflict.

d. Whether the conflict is actual, potential, or perceived.

e. Persons or entities involved.

f. Related Party relationships, where applicable.

g. Business unit or project affected.

h. Risk assessment and materiality determination.

i. Mitigation measures implemented.

j. Approval or review authority.

k. Decisions taken.

l. Monitoring requirements.

m. Date of closure or resolution.

14.4.4 Management of Conflicts

Upon identification of a conflict, IVY Nest may implement one or more mitigation measures, including:

a. Enhanced supervision.

b. Independent review.

c. Recusal from discussions or decision-making.

d. Restriction of access to confidential information.

e. Independent commercial evaluation.

f. Appointment of an alternate decision-maker.

g. Enhanced contractual safeguards.

h. Additional monitoring or audit.

i. Termination or restructuring of the relevant arrangement where necessary.

14.4.5 Periodic Review

The Conflict of Interest Register may be reviewed periodically by the appropriate Approval Authority, Compliance Committee, Risk Management Committee, Governing Authority, or other authorized oversight body, where constituted, to ensure continuing compliance with this Policy and applicable governance requirements.

14.4.6 Failure to Disclose

Failure to disclose an actual, potential, or perceived conflict of interest, submission of misleading information, concealment of material facts, or deliberate circumvention of this Clause may constitute Material Non-Compliance or a Material Breach and may result in disciplinary action, suspension, termination of partnership, contractual remedies, recovery of losses, regulatory reporting where legally required, or any other action permitted under applicable law or contract.

14.5 Related Party Transaction Governance

14.5.1 Policy Objective

IVY Nest is committed to ensuring that all Related Party Transactions are conducted with integrity, transparency, fairness, commercial reasonableness, and in the best interests of the organization.

All Related Party Transactions shall be subject to appropriate governance, disclosure, review, approval, monitoring, and documentation requirements.

14.5.2 Identification of Related Parties

Partners and all relevant persons shall promptly disclose any existing or proposed relationship that may constitute a Related Party relationship as defined under Clause 4 of this Policy or applicable law.

IVY Nest may require declarations, supporting documentation, beneficial ownership information, organizational charts, or other evidence necessary to verify Related Party relationships.

14.5.3 Disclosure Requirement

No Related Party Transaction shall be entered into unless:

a. The relationship has been fully disclosed.

b. The commercial terms have been independently evaluated.

c. The transaction has undergone an appropriate conflict assessment.

d. The required approvals have been obtained in accordance with the Delegation of Authority Matrix and this Policy.

14.5.4 Arm's-Length Principle

All Related Party Transactions shall, wherever reasonably practicable, be undertaken on an arm's-length basis and on terms that are fair, reasonable, commercially justifiable, and comparable to those available between independent parties under similar circumstances.

14.5.5 Independent Review

Where a Related Party Transaction presents elevated legal, financial, governance, reputational, regulatory, or strategic risks, IVY Nest may require:

a. Independent commercial evaluation.

b. Legal review.

c. Compliance review.

d. Financial assessment.

e. Risk assessment.

f. Independent pricing analysis.

g. External expert opinion, where appropriate.

14.5.6 Participation Restrictions

Any person having an actual, potential, or perceived interest in a Related Party Transaction shall not participate in the review, evaluation, recommendation, negotiation, approval, monitoring, or decision-making process relating to that transaction except to the extent necessary to provide factual information or as otherwise permitted by applicable law.

14.5.7 Register of Related Party Transactions

IVY Nest may maintain a Related Party Transaction Register containing:

a. Identity of the Related Party.

b. Nature of the relationship.

c. Description of the transaction.

d. Commercial value.

e. Approval Authority.

f. Supporting documentation.

g. Conflict mitigation measures.

h. Dates of approval.

i. Periodic review status.

j. Completion, renewal, modification, or termination details.

14.5.8 Ongoing Monitoring

Related Party Transactions may be periodically reviewed to ensure:

a. Continued commercial justification.

b. Ongoing compliance with this Policy.

c. Continued arm's-length pricing.

d. Compliance with contractual obligations.

e. Absence of undisclosed conflicts.

f. Continued alignment with IVY Nest's governance framework.

14.5.9 Material Non-Compliance

Failure to disclose a Related Party relationship, concealment of material information, submission of false declarations, circumvention of approval requirements, manipulation of pricing, preferential treatment without authorization, or any attempt to improperly influence decision-making may constitute a Material Breach and may result in suspension, termination, contractual remedies, recovery of losses, blacklisting, regulatory reporting where legally required, or any other remedy available under applicable law or contract.

14.5.10 Record Retention

Records relating to Related Party disclosures, approvals, evaluations, declarations, commercial assessments, conflict reviews, supporting documentation, and monitoring activities shall be retained in accordance with IVY Nest's Record Retention Policy, Legal Hold requirements, applicable law, and regulatory obligations.

15. PARTNERSHIP APPROVAL WORKFLOW

15.1 Approval Requirement

No partnership shall become effective without formal approval.

15.2 Approval Stages

a. Business Sponsorship.

b. Compliance Review.

c. Legal Review.

d. Financial Review.

e. Risk Assessment.

f. Executive Approval.

g. Contract Execution.

h. Onboarding Authorization.

15.3 Escalation

High-risk partnerships shall require enhanced executive and compliance committee review.

15.4 Approval Authority Matrix

The approval authority for partnerships shall be determined having regard to factors including:

a. Financial value.

b. Strategic importance.

c. Regulatory exposure.

d. Data access.

e. Brand impact.

f. Operational dependency.

g. Cross-border implications.

h. Risk classification.

Depending upon the nature and risk of the proposed partnership, approval may be granted by the appropriate operational authority, department head, executive management, designated governing authority, or other authorized approval authority in accordance with IVY Nest's Delegation of Authority Matrix.

16. RISK CLASSIFICATION MATRIX

16.1 Risk Categories

Partners shall be classified as:

a. Low Risk.

b. Moderate Risk.

c. High Risk.

d. Critical Risk.

16.2 Assessment Factors

Classification may consider:

a. Financial exposure.

b. Brand exposure.

c. Data access.

d. Regulatory risk.

e. Cybersecurity maturity.

f. Geographic exposure.

g. Operational dependency.

h. Litigation profile.

16.3 Monitoring Frequency

Low Risk – Annual Review

Moderate Risk – Semi-Annual Review

High Risk – Quarterly Review

Critical Risk – Continuous Monitoring

17. COMMERCIAL TERMS GOVERNANCE

17.1 Written Agreements

All partnerships shall be governed by written agreements.

17.2 Mandatory Clauses

Agreements shall include:

a. Scope.

b. Pricing.

c. Payment terms.

d. Compliance obligations.

e. Audit rights.

f. Confidentiality.

g. Data protection.

h. Cybersecurity obligations.

i. Indemnities.

j. Termination rights.

k. Dispute resolution.

17.3 Unauthorized Commitments

No partner may bind IVY Nest without written authorization.

18. REVENUE SHARING GOVERNANCE

18.1 Transparency Requirement

All revenue-sharing arrangements shall be transparent, documented, auditable, and contractually approved.

18.2 Revenue Reporting

Partners shall provide accurate and complete revenue reporting.

18.3 Auditability

IVY Nest reserves the right to verify revenue calculations and supporting records.

18.4 Concealment

Revenue concealment shall constitute a material breach.

19. COMMISSION & INCENTIVE GOVERNANCE

19.1 Governance Principles

Commissions and incentives shall:

a. Be lawful.

b. Be documented.

c. Be auditable.

d. Be transparent.

e. Avoid conflicts of interest.

19.2 Prohibited Practices

The following are prohibited:

a. Undisclosed commissions.

b. Secret rebates.

c. Kickbacks.

d. Improper incentives.

e. Fraudulent claims.

f. Manipulated bookings.

g. Artificial transaction generation.

19.3 Recovery Rights

IVY Nest may recover improperly paid commissions, incentives, rebates, credits, or benefits.

20. PROPERTY VERIFICATION & QUALITY ASSURANCE STANDARDS

20.1 Mandatory Verification Requirement

No accommodation, property, facility, hostel, PG accommodation, co-living unit, co-working facility, vacation rental, managed property, corporate housing unit, or hospitality asset shall be listed, marketed, distributed, booked, operated, or promoted through IVY Nest unless it has successfully completed the prescribed verification process.

20.2 Verification Components

Verification may include:

a. Ownership verification.

b. Possession verification.

c. Occupancy authorization verification.

d. Municipal compliance verification.

e. Building safety verification.

f. Fire safety verification.

g. Utility connectivity verification.

h. Geo-location verification.

i. Property condition verification.

j. Photograph validation.

k. Amenity verification.

l. Legal occupancy verification.

m. Operational readiness verification.

20.3 Geo-Tagged Verification

IVY Nest reserves the right to require:

a. Geo-tagged photographs.

b. Timestamped inspections.

c. Live video verification.

d. GPS-enabled inspection reports.

e. Independent verification reports.

20.4 Quality Assurance Standards

Partners shall ensure:

a. Habitability.

b. Structural safety.

c. Hygienic conditions.

d. Functional utilities.

e. Clean sanitation facilities.

f. Accurate property descriptions.

g. Safe guest occupancy conditions.

20.5 Continuous Compliance

Property verification may be repeated periodically or whenever risk indicators arise.

21. WORKFORCE COMPLIANCE OBLIGATIONS

21.1 General Requirement

Partners employing workers, staff, contractors, consultants, temporary personnel, housekeeping staff, security personnel, hospitality workers, maintenance personnel, drivers, support staff, or gig workers shall comply with all applicable labour and employment laws.

21.2 Documentation Obligations

Partners shall maintain:

a. Employee records.

b. Attendance records.

c. Wage records.

d. Appointment documents.

e. Contractor agreements.

f. Statutory compliance records.

g. Safety records.

h. Grievance records.

21.3 Verification Rights

IVY Nest reserves the right to verify workforce compliance documentation.

21.4 Non-Compliance Consequences

Material labour violations may result in:

a. Suspension.

b. Financial penalties.

c. Corrective action plans.

d. Termination.

e. Blacklisting.

22. LABOUR LAW COMPLIANCE REQUIREMENTS

22.1 Compliance Obligation

Partners shall comply with all applicable labour laws and workforce regulations.

22.2 Minimum Requirements

Partners shall:

a. Pay lawful wages.

b. Maintain statutory registers.

c. Provide statutory benefits.

d. Comply with working-hour limitations.

e. Comply with overtime requirements.

f. Maintain safe working environments.

g. Comply with social security requirements.

22.3 Statutory Benefits

Where applicable, partners shall comply with:

a. EPF obligations.

b. ESI obligations.

c. Bonus obligations.

d. Gratuity obligations.

e. Leave entitlements.

f. Maternity benefits.

g. Social security obligations.

22.4 Wage Protection

Partners shall not engage in:

a. Wage theft.

b. Unlawful deductions.

c. Delayed payments.

d. Misclassification of workers.

e. Forced wage waivers.

23. CONTRACTOR & GIG WORKFORCE GOVERNANCE

23.1 Contractor Oversight

Partners utilizing contractors or gig workers shall maintain documented governance controls.

23.2 Mandatory Controls

Partners shall:

a. Verify worker identity.

b. Maintain contracts.

c. Verify statutory registrations.

d. Conduct safety training.

e. Maintain grievance channels.

f. Monitor contractor compliance.

23.3 Unauthorized Subcontracting

No partner may subcontract material obligations without prior written approval from IVY Nest.

23.4 Accountability

Partners remain fully responsible for the conduct and compliance of subcontractors.

24. WORKER SAFETY OBLIGATIONS

24.1 Duty of Care

Partners shall maintain safe working conditions.

24.2 Safety Measures

Partners shall implement:

a. Workplace safety protocols.

b. Hazard identification systems.

c. Incident reporting mechanisms.

d. Emergency response procedures.

e. Safety training programs.

f. First-aid arrangements.

g. Fire safety awareness.

24.3 Reporting Obligation

Serious workplace incidents shall be reported to IVY Nest without undue delay and, where legally required, to competent authorities.

24.4 Safety Audits

IVY Nest may conduct or commission safety audits at any time.

25. MIGRANT WORKER PROTECTION OBLIGATIONS

25.1 Protection Commitment

Partners employing migrant workers shall ensure lawful and dignified treatment.

25.2 Minimum Standards

Partners shall provide:

a. Identity documentation support.

b. Wage transparency.

c. Safe accommodation where applicable.

d. Access to grievance mechanisms.

e. Non-discriminatory treatment.

f. Language-accessible communication.

25.3 Prohibited Practices

Partners shall not engage in:

a. Forced labour.

b. Debt bondage.

c. Document confiscation.

d. Wage withholding.

e. Restriction of lawful movement.

26. POSH COMPLIANCE REQUIREMENTS

26.1 Compliance Requirement

Partners shall comply with the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.

26.2 Internal Complaints Mechanism

Where applicable, partners shall establish Internal Committees and grievance mechanisms.

26.3 Cooperation Obligation

Partners shall cooperate with investigations concerning workplace harassment allegations.

26.4 Non-Retaliation

Retaliation against complainants, witnesses, or participants in investigations is strictly prohibited.

26.5 Escalation Rights

IVY Nest may independently review allegations that materially affect its operations, personnel, guests, or reputation.

27. EQUAL OPPORTUNITY & NON-DISCRIMINATION REQUIREMENTS

27.1 Principle

Partners shall promote equal opportunity and non-discriminatory practices.

27.2 Prohibited Discrimination

Discrimination based upon any legally protected characteristic is prohibited.

27.3 Employment Practices

Partners shall maintain fair recruitment, compensation, promotion, and workplace practices.

27.4 Customer Interactions

Partners shall ensure fair treatment of customers, guests, residents, and applicants.

27.5 Accessibility

Reasonable efforts shall be made to improve accessibility and inclusivity.

28. DATA PROTECTION & PRIVACY OBLIGATIONS

28.1 Compliance Framework

Partners shall comply with applicable data protection and privacy laws including the Digital Personal Data Protection Act, 2025.

28.2 Data Governance Principles

Partners shall adhere to:

a. Lawfulness.

b. Purpose limitation.

c. Data minimization.

d. Accuracy.

e. Storage limitation.

f. Accountability.

g. Security.

28.3 Data Fiduciary and Processor Obligations

Where applicable, partners acting as data fiduciaries or data processors shall implement appropriate technical and organizational safeguards.

28.4 Consent Management

Partners shall maintain lawful consent management procedures where consent is required.

28.5 Data Subject Rights

Partners shall assist IVY Nest in responding to lawful privacy-related requests.

28.6 Breach Notification

Partners shall notify IVY Nest of actual or suspected data breaches immediately and no later than twenty-four (24) hours after discovery.

29. CYBERSECURITY GOVERNANCE STANDARDS

29.1 Security Requirement

Partners shall maintain cybersecurity programs appropriate to the nature, scale, and sensitivity of services provided.

29.2 Minimum Security Controls

Partners shall implement:

a. Multi-factor authentication.

b. Role-based access controls.

c. Endpoint protection.

d. Encryption mechanisms.

e. Vulnerability management.

f. Secure backup systems.

g. Incident response plans.

h. Log monitoring.

i. Security awareness training.

29.3 Cybersecurity Maturity Assessment

IVY Nest may assess partner cybersecurity maturity through:

a. Questionnaires.

b. Audits.

c. Security certifications.

d. Penetration testing reviews.

e. Independent assessments.

29.4 Insider Threat Management

Partners shall implement controls to mitigate insider threats.

29.5 Security Updates

Critical vulnerabilities shall be remediated within timelines specified by IVY Nest.

30. ACCESS CONTROL & DATA SHARING GOVERNANCE

30.1 Need-to-Know Principle

Access to IVY Nest information shall be restricted to authorized personnel with legitimate business needs.

30.2 Access Governance

Partners shall maintain:

a. User access inventories.

b. Access approval procedures.

c. Access revocation procedures.

d. Privileged account controls.

e. Segregation of duties.

30.3 Data Sharing Restrictions

Data may only be shared for authorized purposes.

30.4 Cross-Border Transfers

Cross-border transfers shall comply with applicable legal requirements and IVY Nest approval requirements.

30.5 Data Localization

Where required by law or contract, data shall remain stored within approved jurisdictions.

31. CONFIDENTIALITY & INTELLECTUAL PROPERTY PROTECTION

31.1 Confidential Information

Partners shall protect all confidential information received from IVY Nest.

31.2 Use Restrictions

Confidential information shall not be:

a. Misused.

b. Sold.

c. Disclosed.

d. Repurposed.

e. Commercialized.

Without written authorization.

31.3 Intellectual Property Rights

All IVY Nest intellectual property shall remain the exclusive property of IVY Nest.

31.4 Protection Measures

Partners shall implement reasonable safeguards to prevent unauthorized disclosure or misuse.

31.5 Survival

Confidentiality obligations shall survive termination.

32. API & TECHNOLOGY INTEGRATION GOVERNANCE

32.1 Approval Requirement

All API integrations shall require prior authorization.

32.2 Technical Standards

Partners shall comply with:

a. Security standards.

b. Authentication requirements.

c. Data protection requirements.

d. Availability requirements.

e. Logging requirements.

32.3 Security Testing

IVY Nest may require security reviews prior to integration.

32.4 Rate Limiting

Partners shall comply with system usage limits and technical controls.

32.5 Monitoring

API activity may be monitored, logged, analyzed, and audited.

33. DIGITAL PLATFORM USAGE STANDARDS

33.1 Authorized Use

Partners shall use IVY Nest platforms only for authorized purposes.

33.2 Prohibited Activities

Partners shall not:

a. Circumvent controls.

b. Scrape data.

c. Manipulate listings.

d. Misrepresent inventory.

e. Introduce malware.

f. Interfere with systems.

g. Conduct unauthorized testing.

h. Engage in fraudulent transactions.

33.3 Monitoring

IVY Nest reserves the right to monitor platform activity.

33.4 Suspension

Unauthorized activity may result in immediate suspension.

34. OTA LISTING COMPLIANCE STANDARDS

34.1 Listing Accuracy

Partners shall ensure that listings are accurate, complete, current, and verifiable.

34.2 Mandatory Disclosures

Listings shall accurately disclose:

a. Property characteristics.

b. Amenities.

c. Restrictions.

d. Occupancy limits.

e. Applicable charges.

f. Check-in requirements.

g. House rules.

34.3 Misrepresentation

False, misleading, manipulated, deceptive, or inaccurate listings are prohibited.

34.4 Content Verification

IVY Nest may verify listing content through audits and inspections.

35. PRICING TRANSPARENCY REQUIREMENTS

35.1 Transparency Principle

Partners shall maintain transparent and non-deceptive pricing practices.

35.2 Disclosure Requirements

Partners shall disclose:

a. Room charges.

b. Service fees.

c. Taxes.

d. Security deposits.

e. Additional charges.

f. Cancellation charges.

35.3 Prohibited Conduct

Partners shall not:

a. Engage in bait pricing.

b. Conceal fees.

c. Manipulate pricing algorithms unlawfully.

d. Misrepresent discounts.

35.4 Audit Rights

IVY Nest may review pricing practices for compliance.

36. CONSUMER PROTECTION OBLIGATIONS

36.1 Commitment

Partners shall uphold consumer rights and fair trade practices.

36.2 Requirements

Partners shall:

a. Provide truthful information.

b. Address complaints promptly.

c. Honor lawful commitments.

d. Avoid unfair trade practices.

e. Support dispute resolution efforts.

36.3 Cooperation

Partners shall cooperate with consumer investigations, inquiries, and complaint resolution efforts.

37. FRAUD PREVENTION & FINANCIAL CRIME CONTROLS

37.1 Fraud Prevention Program

Partners shall maintain measures to prevent fraud and financial misconduct.

37.2 Fraud Indicators

Partners shall monitor for:

a. Fake bookings.

b. Identity fraud.

c. Chargeback abuse.

d. Revenue concealment.

e. Collusion.

f. Account manipulation.

g. Fake reviews.

h. Unauthorized transactions.

37.3 Reporting Obligation

Suspected fraud shall be reported to IVY Nest immediately.

37.4 Investigative Cooperation

Partners shall cooperate fully in fraud investigations.

38. ANTI-MONEY LAUNDERING (AML) SAFEGUARDS

38.1 AML Commitment

Partners shall support efforts to prevent money laundering and related financial crimes.

38.2 Enhanced Due Diligence

Enhanced review may be required for high-risk transactions or counterparties.

38.3 Monitoring

Partners shall maintain reasonable controls to identify suspicious activities.

38.4 Escalation

Material concerns shall be escalated to IVY Nest without delay.

39. IDENTITY FRAUD PREVENTION MEASURES

39.1 Verification Requirement

Partners shall implement reasonable identity verification procedures.

39.2 Risk Controls

Partners shall establish controls to prevent:

a. Fake identities.

b. Document forgery.

c. Synthetic identities.

d. Account takeovers.

e. Impersonation.

39.3 Verification Rights

IVY Nest reserves the right to require enhanced verification measures.

39.4 Evidence Retention

Verification records shall be retained in accordance with applicable laws and contractual requirements.

40. GUEST SAFETY & PROPERTY SAFETY OBLIGATIONS

40.1 Fundamental Safety Obligation

All partners shall maintain properties, facilities, accommodations, operational premises, transportation services, and customer interaction environments in a safe, secure, hygienic, and legally compliant condition.

40.2 Property Safety Standards

Partners shall ensure:

a. Structural integrity of premises.

b. Fire safety compliance.

c. Functional emergency exits.

d. Safe electrical installations.

e. Safe water systems.

f. Functional sanitation systems.

g. Adequate lighting.

h. Security controls.

i. Pest management.

j. Regular maintenance programs.

40.3 Guest Security Measures

Partners shall maintain appropriate measures including:

a. Visitor management procedures.

b. Access control systems.

c. Emergency contact mechanisms.

d. Security incident reporting.

e. Guest verification procedures where legally permissible.

40.4 Prohibited Conditions

Properties exhibiting dangerous, unsafe, unhealthy, illegal, or materially misleading conditions may be suspended immediately.

40.5 Safety Certifications

IVY Nest may require periodic safety certifications, engineering reports, fire compliance certificates, and other safety-related documentation.

41. EMERGENCY INCIDENT REPORTING PROCEDURES

41.1 Mandatory Reporting

Partners shall immediately report serious incidents affecting:

a. Guest safety.

b. Resident safety.

c. Worker safety.

d. Public safety.

e. Data security.

f. Financial integrity.

g. Property security.

h. Regulatory compliance.

41.2 Reportable Incidents

Examples include:

a. Fire.

b. Building collapse.

c. Serious injury.

d. Fatality.

e. Cyberattack.

f. Data breach.

g. Fraud.

h. Criminal activity.

i. Public health incidents.

j. Regulatory enforcement actions.

41.3 Reporting Timelines

Partners shall notify IVY Nest:

a. Critical incidents – immediately and preferably within one (1) hour.

b. Major incidents – within six (6) hours.

c. Significant incidents – within twenty-four (24) hours.

41.4 Investigation Support

Partners shall preserve evidence and cooperate fully with investigations.

42. BUSINESS CONTINUITY OBLIGATIONS

42.1 Continuity Requirement

Partners providing critical services shall maintain documented Business Continuity Plans (BCPs).

42.2 Scope of Continuity Planning

BCPs should address:

a. Operational disruptions.

b. Cyber incidents.

c. Natural disasters.

d. Workforce disruptions.

e. Infrastructure failures.

f. Vendor failures.

g. Regulatory disruptions.

h. Pandemic or public health events.

42.3 Testing

Partners may be required to periodically test continuity plans.

42.4 Recovery Capability

Partners shall maintain appropriate recovery and resilience capabilities proportionate to risk exposure.

43. INSURANCE & INDEMNITY REQUIREMENTS

43.1 Insurance Obligation

Partners shall maintain adequate insurance coverage based upon the nature of services provided.

43.2 Insurance Types

Where applicable, coverage may include:

a. Public liability insurance.

b. Professional indemnity insurance.

c. Cyber liability insurance.

d. Property insurance.

e. Employer liability insurance.

f. Workers compensation coverage.

g. Commercial general liability insurance.

h. Product liability insurance.

i. Fidelity insurance.

j. Directors and Officers coverage.

43.3 Evidence of Coverage

IVY Nest may require proof of insurance at any time.

43.4 Indemnity

Partners shall indemnify, defend, and hold harmless IVY Nest from losses arising from:

a. Contractual breaches.

b. Regulatory violations.

c. Negligence.

d. Fraud.

e. Misrepresentation.

f. Intellectual property infringement.

g. Data breaches.

h. Labour violations.

i. Third-party claims.

43.5 Regulatory Fine Recovery

IVY Nest reserves the right to recover fines, penalties, settlements, costs, and liabilities attributable to partner misconduct.

44. REGULATORY COOPERATION OBLIGATIONS

44.1 Cooperation Requirement

Partners shall cooperate with lawful requests from regulators, courts, tribunals, law enforcement agencies, and statutory authorities.

44.2 Information Sharing

Subject to applicable law, partners shall provide information reasonably required by IVY Nest to respond to regulatory inquiries.

44.3 Regulatory Investigations

Partners shall promptly notify IVY Nest regarding:

a. Regulatory investigations.

b. Enforcement notices.

c. Compliance orders.

d. Material legal proceedings.

e. Government inspections.

44.4 Non-Interference

Partners shall not obstruct lawful investigations.

44.5 Regulatory Inspection Protocol

44.5.1 Policy Objective

IVY Nest is committed to maintaining full cooperation with competent governmental, statutory, judicial, municipal, regulatory, taxation, law enforcement, data protection, consumer protection, and other authorized authorities during lawful inspections, investigations, inquiries, audits, compliance reviews, or enforcement proceedings.

This Protocol establishes a structured governance framework for managing regulatory inspections in a lawful, transparent, consistent, secure, and well-documented manner while protecting IVY Nest's legal rights, confidential information, commercial interests, customers, employees, Partners, and other stakeholders.

44.5.2 Scope

This Protocol shall apply to:

a. Routine regulatory inspections.

b. Compliance audits.

c. Statutory inspections.

d. Licensing inspections.

e. Consumer protection inspections.

f. Labour inspections.

g. Fire and safety inspections.

h. Municipal inspections.

i. Taxation and financial inspections.

j. Information technology and cybersecurity inspections.

k. Data protection and privacy inspections.

l. Environmental, health, and safety inspections.

m. Competition law investigations.

n. Anti-corruption or financial crime investigations.

o. Judicial commissions, inquiries, and any other lawful inspection or investigation conducted by a competent authority.

44.5.3 Verification of Authority

Before providing access, documents, systems, premises, or information, IVY Nest may, to the extent permitted by applicable law:

a. Verify the identity of inspecting officials.

b. Verify official authorization, warrant, order, notice, or statutory authority where applicable.

c. Record the name, designation, department, and contact details of inspecting officials.

d. Record the purpose, scope, and legal basis of the inspection.

e. Notify the appropriate Approval Authority, Compliance Officer, Legal Department, Data Protection Officer, Cybersecurity Team, or other designated personnel.

Nothing in this Clause shall prevent IVY Nest from immediately complying with any mandatory legal obligation requiring urgent cooperation.

44.5.4 Internal Notification

Upon commencement of a regulatory inspection, the appropriate internal stakeholders may be notified without undue delay, including, where applicable:

a. Governing Authority.

b. Compliance Officer.

c. Legal Counsel.

d. Risk Management Team.

e. Data Protection Officer.

f. Cybersecurity Team.

g. Information Security Team.

h. Business Unit Head.

i. Other personnel responsible for managing the inspection.

44.5.5 Cooperation with Authorities

IVY Nest and its Partners shall cooperate in good faith with competent authorities and shall:

a. Provide lawful access to records, documents, premises, systems, or information required by law.

b. Respond accurately and truthfully to lawful requests.

c. Preserve relevant records and evidence.

d. Avoid concealment, destruction, alteration, fabrication, or obstruction of evidence.

e. Comply with lawful directions, notices, summons, or orders.

f. Facilitate reasonable access for inspections, interviews, demonstrations, or document verification.

Nothing in this Clause shall require disclosure of information protected by legal professional privilege, statutory confidentiality obligations, contractual confidentiality obligations, trade secret protections, or any other applicable legal restriction, except where disclosure is legally required.

44.5.6 Protection of Confidential Information

Where confidential, proprietary, commercially sensitive, personal, or Restricted Information is requested during an inspection, IVY Nest may:

a. Verify the legal authority for disclosure.

b. Limit disclosure to information reasonably required.

c. Maintain a record of information disclosed.

d. Mark confidential material appropriately.

e. Request confidentiality protections where permitted by law.

f. Require secure handling of electronic information where appropriate.

44.5.7 Digital Evidence Preservation

Where an inspection involves electronic systems, digital evidence, cloud environments, logs, databases, electronic records, surveillance systems, or digital devices, IVY Nest may implement reasonable measures to preserve data integrity, maintain audit trails, protect cybersecurity controls, and ensure proper chain of custody without unlawfully interfering with the inspection.

44.5.8 Inspection Documentation

A written inspection record may be maintained including:

a. Date and time of inspection.

b. Identity and designation of inspecting officials.

c. Legal authority relied upon.

d. Scope of inspection.

e. Documents reviewed or copied.

f. Electronic records accessed.

g. Physical areas inspected.

h. Statements or explanations provided.

i. Samples or evidence collected.

j. Notices, observations, or directions issued.

k. Immediate corrective actions taken.

l. Follow-up obligations and deadlines.

44.5.9 Regulatory Response and Corrective Action

Following completion of the inspection, IVY Nest may:

a. Review inspection findings.

b. Conduct internal investigations where appropriate.

c. Prepare a Corrective and Preventive Action (CAPA) Plan.

d. Assign implementation responsibilities.

e. Monitor completion of corrective actions.

f. Verify compliance before closure.

g. Report material findings to the Governing Authority where required.

44.5.10 Partner Cooperation

Partners shall promptly cooperate with lawful regulatory inspections affecting the partnership and shall provide reasonable assistance, records, certifications, declarations, access, explanations, or supporting documentation requested by IVY Nest or competent authorities, subject to applicable law and contractual obligations.

Partners shall promptly notify IVY Nest of any regulatory inspection, investigation, enforcement action, or material regulatory communication relating to services, products, systems, data, facilities, or activities connected with the partnership.

44.5.11 Preservation of Rights

Nothing contained in this Policy shall:

a. Waive any legal, contractual, statutory, or constitutional rights available to IVY Nest.

b. Prevent IVY Nest from seeking legal advice before responding where legally permissible.

c. Limit the protection of legally privileged communications.

d. Restrict IVY Nest from asserting confidentiality, trade secret, intellectual property, privacy, or other lawful protections.

e. Prevent IVY Nest from challenging unlawful, excessive, or unauthorized requests through lawful legal processes.

44.5.12 Material Non-Compliance

Failure by a Partner to cooperate with lawful regulatory inspections, destruction or concealment of evidence, obstruction of lawful investigations, submission of false information, failure to preserve records, unauthorized disclosure of confidential information, or any attempt to interfere with a lawful inspection may constitute a Material Breach under this Policy and may result in enhanced monitoring, corrective action, suspension, termination of the partnership, recovery of losses, contractual remedies, blacklisting, regulatory reporting where legally required, or any other remedy available under applicable law or contract.

44.5.13 Continuous Improvement

IVY Nest may periodically review and update this Regulatory Inspection Protocol in response to changes in applicable law, regulatory expectations, industry best practices, operational experience, technological developments, enterprise risk assessments, audit findings, or lessons learned from previous inspections to ensure the continued effectiveness of its regulatory compliance framework.

45. AUDIT RIGHTS & INSPECTION FRAMEWORK

45.1 Audit Authority

IVY Nest reserves the right to audit partner compliance.

45.2 Audit Scope

Audits may cover:

a. Legal compliance.

b. Financial records.

c. Revenue reporting.

d. Labour compliance.

e. Cybersecurity controls.

f. Data governance.

g. Property standards.

h. Operational practices.

i. Contractual obligations.

45.3 Access Rights

Partners shall provide reasonable access to:

a. Records.

b. Personnel.

c. Systems.

d. Facilities.

e. Documentation.

45.4 Third-Party Auditors

Audits may be conducted by authorized internal or external representatives.

46. SURPRISE COMPLIANCE INSPECTION RIGHTS

46.1 Unannounced Inspections

IVY Nest may conduct surprise inspections where reasonably necessary.

46.2 Grounds

Such inspections may be initiated upon:

a. Complaints.

b. Fraud indicators.

c. Safety concerns.

d. Regulatory concerns.

e. Quality concerns.

f. Reputation risks.

g. Compliance failures.

46.3 Cooperation Obligation

Partners shall not obstruct inspection activities.

46.4 Evidence Collection

IVY Nest may collect photographs, videos, records, logs, and inspection reports.

47. PERFORMANCE MONITORING FRAMEWORK

47.1 Continuous Monitoring

Partner performance shall be monitored continuously.

47.2 Performance Indicators

Monitoring may include:

a. Customer satisfaction.

b. Complaint volumes.

c. Service quality.

d. Booking fulfillment.

e. Operational responsiveness.

f. Compliance performance.

g. Revenue integrity.

h. Cybersecurity maturity.

i. Safety performance.

j. Audit findings.

47.3 Performance Ratings

Partners may be assigned risk-adjusted performance ratings.

47.4 Improvement Plans

Underperforming partners may be required to implement corrective action plans.

48. ESG & ETHICAL GOVERNANCE EXPECTATIONS

48.1 Commitment

Partners shall operate in a manner consistent with responsible business conduct principles.

48.2 Governance Expectations

Partners shall promote:

a. Ethical business conduct.

b. Transparency.

c. Accountability.

d. Responsible governance.

e. Human rights protection.

f. Environmental responsibility.

48.3 Prohibited Conduct

Partners shall not engage in:

a. Human trafficking.

b. Forced labour.

c. Child labour.

d. Corruption.

e. Illegal discrimination.

f. Environmental misconduct.

48.4 ESG Reporting

IVY Nest may require ESG-related disclosures and certifications.

49. SUSTAINABILITY & RESPONSIBLE OPERATIONS STANDARDS

49.1 Sustainability Commitment

Partners are encouraged to adopt environmentally responsible practices.

49.2 Recommended Measures

Examples include:

a. Energy efficiency.

b. Water conservation.

c. Waste reduction.

d. Recycling programs.

e. Sustainable procurement.

f. Responsible resource management.

49.3 Compliance

Sustainability initiatives shall not conflict with safety, legal, or operational requirements.

50. SOCIAL MEDIA & BRAND USAGE RESTRICTIONS

50.1 Ownership

All IVY Nest trademarks, logos, brand assets, domain names, and proprietary identifiers remain the exclusive property of IVY Nest.

50.2 Usage Restrictions

Partners shall not:

a. Alter brand assets.

b. Misrepresent affiliation.

c. Create misleading content.

d. Use deceptive advertising.

e. Register confusingly similar domains.

f. Use brand assets without authorization.

50.3 Social Media Conduct

Partners shall avoid content that may:

a. Harm reputation.

b. Mislead customers.

c. Violate laws.

d. Damage stakeholder confidence.

50.4 Immediate Revocation

Brand usage permissions may be revoked immediately.

51. PUBLIC REPRESENTATION & MARKETING CONTROLS

51.1 Approval Requirement

Certain public statements may require prior approval.

51.2 Restricted Activities

Partners shall not:

a. Represent themselves as agents unless authorized.

b. Make regulatory claims without approval.

c. Issue official company statements.

d. Promise services beyond authorized scope.

51.3 Marketing Compliance

All marketing shall comply with:

a. Consumer protection laws.

b. Advertising standards.

c. Competition laws.

d. Applicable platform requirements.

52. INCIDENT ESCALATION MATRIX

52.1 Classification Framework

Incidents shall be categorized as:

a. Level 1 – Minor.

b. Level 2 – Significant.

c. Level 3 – Major.

d. Level 4 – Critical.

52.2 Escalation Criteria

Classification shall consider:

a. Legal exposure.

b. Financial impact.

c. Customer impact.

d. Safety implications.

e. Regulatory consequences.

f. Reputational harm.

52.3 Mandatory Escalation

Critical incidents shall be escalated to designated IVY Nest authorities immediately.

53. GRIEVANCE & COMPLAINT HANDLING PROCEDURES

53.1 Complaint Mechanism

Partners shall maintain accessible complaint-handling procedures.

53.2 Complaint Categories

Complaints may include:

a. Service complaints.

b. Safety concerns.

c. Data concerns.

d. Labour concerns.

e. Harassment concerns.

f. Fraud concerns.

53.3 Resolution Requirements

Partners shall investigate and address complaints in a timely manner.

53.4 Escalation Rights

IVY Nest may intervene where complaints present material risk.

54. WHISTLEBLOWER PROTECTION FRAMEWORK

54.1 Reporting Channels

Partners shall encourage reporting of suspected misconduct.

54.2 Protected Disclosures

Reports may concern:

a. Fraud.

b. Corruption.

c. Safety violations.

d. Data misuse.

e. Regulatory breaches.

f. Financial misconduct.

54.3 Anti-Retaliation

Retaliation against whistleblowers is strictly prohibited.

54.4 Confidentiality

Whistleblower identities shall be protected to the extent permitted by law.

55. INVESTIGATION PROCEDURES

55.1 Investigation Authority

IVY Nest reserves the right to investigate actual or suspected misconduct.

55.2 Scope

Investigations may involve:

a. Interviews.

b. Document reviews.

c. System reviews.

d. Audit activities.

e. Site inspections.

f. Forensic analysis.

55.3 Cooperation Obligation

Partners shall provide timely cooperation.

55.4 Evidence Preservation

Partners shall preserve all relevant information and evidence.

56. CORRECTIVE & PREVENTIVE ACTION (CAPA) MECHANISM

56.1 CAPA Requirement

Partners shall implement corrective and preventive measures when deficiencies are identified.

56.2 CAPA Elements

Plans may include:

a. Root cause analysis.

b. Corrective actions.

c. Preventive controls.

d. Responsible owners.

e. Timelines.

f. Validation activities.

56.3 Verification

IVY Nest may verify implementation effectiveness.

57. BREACH CLASSIFICATION FRAMEWORK

57.1 Categories

Breaches may be classified as:

a. Minor.

b. Moderate.

c. Material.

d. Severe.

e. Critical.

57.2 Evaluation Factors

Assessment may consider:

a. Intent.

b. Impact.

c. Recurrence.

d. Regulatory consequences.

e. Customer harm.

f. Financial loss.

g. Reputational impact.

57.3 Escalation

Material and above breaches shall be escalated to senior management.

58. SUSPENSION & RESTRICTION POWERS

58.1 Immediate Suspension Authority

IVY Nest may immediately suspend or restrict a partner upon reasonable belief of:

a. Fraud.

b. Safety threats.

c. Data compromise.

d. Regulatory violations.

e. Criminal conduct.

f. Material contract breaches.

58.2 Interim Measures

IVY Nest may impose:

a. Listing restrictions.

b. Payment holds.

c. Data access restrictions.

d. Operational limitations.

e. Enhanced monitoring.

58.3 No Waiver

Failure to suspend immediately shall not constitute waiver of rights.

59. TERMINATION & EXIT MANAGEMENT PROCEDURES

59.1 Termination Rights

IVY Nest may terminate partnerships in accordance with contractual rights and applicable laws.

59.2 Grounds for Termination

Termination may occur due to:

a. Material breach.

b. Fraud.

c. Corruption.

d. Safety failures.

e. Regulatory violations.

f. Insolvency.

g. Reputational harm.

h. Persistent non-compliance.

i. Data security failures.

59.3 Exit Requirements

Partners shall cooperate with orderly transition activities.

59.4 Recovery Rights

Termination shall not affect accrued rights, remedies, liabilities, or obligations.

59.5 Survival

Provisions relating to confidentiality, indemnity, intellectual property, audit cooperation, data protection, dispute resolution, evidence preservation, and post-termination obligations shall survive termination.

60. BLACKLISTING & DEBARMENT FRAMEWORK

60.1 Authority

IVY Nest reserves the right to blacklist, debar, suspend, restrict, or permanently prohibit any partner from participating in its ecosystem.

60.2 Grounds for Blacklisting

Grounds may include:

a. Fraud.

b. Corruption.

c. Bribery.

d. Revenue concealment.

e. Cybersecurity violations.

f. Data misuse.

g. Human trafficking.

h. Child labour.

i. Forced labour.

j. Serious labour law violations.

k. Regulatory violations.

l. Repeated contractual breaches.

m. Safety violations.

n. Material reputational harm.

o. Submission of false information.

60.3 Debarment Period

Debarment may be:

a. Temporary.

b. Conditional.

c. Permanent.

60.4 Industry Notifications

Where legally permissible, IVY Nest may notify relevant stakeholders, industry bodies, service providers, insurers, regulators, or law enforcement authorities regarding blacklisted entities.

61. POST-TERMINATION OBLIGATIONS

61.1 Continuing Obligations

Following termination, partners shall:

a. Cease representing affiliation with IVY Nest.

b. Return confidential information.

c. Remove brand assets.

d. Revoke unauthorized access.

e. Settle outstanding obligations.

f. Cooperate in transition activities.

61.2 Data Handling

Partners shall:

a. Return data where required.

b. Securely delete retained data.

c. Certify destruction upon request.

d. Preserve records required by law.

61.3 Continuing Cooperation

Partners shall continue cooperating with audits, investigations, regulatory proceedings, and legal matters relating to activities occurring during the partnership term.

62. REGULATORY REPORTING OBLIGATIONS

62.1 Reporting Requirement

Partners shall promptly notify IVY Nest regarding:

a. Regulatory investigations.

b. Compliance notices.

c. Enforcement actions.

d. Government inspections.

e. Material legal proceedings.

f. Licence suspensions.

g. Cybersecurity incidents.

h. Safety incidents.

62.2 Materiality Standard

Any matter reasonably capable of affecting customers, operations, legal compliance, financial stability, or reputation shall be considered reportable.

62.3 Regulatory Cooperation

Partners shall assist IVY Nest in fulfilling lawful reporting obligations.

63. RECORD RETENTION & DOCUMENTATION GOVERNANCE

63.1 Documentation Obligation

Partners shall maintain complete, accurate, and reliable records.

63.2 Categories of Records

Records may include:

a. Contracts.

b. Financial records.

c. Tax records.

d. Property records.

e. Compliance certifications.

f. Workforce records.

g. Audit records.

h. Cybersecurity logs.

i. Investigation records.

j. Training records.

63.3 Retention Period

Unless a longer period is required by law, contract, investigation, or legal hold notice, records shall be retained for a minimum of eight (8) years.

63.4 Accessibility

Records shall remain accessible, searchable, authentic, and capable of evidentiary use.

64. ELECTRONIC EVIDENCE PRESERVATION STANDARDS

64.1 Preservation Requirement

Partners shall preserve electronic evidence relevant to:

a. Investigations.

b. Disputes.

c. Regulatory inquiries.

d. Safety incidents.

e. Cybersecurity incidents.

f. Financial irregularities.

64.2 Types of Electronic Evidence

Electronic evidence may include:

a. Emails.

b. Messages.

c. System logs.

d. CCTV recordings.

e. GPS records.

f. Access logs.

g. Booking records.

h. Financial records.

i. Cloud records.

j. Metadata.

64.3 Integrity Controls

Electronic evidence shall be preserved in a manner ensuring:

a. Authenticity.

b. Integrity.

c. Traceability.

d. Admissibility.

e. Chain of custody.

64.4 Destruction Prohibition

Relevant electronic evidence shall not be altered, deleted, concealed, or destroyed.

65. LEGAL HOLD & LITIGATION PRESERVATION REQUIREMENTS

65.1 Legal Hold Authority

IVY Nest may issue legal hold notices requiring preservation of information.

65.2 Scope

Legal holds may apply to:

a. Physical records.

b. Electronic records.

c. Communications.

d. Financial records.

e. Property records.

f. CCTV footage.

g. Mobile device data.

h. Cloud storage records.

65.3 Compliance Requirement

Partners shall immediately suspend routine deletion activities affecting preserved information.

65.4 Certification

Partners may be required to certify compliance with legal hold requirements.

66. DISPUTE RESOLUTION FRAMEWORK

66.1 Objective

Disputes shall be managed efficiently, fairly, confidentially, and in a commercially reasonable manner.

66.2 Escalation Hierarchy

Disputes should generally proceed through:

a. Operational discussion.

b. Management review.

c. Executive escalation.

d. Mediation where appropriate.

e. Arbitration.

f. Judicial enforcement where necessary.

66.3 Good Faith Requirement

Parties shall attempt good faith resolution prior to initiating formal proceedings unless immediate action is required to protect rights, assets, customers, data, reputation, or safety.

66.4 Interim Relief

Nothing in this Policy shall restrict IVY Nest from seeking urgent equitable, injunctive, or protective relief.

67. ARBITRATION & GOVERNING LAW CLAUSE

67.1 Governing Law

This Policy and all partnerships governed under it shall be interpreted in accordance with the laws of India.

67.2 Arbitration

Unless otherwise specified in a written agreement, disputes may be referred to arbitration under the Arbitration and Conciliation Act, 1996.

67.3 Tribunal

The arbitration tribunal shall ordinarily consist of a sole arbitrator appointed in accordance with applicable contractual provisions.

67.4 Language

Arbitration proceedings shall ordinarily be conducted in English unless otherwise agreed.

67.5 Binding Nature

Arbitration awards shall be final and binding upon the parties.

68. JURISDICTION CLAUSE

68.1 Exclusive Jurisdiction

Subject to applicable arbitration provisions, courts having jurisdiction over the registered office of IVY Nest shall possess exclusive jurisdiction over disputes arising from or relating to this Policy.

68.2 Regulatory Jurisdiction

Nothing herein shall restrict the jurisdiction of statutory authorities, regulators, tribunals, or governmental agencies.

69. FORCE MAJEURE GOVERNANCE

69.1 Force Majeure Events

Force majeure events may include:

a. Natural disasters.

b. Floods.

c. Earthquakes.

d. Epidemics.

e. Pandemics.

f. Government actions.

g. War.

h. Civil unrest.

i. Terrorist incidents.

j. Widespread cyberattacks.

k. Infrastructure failures.

69.2 Notification Requirement

Affected parties shall promptly notify the other party.

69.3 Mitigation Obligation

Affected parties shall take reasonable steps to mitigate impacts.

69.4 Limitation

Force majeure shall not excuse obligations capable of performance through reasonable alternative means.

70. LEGAL SUPREMACY CLAUSE

70.1 Supremacy

This Policy shall be interpreted consistently with applicable law.

70.2 Conflict Resolution

Where a conflict exists between this Policy and applicable law, the applicable law shall prevail to the extent of such conflict.

70.3 Severability

Invalidity of any provision shall not affect the enforceability of remaining provisions.

71. STATE-SPECIFIC ADAPTABILITY CLAUSE

71.1 Multi-State Operations

IVY Nest operates across multiple jurisdictions and regulatory environments.

71.2 Supplemental Requirements

State-specific requirements may supplement this Policy.

71.3 Stricter Standard Rule

Where multiple standards apply, the stricter requirement shall ordinarily prevail unless prohibited by law.

71.4 Local Compliance

Partners shall comply with all local registrations, licences, permits, and regulatory obligations.

72. REVIEW & AMENDMENT FRAMEWORK

72.1 Review Frequency

This Policy shall be reviewed periodically and at least annually.

72.2 Review Triggers

Review may occur upon:

a. Regulatory changes.

b. Material incidents.

c. Business expansion.

d. New service offerings.

e. Emerging risks.

f. Audit findings.

72.3 Amendment Authority

IVY Nest reserves the right to amend this Policy at its discretion.

72.4 Notice

Updated versions may be published through appropriate communication channels.

73. VERSION CONTROL

73.1 Documentation

IVY Nest shall maintain version control records.

73.2 Minimum Information

Version records may include:

a. Version number.

b. Effective date.

c. Approval authority.

d. Summary of changes.

e. Review date.

73.3 Authoritative Version

The most recently approved version shall govern unless otherwise specified.

74. EFFECTIVE DATE

74.1 Effectiveness

This Policy shall become effective on the date approved by IVY Nest and published through authorized channels.

74.2 Continuing Applicability

This Policy shall remain effective until amended, replaced, or withdrawn.

75. POLICY OWNER

75.1 Ownership

The Legal, Compliance, Risk Management, and Corporate Governance functions of IVY Nest shall serve as the custodians of this Policy.

75.2 Responsibilities

Policy owners shall be responsible for:

a. Governance oversight.

b. Periodic review.

c. Regulatory alignment.

d. Training coordination.

e. Compliance monitoring.

f. Policy maintenance.

76. BOARD & COMPLIANCE COMMITTEE OVERSIGHT

76.1 Oversight Authority

The Board of Directors, Designated Partners, Managing Partners, Governing Body, or equivalent governing authority, as applicable and designated Compliance Committee shall oversee implementation of this Policy.

76.2 Responsibilities

Oversight responsibilities may include:

a. Governance review.

b. Risk oversight.

c. Compliance monitoring.

d. Strategic direction.

e. Incident review.

f. Audit review.

g. Policy approval.

76.3 Reporting

Management shall periodically report material partnership risks and compliance matters.

77. ENTERPRISE COMPLIANCE CERTIFICATION REQUIREMENTS

77.1 Certification Requirement

IVY Nest may require partners to provide periodic compliance certifications.

77.2 Certification Topics

Certifications may address:

a. Legal compliance.

b. Labour compliance.

c. Tax compliance.

d. Data protection.

e. Cybersecurity.

f. Anti-corruption.

g. Safety compliance.

h. ESG compliance.

77.3 False Certifications

False certifications shall constitute a material breach.

78. PERIODIC COMPLIANCE AUDIT OBLIGATIONS

78.1 Audit Program

Partners shall participate in periodic compliance reviews and audits.

78.2 Audit Areas

Reviews may include:

a. Contract compliance.

b. Labour compliance.

c. Data protection.

d. Cybersecurity.

e. Financial integrity.

f. Safety compliance.

g. Consumer protection.

h. Operational quality.

78.3 Remediation

Partners shall promptly address audit findings.

78.4 Repeat Violations

Repeated non-compliance may result in enhanced oversight, suspension, termination, or blacklisting.

79. COMPREHENSIVE PARTNERSHIP COMPLIANCE DECLARATION – IVY NEST APARTMENTS

IVY Nest Apartments affirms its commitment to maintaining a partnership ecosystem founded upon legality, transparency, accountability, ethical conduct, operational excellence, worker protection, customer trust, cybersecurity resilience, and sustainable growth.

IVY Nest expects every partner, affiliate, franchisee, vendor, property owner, technology provider, strategic alliance participant, contractor, service provider, and commercial counterparty to comply with all applicable laws, regulations, contractual obligations, and governance requirements.

IVY Nest further affirms its commitment to:

a. Compliance with applicable corporate, commercial, labour, hospitality, consumer protection, cybersecurity, privacy, and regulatory requirements.

b. Protection of workers from discrimination, harassment, exploitation, unsafe working conditions, wage theft, forced labour, child labour, and unlawful treatment.

c. Promotion of equal opportunity, dignity, inclusion, fairness, and workplace respect.

d. Maintenance of robust data protection and privacy safeguards in alignment with applicable legal requirements including the Digital Personal Data Protection Act, 2025.

e. Implementation of cybersecurity controls designed to protect customers, residents, workers, partners, systems, and information assets.

f. Continuous enhancement of operational resilience, risk management capabilities, and compliance programs.

g. Cooperation with lawful investigations, audits, inspections, and regulatory oversight activities.

h. Protection of consumers through transparency, accuracy, fair dealing, and responsible business practices.

i. Promotion of ethical governance, anti-corruption standards, financial integrity, and responsible commercial conduct.

j. Ongoing review and improvement of partnership governance frameworks to address emerging legal, operational, technological, and societal risks.

All partners engaging with IVY Nest acknowledge that compliance with this Policy constitutes a material condition of partnership and that failure to comply may result in corrective action, suspension, termination, legal action, financial recovery measures, blacklisting, regulatory reporting, or any other remedy available under applicable law, contract, or equity.

This Comprehensive Partnership Compliance Declaration shall be interpreted broadly to protect the legitimate interests of customers, workers, residents, stakeholders, investors, regulators, and the IVY Nest ecosystem while promoting responsible, secure, and sustainable business operations.

ANNEXURE A

PARTNER RISK SCORING MODEL

A.1 Risk Categories

Each partner shall be assigned a risk score based upon:

Risk Factor	Weight
Regulatory Risk	20%
Financial Stability	15%
Litigation Exposure	10%
Data Access Level	15%
Cybersecurity Maturity	15%
Operational Dependency	10%
Reputational Risk	10%
Geographic Risk	5%

A.2 Risk Classification

0–25 = Low Risk

26–50 = Moderate Risk

51–75 = High Risk

76–100 = Critical Risk

A.3 Enhanced Controls

High-Risk and Critical-Risk Partners may be subjected to:

a. Quarterly audits.

b. Executive review.

c. Enhanced contractual controls.

d. Additional insurance requirements.

e. Increased reporting obligations.

ANNEXURE B

MANDATORY PARTNER DOCUMENT CHECKLIST

B.1 Corporate Partners

Mandatory documentation may include:

a. Certificate of Incorporation.

b. PAN.

c. GST Registration.

d. CIN.

e. Memorandum and Articles.

f. Board Resolution.

g. Authorized Signatory Proof.

h. Audited Financial Statements.

i. Bank Verification Letter.

j. MSME/Udyam Registration (if applicable).

B.2 LLP Partners

a. LLP Registration Certificate.

b. LLP Agreement.

c. PAN.

d. GST Registration.

e. Partner KYC.

f. Beneficial Ownership Declaration.

B.3 Individual Property Owners

a. PAN.

b. Aadhaar or other permissible identification.

c. Ownership Proof.

d. Utility Bill.

e. Bank Details.

f. Property Tax Receipt.

g. Occupancy Documentation.

ANNEXURE C

BENEFICIAL OWNERSHIP DECLARATION

Every partner shall certify:

a. Ultimate beneficial ownership structure.

b. Percentage ownership.

c. Control rights.

d. Voting rights.

e. Related-party interests.

f. Politically Exposed Person status.

g. Sanctions exposure status.

False declarations shall constitute material fraud.

ANNEXURE D

SANCTIONS & WATCHLIST SCREENING PROTOCOL

D.1 Screening Sources

Where appropriate and proportionate to risk, Partners may be screened against:

a. United Nations sanctions and designated persons lists.

b. Domestic regulatory, enforcement, judicial, tribunal, and law enforcement records.

c. Insolvency and bankruptcy records.

d. Commercial compliance intelligence databases.

e. Applicable international sanctions regimes.

f. Export control and restricted-party screening databases.

g. International trade restriction databases.

h. Customs enforcement records.

i. Government-issued debarment or prohibited entity lists.

j. Politically Exposed Person (PEP) databases, where appropriate.

k. Adverse media, financial crime intelligence, fraud intelligence, and reputational risk databases.

l. Government advisories and intergovernmental compliance publications.

m. Any other publicly available or commercially licensed compliance intelligence sources reasonably considered appropriate by IVY Nest.

D.2 Rescreening

Screening may be repeated:

a. At onboarding.

b. Annually.

c. Upon changes in ownership or beneficial ownership.

d. Upon changes in directors, partners, or key management personnel.

e. Upon entry into new jurisdictions.

f. Upon significant changes in business activities.

g. Following mergers, acquisitions, restructurings, or material corporate changes.

h. Following significant contractual amendments.

i. Following material regulatory investigations or enforcement proceedings.

j. Following significant adverse media reports.

k. Following material cybersecurity or fraud incidents.

l. Following identification of elevated sanctions, export control, financial crime, or international trade risks.

m. Whenever IVY Nest reasonably determines that additional screening is necessary.

D.3 International Trade Compliance

Where applicable, Partners shall comply with all applicable international sanctions regimes, export control laws, customs requirements, international trade restrictions, economic embargoes, anti-boycott laws, strategic trade controls, and other cross-border legal requirements relevant to the partnership.

Partners may be required to provide declarations, certifications, licences, approvals, supporting documentation, or other evidence demonstrating ongoing compliance.

D.4 Enhanced International Risk Review

IVY Nest may conduct enhanced compliance reviews for partnerships involving:

a. International strategic alliances.

b. Cross-border commercial transactions.

c. Overseas technology providers.

d. Cloud infrastructure providers.

e. Cross-border data hosting or processing.

f. International payment providers.

g. Foreign investors.

h. International franchise or licensing arrangements.

i. Controlled technologies.

j. Artificial Intelligence systems.

k. Encryption technologies.

l. Jurisdictions presenting elevated geopolitical, sanctions, regulatory, financial crime, cybersecurity, export control, or international trade risks.

D.5 Supply Chain Trade Compliance

Partners shall exercise reasonable due diligence over subcontractors, suppliers, affiliates, consultants, logistics providers, distributors, intermediaries, and other third parties participating in activities connected with the partnership.

Reasonable measures shall be implemented to identify and mitigate indirect sanctions exposure, diversion risks, transshipment risks, export control violations, and other material supply chain compliance risks.

D.6 Material Non-Compliance

Failure to comply with applicable international sanctions, export control laws, customs requirements, international trade restrictions, anti-boycott laws, strategic trade controls, or other applicable cross-border legal obligations may constitute a Material Breach of this Policy and may result in enhanced due diligence, corrective action, suspension, restriction, termination, blacklisting, contractual remedies, regulatory reporting where legally required, recovery of losses, or any other remedy available under applicable law or contract.

ANNEXURE E

CYBERSECURITY CONTROL BASELINE

Partners with access to IVY Nest systems or data shall maintain:

E.1 Identity Security

a. MFA.

b. Strong password policies.

c. Privileged access controls.

E.2 Infrastructure Security

a. Endpoint protection.

b. Patch management.

c. Vulnerability scanning.

d. Secure configuration standards.

E.3 Monitoring

a. Security logging.

b. Incident monitoring.

c. Alerting mechanisms.

d. Audit trails.

E.4 Data Protection

a. Encryption at rest.

b. Encryption in transit.

c. Access logging.

d. Backup management.

ANNEXURE F

CYBER INCIDENT REPORTING MATRIX

Incident Type	Reporting Time
Critical Incident	Within 1 Hour
Major Incident	Within 6 Hours
Significant Incident	Within 24 Hours
Minor Incident	Within 72 Hours

Partners shall cooperate with any reporting obligations applicable under law, including CERT-In reporting requirements where applicable.

ANNEXURE G

PROPERTY COMPLIANCE INSPECTION CHECKLIST

G.1 Legal Compliance

a. Ownership verification.

b. Municipal permissions.

c. Occupancy permissions.

d. Fire compliance.

G.2 Safety Compliance

a. Fire extinguishers.

b. Emergency exits.

c. Electrical safety.

d. Structural safety.

G.3 Hygiene Compliance

a. Cleanliness.

b. Water quality.

c. Waste disposal.

d. Sanitation.

G.4 Guest Readiness

a. Amenities.

b. Security arrangements.

c. House rules.

d. Emergency contacts.

ANNEXURE H

WORKER PROTECTION CERTIFICATION

Partners shall annually certify:

a. No child labour.

b. No forced labour.

c. No human trafficking.

d. No wage theft.

e. Compliance with labour laws.

f. Compliance with POSH obligations.

g. Compliance with social security obligations.

ANNEXURE I

ESG COMPLIANCE DECLARATION

Partners shall declare:

a. Environmental responsibility measures.

b. Ethical sourcing practices.

c. Anti-corruption controls.

d. Human rights compliance.

e. Worker welfare measures.

f. Community impact initiatives.

ANNEXURE J

CRITICAL BREACH EVENTS

The following shall automatically constitute Critical Breaches:

a. Human trafficking.

b. Child labour.

c. Forced labour.

d. Bribery.

e. Corruption.

f. Cybersecurity compromise affecting customer data.

g. Revenue fraud.

h. Guest safety incidents involving death.

i. Intentional regulatory violations.

j. Material misrepresentation.

IVY Nest may immediately suspend the partner pending investigation.

ANNEXURE K

ENTERPRISE COMPLIANCE CERTIFICATE

Each partner shall certify annually that:

a. Information previously provided remains accurate.

b. No undisclosed litigation exists.

c. No sanctions exposure exists.

d. Labour law obligations are complied with.

e. Tax obligations are complied with.

f. Data protection obligations are complied with.

g. Cybersecurity obligations are complied with.

h. Material incidents have been disclosed.

i. No conflict of interest remains undisclosed.

j. This Policy continues to be accepted and binding.

ANNEXURE L

BOARD-LEVEL RESERVED MATTERS

The following partnerships may require Board or Compliance Committee approval:

a. Strategic alliances exceeding prescribed thresholds.

b. International expansion partnerships.

c. Joint ventures.

d. Franchise network expansion.

e. Data-sharing partnerships involving sensitive personal data.

f. High-risk technology integrations.

g. Acquisitions and merger-related partnerships.

h. Partnerships carrying significant reputational exposure.

IMPLEMENTATION STATEMENT

These Annexures form an integral part of the IVY Nest Apartments Partnership Policy & Strategic Alliance Governance Framework and shall be interpreted together with the main Policy. In the event of inconsistency, the stricter compliance requirement shall prevail unless prohibited by applicable law.

SCHEDULE M

THIRD-PARTY RISK MANAGEMENT (TPRM) FRAMEWORK

M.1 Risk-Based Oversight

All partners shall be governed through a formal Third-Party Risk Management Program.

M.2 Lifecycle Governance

The TPRM lifecycle shall include:

a. Identification.

b. Risk Screening.

c. Due Diligence.

d. Contractual Controls.

e. Onboarding.

f. Continuous Monitoring.

g. Incident Management.

h. Renewal Assessment.

i. Exit Governance.

M.3 Critical Third Parties

The following shall be classified as Critical Third Parties:

a. Managed Property Operators.

b. Franchise Partners.

c. Technology Providers.

d. Cloud Service Providers.

e. Payment Processing Partners.

f. Data Processing Partners.

g. Customer Support Vendors.

h. OTA Distribution Partners.

i. Strategic Revenue Partners.

j. Core Operational Vendors.

M.4 Enhanced Oversight

Critical third parties shall be subject to:

a. Annual governance review.

b. Quarterly compliance certification.

c. Enhanced cybersecurity assessments.

d. Business continuity testing.

e. Executive-level oversight.

SCHEDULE N

REGULATORY INTELLIGENCE & LEGAL CHANGE MANAGEMENT

N.1 Continuous Monitoring

IVY Nest shall maintain mechanisms to monitor:

a. Legislative changes.

b. Regulatory notifications.

c. Court judgments.

d. Tribunal decisions.

e. Industry advisories.

f. Enforcement actions.

g. CERT-In advisories.

h. Data protection developments.

N.2 Partner Obligation

Partners shall promptly notify IVY Nest of legal or regulatory changes materially affecting service delivery.

N.3 Compliance Updates

Partners shall implement required compliance modifications within timelines prescribed by law or IVY Nest.

SCHEDULE O

ARTIFICIAL INTELLIGENCE & AUTOMATED DECISION GOVERNANCE

O.1 Scope

This Schedule applies to partners using Artificial Intelligence, Machine Learning, Automated Decision Systems, Generative AI, Recommendation Engines, Pricing Algorithms, or Predictive Analytics affecting IVY Nest operations.

O.2 Transparency

Partners shall disclose:

a. Material AI systems.

b. Automated decision processes.

c. Significant AI-assisted customer interactions.

d. Algorithmic risk factors.

O.3 Prohibited AI Uses

Partners shall not use AI systems for:

a. Unlawful discrimination.

b. Fraudulent activity.

c. Identity manipulation.

d. Deepfake abuse.

e. Unauthorized surveillance.

f. Consumer deception.

g. Illegal profiling.

O.4 Human Oversight

Material business decisions affecting customers, workers, residents, or compliance obligations shall remain subject to meaningful human review.

SCHEDULE P

INSIDER THREAT MANAGEMENT FRAMEWORK

P.1 Objective

Partners shall implement safeguards against insider misuse of systems, data, facilities, financial assets, or confidential information.

P.2 Monitoring Controls

Controls may include:

a. Access logging.

b. Privileged account monitoring.

c. Activity reviews.

d. Data loss prevention measures.

e. Segregation of duties.

f. Behavioural risk indicators.

P.3 Escalation

Suspicious insider activity shall be reported to IVY Nest immediately.

SCHEDULE Q

CRISIS MANAGEMENT & REPUTATIONAL RISK GOVERNANCE

Q.1 Crisis Events

A crisis may include:

a. Fatal incidents.

b. Major cyberattacks.

c. Large-scale data breaches.

d. Regulatory raids.

e. Major media investigations.

f. Human trafficking allegations.

g. System-wide outages.

h. Public safety emergencies.

Q.2 Crisis Communication

Partners shall not issue public statements relating to IVY Nest without authorization.

Q.3 Media Escalation

All media inquiries involving IVY Nest shall be escalated immediately to designated representatives.

Q.4 Reputation Protection

Partners shall cooperate in remediation, communication, and stakeholder management efforts.

SCHEDULE R

COMPLIANCE COMMITTEE CHARTER

R.1 Establishment

IVY Nest may establish one or more Governance Committees, Compliance Committees, Risk Management Committees, Ethics Committees, Cybersecurity Committees, Data Protection Committees, or other oversight bodies, either on a permanent or ad hoc basis, to supervise implementation of this Policy. Such committees may exercise powers delegated by the applicable governing authority in accordance with internal governance requirements.

R.2 Responsibilities

The Committee may oversee:

a. Partnership risk management.

b. Regulatory compliance.

c. Data protection governance.

d. Cybersecurity oversight.

e. Investigation reviews.

f. High-risk partner approvals.

g. Audit findings.

h. Blacklisting decisions.

i. Crisis management.

j. Policy governance.

R.3 Reporting

The Committee shall periodically report material matters to senior management and/or the Board.

SCHEDULE S

ENTERPRISE TRAINING & AWARENESS REQUIREMENTS

S.1 Training Obligation

Partners shall ensure that relevant personnel receive periodic training on:

a. Ethics.

b. Anti-corruption.

c. Data protection.

d. Cybersecurity.

e. Workplace conduct.

f. Labour compliance.

g. Safety requirements.

h. Fraud prevention.

i. Consumer protection.

S.2 Evidence

Partners shall maintain training records and make them available upon request.

SCHEDULE T

GLOBAL HUMAN RIGHTS COMMITMENT

T.1 Commitment

IVY Nest expects all partners to respect internationally recognized human rights principles.

T.2 Prohibited Conduct

Partners shall not engage in:

a. Human trafficking.

b. Child exploitation.

c. Forced labour.

d. Modern slavery.

e. Coercive employment practices.

f. Inhumane treatment.

T.3 Supply Chain Responsibility

Partners shall exercise reasonable diligence within their own supply chains.

SCHEDULE U

DATA RETENTION & DESTRUCTION MATRIX

U.1 Minimum Standards

Partners shall maintain documented retention schedules.

U.2 Secure Destruction

Upon expiration of retention requirements, information shall be securely destroyed using industry-accepted methods.

U.3 Destruction Certification

IVY Nest may require written certification of destruction.

SCHEDULE V

ENTERPRISE PARTNER CODE OF CONDUCT

All partners shall:

a. Act honestly.

b. Act ethically.

c. Comply with applicable laws.

d. Respect customer rights.

e. Protect confidential information.

f. Maintain accurate records.

g. Avoid conflicts of interest.

h. Prevent corruption.

i. Protect workers.

j. Promote safe operations.

k. Cooperate with audits.

l. Support investigations.

m. Protect brand integrity.

n. Maintain cybersecurity safeguards.

o. Report misconduct.

Schedule W

Delegation Of Authority (DOA) Matrix

W.1 Purpose

This Delegation of Authority ("DOA") Matrix establishes the approval hierarchy, financial authority, governance responsibilities, escalation requirements, and decision-making powers applicable to partnerships, strategic alliances, procurement activities, contractual arrangements, regulatory matters, dispute resolution, emergency actions, and other matters governed by this Policy.

The DOA Matrix is intended to ensure accountability, segregation of duties, appropriate internal controls, enterprise risk management, regulatory compliance, and transparent decision-making.

W.2 General Principles

a. All approvals shall be exercised honestly, reasonably, independently, and in the best interests of IVY Nest.

b. Approval Authority shall be exercised only within delegated authority.

c. Matters exceeding delegated authority shall be escalated to the next higher Approval Authority.

d. Monetary limits shall include the total contractual value, renewals, amendments, extensions, recurring commitments, and any associated financial obligations.

e. Artificial splitting of transactions to avoid approval thresholds is strictly prohibited.

f. Higher Approval Authorities may review, modify, or revoke approvals granted by subordinate authorities where permitted by applicable law.

g. Emergency approvals shall be documented and ratified in accordance with Clause W.12 of this Schedule.

W.3 Approval Authority Levels

Level	Approval Authority

Level 1	Department Head / Functional Manager
Level 2	Business Head / Operations Head
Level 3	Executive Management / Senior Management
Level 4	Designated Partner(s), Managing Partner(s), Director(s), Proprietor, or Equivalent Governing Authority
Level 5	Governing Authority acting collectively, where applicable

W.4 Financial Approval Matrix

Total Contract Value	Approval Authority
Up to ₹5,00,000	Level 1
Above ₹5,00,000 up to ₹25,00,000	Level 2
Above ₹25,00,000 up to ₹1,00,00,000	Level 3
Above ₹1,00,00,000	Level 4
Transactions involving extraordinary strategic, regulatory, or enterprise-wide implications	Level 5

The Governing Authority may revise these monetary thresholds from time to time without requiring amendment of the main Policy.

W.5 Partnership Approval Matrix

Partnership Category	Minimum Approval Authority
Operational Vendor Partnerships	Level 1
Routine Service Agreements	Level 2

Technology and API Partnerships	Level 3
Data Processing or Data Sharing Partnerships	Level 3
Strategic Commercial Alliances	Level 4
International Partnerships	Level 4
Joint Ventures	Level 5
Equity Investments or Strategic Acquisitions	Level 5

W.6 Regulatory & Compliance Decisions

The following matters shall require approval of not less than Level 4 unless otherwise required by law:

a. Regulatory settlements.

b. Significant regulatory disclosures.

c. Self-reporting to regulatory authorities.

d. Major compliance remediation programmes.

e. Enterprise-wide regulatory investigations.

f. Material sanctions or export-control matters.

g. Cross-border data transfer arrangements presenting elevated regulatory risk.

W.7 Litigation Authority

Matter	Minimum Approval
Routine legal notices	Level 2
Legal replies	Level 3
Civil proceedings	Level 4
Criminal complaints	Level 4
Arbitration proceedings	Level 4

Appeals before higher judicial forums	Level 5
Settlement of litigation exceeding delegated financial limits	Level 5

Legal Counsel may provide legal advice but shall not independently approve commercial settlements unless specifically authorized.

W.8 Suspension & Restriction Authority

The following actions may be approved:

Action	Approval Authority
Temporary operational restriction	Level 2
Temporary suspension of partnership	Level 3
Suspension involving regulatory concerns	Level 4
Suspension involving fraud, financial crime, cybersecurity, or guest safety	Level 4
Enterprise-wide suspension affecting multiple partners	Level 5

W.9 Termination Authority

Matter	Minimum Approval
Routine contract termination	Level 2
Material Breach termination	Level 3
Regulatory termination	Level 4
Fraud, corruption, sanctions, or criminal misconduct	Level 4
Termination of strategic partnerships	Level 5

W.10 Blacklisting Authority

Permanent or temporary blacklisting may only be approved by Level 4 or higher after considering:

a. Nature and seriousness of misconduct.

b. Regulatory findings.

c. Material Breach.

d. Fraud.

e. Repeated contractual defaults.

f. Financial crime.

g. Cybersecurity incidents.

h. Guest safety concerns.

i. Previous corrective actions.

Where reasonably practicable, the affected Partner shall be afforded an opportunity to present its explanation before permanent blacklisting, except where immediate action is required by law, regulatory direction, public safety, fraud prevention, cybersecurity protection, or other compelling circumstances.

W.11 Policy Waivers & Exceptions

No waiver of this Policy shall be granted unless:

a. The request is documented.

b. Business justification is recorded.

c. Compliance implications are assessed.

d. Legal implications are considered where appropriate.

e. The appropriate Approval Authority grants written approval.

No waiver shall permit unlawful conduct or violation of applicable law.

W.12 Emergency Powers

In circumstances involving imminent risk to:

a. Human life.

b. Guest safety.

c. Public safety.

d. Cybersecurity.

e. Critical Infrastructure.

f. Business continuity.

g. Regulatory compliance.

h. Financial systems.

i. Personal Data.

j. Confidential Information.

the highest available Approval Authority may authorize immediate protective action without prior completion of ordinary approval procedures.

All emergency decisions shall:

a. Be documented.

b. Record reasons for urgency.

c. Identify the approving authority.

d. Be reported to the Governing Authority as soon as reasonably practicable.

e. Be reviewed for ratification within **30 calendar days**, unless a shorter period is required by applicable law or internal governance requirements.

W.13 Segregation of Duties

No individual shall:

a. Initiate,

b. Review,

c. Approve,

d. Execute,

e. Certify,

f. Audit,

the same transaction where such concentration of authority may create a material conflict of interest, fraud risk, governance failure, or internal control weakness, except where unavoidable due to organizational structure and expressly authorized by the Governing Authority with appropriate compensating controls.

W.14 Residual Risk Acceptance

Where a proposed partnership, transaction, or activity remains classified as High Risk or Critical Risk after implementation of available mitigation measures, acceptance of the residual risk shall require documented approval by Level 4 or Level 5, as appropriate.

The approval record shall include:

a. Nature of the residual risk.

b. Mitigation measures implemented.

c. Business justification.

d. Duration of approval.

e. Monitoring requirements.

f. Review schedule.

W.15 Review of Delegation Matrix

This Delegation of Authority Matrix shall be reviewed:

a. At least annually.

b. Following significant organizational restructuring.

c. Following material changes in applicable law.

d. Following significant regulatory findings.

e. Following major fraud or cybersecurity incidents.

f. Following changes in enterprise risk appetite.

g. Whenever otherwise considered necessary by the Governing Authority.

The Governing Authority may amend this Schedule without requiring revision of the substantive provisions of this Policy, provided that such amendments remain consistent with applicable law and IVY Nest's governance framework.

SCHEDULE X

ENTERPRISE DOCUMENT CLASSIFICATION MATRIX

X.1 Purpose

This Schedule establishes the enterprise-wide document classification framework applicable to all records, documents, files, reports, agreements, correspondence, communications, electronic records, digital content, and other documentary information created, received, maintained, processed, transmitted, stored, or disposed of by IVY Nest or its Partners.

The objective of this Schedule is to ensure consistent protection of information assets, effective information governance, regulatory compliance, business continuity, confidentiality, integrity, availability, and appropriate lifecycle management of documentary information.

X.2 Scope

This Schedule applies to:

a. Physical documents.

b. Electronic documents.

c. Digital records.

d. Contracts and agreements.

e. Legal records.

f. Financial records.

g. Human Resource records.

h. Customer documentation.

i. Vendor documentation.

j. Operational records.

k. Regulatory correspondence.

l. Email communications.

m. Cloud-hosted documents.

n. Audio, video, photographic, and multimedia records.

o. Any other documentary information created or maintained by IVY Nest.

X.3 Classification Principles

Document classification shall be determined based upon:

a. Confidentiality requirements.

b. Regulatory obligations.

c. Commercial sensitivity.

d. Legal privilege.

e. Privacy obligations.

f. Business criticality.

g. Cybersecurity risks.

h. Contractual obligations.

i. Operational importance.

j. Potential impact of unauthorized disclosure, alteration, destruction, or loss.

X.4 Enterprise Document Classification Matrix

Classification	Description	Examples	Access	Encryption	External Sharing
Public	Information approved for unrestricted public disclosure.	Website content, brochures, published policies, press releases, public advertisements.	Unrestricted.	Not mandatory.	Permitted.
Internal	Information intended only for internal operational use.	Internal procedures, meeting agendas, operational manuals, training materials.	Authorized personnel.	Recommended.	Only with authorization.

Confidential	Commercially sensitive or operationally important information requiring controlled access.	Contracts, pricing, vendor agreements, customer communications, internal reports, audit reports.	Need-to-know basis.	Required.	Restricted.
Restricted	Highly sensitive information requiring enhanced protection due to legal, regulatory, cybersecurity, financial, or operational risk.	Financial records, legal advice, investigations, security assessments, compliance reports, incident response documentation, regulatory submissions.	Limited authorized personnel.	Mandatory.	Exceptional approval required.
Highly Restricted	Information whose unauthorized disclosure may result in severe legal, regulatory, financial, cybersecurity, operational, or reputational harm.	Encryption keys, authentication credentials, source code, cryptographic materials, disaster recovery plans, penetration testing reports, privileged legal communications, merger and acquisition documentation, executive strategic plans.	Strictly limited.	Mandatory with enhanced security controls.	Prohibited unless expressly authorized.

X.5 Classification Responsibilities

Every document owner shall ensure that documents are:

a. Correctly classified.

b. Properly labelled.

c. Stored securely.

d. Shared only with authorized persons.

e. Reviewed periodically.

f. Retained for the applicable retention period.

g. Securely archived or destroyed when no longer required.

X.6 Access Control

Access to classified documents shall be governed by:

a. Business need.

b. Least privilege principle.

c. Need-to-know principle.

d. Role-based access controls.

e. Multi-factor authentication where appropriate.

f. Segregation of duties.

g. Periodic access reviews.

X.7 Document Labelling

Where reasonably practicable, documents should clearly indicate their classification.

Examples include:

PUBLIC

INTERNAL

CONFIDENTIAL

RESTRICTED

HIGHLY RESTRICTED

Electronic document management systems may automatically apply classification labels where technically feasible.

X.8 Storage Requirements

Documents shall be stored using security controls proportionate to their classification.

Examples include:

a. Locked physical storage.

b. Secure filing systems.

c. Encrypted cloud storage.

d. Secure document repositories.

e. Access-controlled servers.

f. Backup repositories.

g. Disaster recovery storage.

h. Secure off-site archival facilities.

X.9 Transmission Requirements

Documents shall only be transmitted through authorized communication channels appropriate to their classification.

Additional safeguards may include:

a. Encryption.

b. Password protection.

c. Digital signatures.

d. Secure file transfer mechanisms.

e. Access-controlled collaboration platforms.

f. Identity verification.

g. Audit logging.

X.10 Printing, Copying and Disposal

Printing, copying, scanning, photographing, exporting, or reproducing Restricted or Highly Restricted documents shall only occur where operationally necessary and authorized.

Disposal shall occur through secure destruction methods appropriate to the document classification, including shredding, secure deletion, cryptographic erasure, or other approved destruction techniques.

X.11 Legal Hold

Documents subject to:

a. Litigation.

b. Arbitration.

c. Regulatory investigation.

d. Audit.

e. Law enforcement request.

f. Government inquiry.

g. Internal investigation.

shall not be altered, deleted, destroyed, or disposed of until the Legal Hold has been formally released.

X.12 Periodic Review

Document classifications shall be reviewed:

a. At least annually.

b. Following material changes to document content.

c. Following changes in applicable law.

d. Following cybersecurity incidents.

e. Following changes in business operations.

f. Following mergers, acquisitions, restructuring, or strategic initiatives.

g. Whenever otherwise required by the Governing Authority.

X.13 Non-Compliance

Failure to comply with this Schedule may constitute Material Non-Compliance or a Material Breach under this Policy and may result in corrective action, disciplinary proceedings, suspension of access privileges, contractual remedies, termination of partnership, recovery of losses, regulatory reporting where legally required, or any other action available under applicable law or contract.

X.14 Relationship with Other Policies

This Schedule shall be read together with:

a. Information Security Policy.

b. Data Protection & Privacy Policy.

c. Record Retention & Secure Destruction Policy.

d. Cybersecurity Policy.

e. Incident Response Policy.

f. Partnership Policy.

g. Confidentiality obligations.

h. Applicable contractual commitments.

In the event of inconsistency, the higher standard of protection shall apply unless otherwise required by applicable law.

X.15 Review and Amendment

This Schedule shall be reviewed:

a. At least annually.

b. Following significant legal or regulatory changes.

c. Following major cybersecurity incidents.

d. Following material governance changes.

e. Following recommendations arising from audits or risk assessments.

f. Whenever directed by the Governing Authority.

The Governing Authority may amend this Schedule from time to time without requiring amendment of the substantive provisions of this Policy, provided such amendments remain consistent with applicable law and IVY Nest's enterprise governance framework.

SCHEDULE Y

ENTERPRISE DATA CLASSIFICATION MATRIX

Y.1 Purpose

This Schedule establishes the enterprise-wide data classification framework for the identification, classification, handling, storage, processing, transmission, sharing, retention, archival, and secure disposal of data processed by IVY Nest and its Partners.

The objective of this Schedule is to ensure appropriate protection of information assets, compliance with applicable data protection and cybersecurity laws, effective enterprise risk management, business continuity, regulatory compliance, and preservation of the confidentiality, integrity, availability, authenticity, and resilience of organizational data.

Y.2 Scope

This Schedule applies to all structured and unstructured data processed by or on behalf of IVY Nest, including but not limited to:

a. Personal Data.

b. Customer Data.

c. Partner Data.

d. Employee Data.

e. Vendor Data.

f. Financial Data.

g. Accounting Records.

h. Booking and Reservation Data.

i. Property Information.

j. Identity Verification Records.

k. Payment Information.

l. Operational Data.

m. Business Intelligence.

n. Source Code.

o. APIs and Integration Data.

p. Artificial Intelligence models and training datasets.

q. Machine learning datasets.

r. Cloud-hosted information.

s. Database records.

t. Cybersecurity logs.

u. Audit trails.

v. Backup data.

w. Metadata.

x. Any other electronic or digital information processed by IVY Nest.

Y.3 Data Classification Principles

Data shall be classified based upon:

a. Legal obligations.

b. Privacy obligations.

c. Business sensitivity.

d. Confidentiality requirements.

e. Regulatory obligations.

f. Cybersecurity risks.

g. Commercial value.

h. Operational importance.

i. Criticality to business continuity.

j. Potential impact arising from unauthorized access, disclosure, alteration, destruction, corruption, or loss.

Y.4 Enterprise Data Classification Matrix

Classification	Description	Examples	Minimum Protection
Public Data	Information approved for unrestricted public disclosure.	Website content, public announcements, published policies, marketing material, press releases.	Basic integrity protection.
Internal Data	Operational information intended solely for internal business use.	Internal reports, operational procedures, meeting notes, internal dashboards, training content.	Role-based access control and reasonable security measures.
Confidential Data	Information whose unauthorized disclosure may adversely affect IVY Nest, its customers, Partners, employees, or commercial interests.	Customer records, vendor agreements, pricing information, contracts, invoices, booking history, operational analytics, audit reports.	Encryption, authentication, logging, least-privilege access, monitoring.
Restricted Data	Highly sensitive information requiring enhanced protection due to legal, regulatory, financial, cybersecurity, or operational significance.	Personal Data, identity documents, KYC information, financial statements, payment information, security logs, investigation records, legal documentation, compliance reports.	Strong encryption, multi-factor authentication, strict access controls, continuous monitoring, audit logging.
Highly Restricted Data	Information whose unauthorized disclosure, compromise, alteration, or destruction could result in severe legal, regulatory, financial,	Encryption keys, API secrets, cryptographic materials, source code repositories, production credentials, disaster recovery information, penetration testing reports, privileged legal communications, AI	Maximum security controls, hardware-backed protection where appropriate, privileged access management, enhanced monitoring, segregation, and

	cybersecurity, operational, or reputational harm.	model parameters, security architecture, digital certificates.	formal approval for access.

Y.5 Special Categories of Data

The following categories shall receive additional protection where applicable:

a. Personal Data.

b. Sensitive Personal Data or any equivalent category recognised under applicable law.

c. Financial Data.

d. Authentication Credentials.

e. Source Code.

f. Cryptographic Keys.

g. Artificial Intelligence training data.

h. Machine Learning models.

i. Cybersecurity logs.

j. Incident Response documentation.

k. Digital Identity records.

l. Biometric information, where lawfully processed.

m. Any other data designated as requiring enhanced protection by the Governing Authority.

Y.6 Data Ownership

Each category of enterprise data shall have an identified Data Owner responsible for:

a. Appropriate classification.

b. Accuracy.

c. Security.

d. Access authorization.

e. Retention.

f. Regulatory compliance.

g. Periodic review.

Operational responsibility may be delegated to designated Data Custodians or System Owners without transferring overall accountability.

Y.7 Data Access Management

Access to enterprise data shall be granted only on the basis of:

a. Legitimate business need.

b. Least privilege.

c. Need-to-know.

d. Role-based access control.

e. Multi-factor authentication where appropriate.

f. Segregation of duties.

g. Periodic access review.

h. Immediate revocation upon termination or change of role.

Y.8 Storage and Protection

Data shall be stored using security measures proportionate to its classification, including where appropriate:

a. Encryption at rest.

b. Encryption in transit.

c. Secure cloud infrastructure.

d. Secure database architecture.

e. Network segmentation.

f. Backup and disaster recovery.

g. Access monitoring.

h. Integrity verification.

i. Endpoint protection.

j. Secure key management.

Y.9 Data Transmission

Enterprise data shall only be transmitted using authorized communication channels appropriate to its classification.

Where applicable, transmission safeguards may include:

a. End-to-end encryption.

b. Digital signatures.

c. Secure APIs.

d. Virtual Private Networks (VPNs).

e. Secure file transfer mechanisms.

f. Identity verification.

g. Integrity validation.

Y.10 Cross-Border Data Transfers

Cross-border transfers of data shall be undertaken only where permitted by applicable law, contractual commitments, regulatory requirements, and IVY Nest's approved governance framework.

Where appropriate, IVY Nest may require:

a. Data transfer agreements.

b. Security assessments.

c. Privacy impact assessments.

d. Regulatory approvals.

e. Risk assessments.

f. Technical safeguards.

g. Ongoing compliance monitoring.

Y.11 Data Retention and Secure Disposal

Data shall be retained only for the period necessary to satisfy:

a. Business requirements.

b. Contractual obligations.

c. Legal obligations.

d. Regulatory requirements.

e. Litigation hold.

f. Audit requirements.

Upon expiry of the applicable retention period, data shall be securely deleted, anonymized, destroyed, archived, or otherwise disposed of using approved methods appropriate to its classification.

Y.12 Data Breach and Security Incidents

Any actual or suspected unauthorized access, disclosure, alteration, destruction, corruption, loss, compromise, ransomware incident, malware infection, credential compromise, or other security incident involving enterprise data shall be reported immediately through IVY Nest's Incident Response and Data Breach Management procedures.

Appropriate containment, investigation, remediation, recovery, documentation, and regulatory notification measures shall be implemented where required by applicable law.

Y.13 Monitoring and Audit

IVY Nest may conduct periodic reviews, monitoring, compliance assessments, vulnerability assessments, penetration testing, access reviews, security audits, and other verification activities to ensure continued compliance with this Schedule.

Partners shall cooperate with reasonable audit and compliance activities in accordance with applicable contractual obligations.

Y.14 Non-Compliance

Failure to comply with this Schedule may constitute Material Non-Compliance or a Material Breach under this Policy and may result in:

a. Corrective action.

b. Suspension of access privileges.

c. Enhanced monitoring.

d. Contractual remedies.

e. Termination of partnership.

f. Recovery of losses.

g. Regulatory reporting where legally required.

h. Civil or criminal proceedings where applicable.

i. Any other remedy available under applicable law or contract.

Y.15 Relationship with Other Policies

This Schedule shall be read together with:

a. Data Protection & Privacy Policy.

b. Information Security Policy.

c. Cybersecurity Policy.

d. Record Retention & Secure Destruction Policy.

e. Incident Response & Data Breach Management Policy.

f. Partnership Policy.

g. Confidentiality obligations.

h. Applicable contractual commitments.

Where two policies prescribe different standards, the higher standard of protection shall apply unless otherwise required by applicable law.

Y.16 Review and Amendment

This Schedule shall be reviewed:

a. At least annually.

b. Following significant legal or regulatory changes.

c. Following material cybersecurity incidents.

d. Following changes in technology architecture.

e. Following changes in enterprise risk assessments.

f. Following major organizational restructuring.

g. Following recommendations arising from audits, investigations, or regulatory inspections.

h. Whenever otherwise directed by the Governing Authority.

The Governing Authority may amend this Schedule from time to time without requiring amendment of the substantive provisions of this Policy, provided that such amendments remain consistent with applicable law and IVY Nest's enterprise governance framework.

SCHEDULE Z

VENDOR EXIT & OFFBOARDING CHECKLIST

Z.1 Purpose

This Schedule establishes the enterprise-wide Vendor Exit and Offboarding Framework applicable to all Partners, vendors, suppliers, contractors, consultants, technology providers, strategic alliance participants, service providers, channel partners, intermediaries, and other third parties upon suspension, expiration, termination, non-renewal, completion, or cessation of any business relationship with IVY Nest.

The objective of this Schedule is to ensure an orderly, secure, legally compliant, commercially appropriate, and risk-controlled exit process that protects IVY Nest's legal rights, information assets, business continuity, customers, intellectual property, financial interests, regulatory obligations, and reputation.

Z.2 Applicability

This Schedule applies where a partnership ends due to:

a. Contract expiry.

b. Mutual termination.

c. Termination for convenience.

d. Termination for Material Breach.

e. Fraud or misconduct.

f. Regulatory direction.

g. Insolvency or bankruptcy.

h. Change in ownership or control.

i. Persistent non-performance.

j. Force Majeure.

k. Business restructuring.

l. Strategic realignment.

m. Any other lawful cessation of the relationship.

Z.3 Offboarding Governance

The designated Approval Authority shall coordinate the offboarding process with support from the relevant business units, including Legal, Compliance, Finance, Information Technology, Information Security, Data Protection, Procurement, Operations, and other stakeholders as appropriate.

Where the circumstances involve fraud, cybersecurity incidents, regulatory investigations, litigation, or other material risks, enhanced offboarding procedures may be implemented.

Z.4 Vendor Exit Checklist

Before a partnership is formally closed, the following matters shall be reviewed and documented where applicable:

A. Contractual Closure

□ Confirm termination or expiry date.

□ Verify contractual notice requirements.

□ Confirm all contractual obligations have been completed or appropriately waived.

□ Record reasons for termination.

□ Verify completion of exit approvals.

B. Financial Closure

□ Outstanding invoices reviewed.

□ Payments reconciled.

☐ Security deposits adjusted where applicable.

☐ Refunds processed where required.

☐ Outstanding liabilities identified.

☐ Taxes and statutory obligations reviewed.

☐ Final financial reconciliation completed.

C. Information & Data Protection

☐ Return of Confidential Information.

☐ Secure deletion of IVY Nest data.

☐ Confirmation of data destruction where required.

☐ Return or deletion of customer information.

☐ Removal of backup copies where applicable.

☐ Revocation of data-sharing permissions.

☐ Compliance with applicable data protection obligations verified.

D. Technology & Access Management

☐ Disable system accounts.

☐ Revoke user credentials.

☐ Remove API access.

☐ Revoke VPN access.

☐ Remove cloud platform permissions.

☐ Disable remote access.

☐ Recover company-issued devices where applicable.

☐ Rotate passwords, tokens, certificates, or cryptographic keys where necessary.

E. Intellectual Property

☐ Return IVY Nest intellectual property.

□ Return licensed software.

□ Confirm cessation of trademark use.

□ Remove branding from websites and marketing materials.

□ Return confidential technical documentation.

□ Verify compliance with intellectual property obligations.

F. Operational Transition

□ Transition active work.

□ Transfer documentation.

□ Handover customer information where authorized.

□ Identify replacement vendor if required.

□ Ensure business continuity measures are implemented.

□ Confirm no critical operational dependency remains.

G. Regulatory & Compliance

□ Legal Hold requirements reviewed.

□ Regulatory investigations identified.

□ Audit obligations completed.

□ Record retention obligations confirmed.

□ Compliance certificates obtained where applicable.

□ Regulatory notifications completed where legally required.

H. Litigation Review

□ Pending disputes identified.

□ Arbitration status reviewed.

□ Court proceedings reviewed.

□ Preservation of evidence confirmed.

□ Insurance notifications completed where required.

□ Recovery actions documented.

I. Security Verification

□ Security logs reviewed.

□ Cybersecurity incidents assessed.

□ Security monitoring completed.

□ Vulnerability assessment performed where appropriate.

□ Incident Response records updated.

□ Digital forensic preservation completed where required.

J. Final Management Review

□ Business Unit approval.

□ Compliance review.

□ Legal review.

□ Finance clearance.

□ Information Security clearance.

□ Data Protection review.

□ Executive approval where required.

□ Final closure approval recorded.

Z.5 Exit Certification

Where appropriate, IVY Nest may require the exiting Partner to provide written certification confirming that:

a. All Confidential Information has been returned or securely destroyed.

b. No unauthorized copies have been retained.

c. Access to IVY Nest systems has ceased.

d. Intellectual Property obligations have been complied with.

e. Applicable contractual obligations have been fulfilled.

f. Continuing confidentiality obligations are acknowledged.

g. Applicable legal, regulatory, privacy, cybersecurity, and contractual obligations continue to be observed following termination where required.

Z.6 Post-Termination Obligations

Termination of a partnership shall not affect obligations intended to survive termination, including but not limited to:

a. Confidentiality.

b. Intellectual Property.

c. Data Protection.

d. Record Retention.

e. Legal Hold.

f. Regulatory cooperation.

g. Audit rights.

h. Indemnity.

i. Dispute resolution.

j. Payment obligations.

k. Any other obligations expressly stated to survive termination.

Z.7 Exit Risk Assessment

Where appropriate, IVY Nest may conduct a final exit risk assessment considering:

a. Outstanding legal exposure.

b. Financial exposure.

c. Cybersecurity risks.

d. Data protection risks.

e. Reputational risks.

f. Operational dependencies.

g. Customer impact.

h. Regulatory implications.

i. Third-party supply chain risks.

j. Business continuity risks.

Appropriate mitigation measures shall be implemented before final closure where reasonably practicable.

Z.8 Lessons Learned

Following completion of significant vendor exits, IVY Nest may conduct a post-offboarding review to identify:

a. Governance improvements.

b. Procurement improvements.

c. Contract management improvements.

d. Cybersecurity improvements.

e. Data governance improvements.

f. Risk management improvements.

g. Supplier performance trends.

h. Business continuity improvements.

Findings may be incorporated into future procurement, due diligence, contracting, and partnership governance processes.

Z.9 Non-Compliance

Failure by a Partner to comply with this Schedule, including failure to return Confidential Information, unauthorized retention of data, continued use of IVY Nest Intellectual Property, refusal to surrender access credentials, obstruction of the offboarding process, or any other material non-compliance, may constitute a Material Breach and may result in:

a. Suspension of pending payments where contractually permissible.

b. Recovery of losses.

c. Blacklisting.

d. Injunctive relief.

e. Civil or criminal proceedings where applicable.

f. Regulatory reporting where legally required.

g. Any other contractual or legal remedy available under applicable law.

Z.10 Review and Amendment

This Schedule shall be reviewed:

a. At least annually.

b. Following significant organizational restructuring.

c. Following material legal or regulatory changes.

d. Following significant cybersecurity or data breach incidents.

e. Following major procurement reviews.

f. Following recommendations arising from audits, investigations, or regulatory inspections.

g. Whenever otherwise directed by the Governing Authority.

The Governing Authority may amend this Schedule from time to time without requiring amendment of the substantive provisions of this Policy, provided that such amendments remain consistent with applicable law and IVY Nest's enterprise governance framework.

FINAL BOARD ADOPTION RESOLUTION

This Partnership Policy & Strategic Alliance Governance Framework, together Annexures, Schedules, Compliance Certifications, Risk Frameworks, Audit Controls, and Governance Mechanisms, shall constitute the official enterprise partnership governance standard of IVY Nest Apartments.

All partnerships, strategic alliances, franchise arrangements, property-owner relationships, technology integrations, vendors, contractors, affiliates, distribution partners, managed property operators, marketing partners, mobility providers, and ecosystem participants shall be governed by this Framework unless superseded by stricter contractual or statutory requirements.

The Board, Compliance Committee, Management, Employees, Contractors, and Partners are expected to support the implementation, monitoring, enforcement, and continuous improvement of this Framework to ensure legal compliance, ethical operations, customer trust, worker protection, data security, operational resilience, and sustainable growth.