Remote Worker Trust & Sanctions Compliance Policy

Purpose

Protect the organization from remote employment fraud, insider risk, and sanctions violations by embedding identity verification, sanctions screening, and secure delivery practices into the project lifecycle.

Scope

Applies to:

- All remote hires and contractors with access to source code, production systems, sensitive data or financial assets
- All vendors / staffing agencies supplying personnel for project delivery

Policy Requirements

1. Risk Classification at Intake
    a. All roles classified P0/P1 (high privilege or sensitive access) require enhanced vetting before staffing approval.
2. Enhanced Identity & Sanctions Screening
    a. Government-issued ID verification with liveness detection.
    b. Cross-check against U.S. and international sanctions/watchlists (OFAC, UN, EU).
    c. No offer without Staffing Risk Review Board sign-off.
3. Secure Onboarding
    a. Corporate-issued device with MDM.
    b. Hardware-based MFA.
    c. Geofencing and prohibition of remote-control tools.
    d. Least privilege until passing initial trust/quality gates
4. Vendor & Contractor Controls
    a. No subcontracting without disclosure and re-verification.
    b. Contract clauses requiring sanctions, compliance and identity attestations.
    c. Quarterly spot checks of active personnel.
5. Monitoring & Escalation
    a. Continuous user and entity behavior analytics (UEBA).
    b. Immediate escalation to Legal/Compliance if sanctions or insider-risk indicators arise.
    c. PMO coordinates incident response with HR, IT Security, and Legal.

PMO Checklist for High-Risk Remote Roles

Step	Description	Owner	Complete?
1.	**Role risk classification assigned (P0/P1)**	PMO Intake Lead	□
2.	**Enhanced ID verification (liveness + govt ID)**	HR / Vendor	□
3.	**Sanctions screening completed (OFAC, UN, EU)**	Compliance	□
4.	**Staffing Risk Review Board approval**	PMO + HR + Security	□
5.	**Secure device provisioned & MDM applied**	IT Ops	□
6.	**Hardware MFA enabled**	IT Security	□
7.	**Geofencing & prohibited tools policy enforced**	IT Security	□
8.	**Least-privilege applied (read-only until cleared)**	Project Lead	□
9.	**Vendor contract clauses verified & signed**	Procurement / Legal	□
10.	**Quarterly identity & sanctions re-check scheduled**	PMO Vendor Mgmt	□
11.	**UEBA baseline created & alerts configured**	IT Security	□
12.	**Incident response plan updated for REF scenario**	PMO + IR Team	□

Effective Date: [Insert Date]
Policy Owner: PMO Director
Review Cycle: Quarterly, or after any insider-risk incident.