EECHECK · ASIA BACKGROUND CHECK

Background Screening Policy Template

for Asia-Pacific

A Structured Framework for HR & Compliance Leaders

A compliant screening policy defines role-based tiers, jurisdiction-specific requirements, consent frameworks, data governance controls, and escalation procedures — transforming ad hoc screening into a defensible compliance program.

01

Policy Purpose & Scope of Application

Policy Purpose

- ✓ Protect the organization from fraud, misconduct, and regulatory risk
- ✓ Ensure compliance with applicable data protection and employment laws
- ✓ Align screening scope with role-specific risk exposure
- ✓ Maintain audit-ready documentation and governance oversight

Scope of Application

- Full-time employees
- Contract employees (if applicable)
- Directors and officers
- Regulated or licensed roles
- Temporary / project-based hires

Jurisdiction-specific variations may apply

02

Risk-Based Screening Framework & Scope Matrix

T1 — Administrative
Foundational checks

T2 — Professional
Enhanced credential checks

T3 — Regulated
Expanded regulatory checks

T4 — Executive
Comprehensive screening

Check Type	T1	T2	T3	T4
Identity Verification	✓	✓	✓	✓
CV Validation	✓	✓	✓	✓
Employment Verification	✓	✓	✓	✓
Education Verification	✓	✓	✓	✓
Professional License	—	If appl.	✓	✓
Criminal Record Check	—	Role dep.	✓	✓
Regulatory History	—	—	✓	✓
Credit Check	—	Role dep.	✓	✓
Sanctions Screening	—	✓	✓	✓
Conflict of Interest	—	—	✓	✓

All checks must comply with local legal permissibility requirements.

03

Jurisdictional Compliance & Consent Framework

Jurisdictional Requirements

- Conduct jurisdiction-specific legal assessments
- Adapt consent language per country
- Confirm permissibility of criminal, credit & social media checks
- Review cross-border data transfer obligations
- Reflect both role risk and legal boundaries in scope

Consent Framework Requirements

1. Written consent must be obtained
2. Scope of checks disclosed to candidate
3. Purpose of processing clearly defined
4. Cross-border transfer disclosure included
5. Data retention period specified
6. Consent records retained for audit

Consent forms must be reviewed locally — generic global templates may not comply.

04

Data Protection & Governance Controls

Encryption

Screening data encrypted in transit and at rest

Access Controls

Role-based access and multi-factor authentication

Access Logging

All system access logged and monitored

Data Retention

Defined retention schedules per jurisdiction

Secure Deletion

Documented secure deletion procedures

Incident Response

Formal framework for data breach handling

Data governance controls must be formally documented and regularly reviewed.

05

Discrepancy Management & Escalation

All discrepancies must be categorized, documented, and reviewed by designated authority.

Minor Inconsistency — **Clarification Request**

e.g. Small date gap or CV format difference

Material Inconsistency — **Secondary Verification**

e.g. Undisclosed employment or credential gap

Critical Finding — **Escalation to HR & Compliance**

e.g. Confirmed disqualification or fraud flag

Final hiring decisions must be documented. Employers retain full compliance responsibility.

06

Vendor Oversight & Cross-Border Data Controls

Vendor Oversight (If Outsourced)

- ✓ Vendor due diligence must be conducted
- ✓ Data protection controls reviewed before engagement
- ✓ Service-level agreements formally documented
- ✓ Escalation procedures clearly defined
- ✓ Audit rights included in vendor contracts

The employer retains ultimate compliance responsibility.

Cross-Border Data Transfer Controls

- Transfer mechanisms assessed per jurisdiction
- Data localization rules reviewed
- Access controls documented
- Data minimization principles applied
- Cross-border data mapping maintained

07

AI Governance & Documentation Requirements

AI & Automation Governance

- AI must not replace final human review
- Discrepancy materiality: human-assessed only
- Regulatory interpretation: human-led only
- Adverse hiring decisions must not be automated
- All AI usage must be documented

⚠ *AI enhances process efficiency — it does not replace human compliance judgment.*

Documentation & Audit Readiness

- Screening request logs
- Consent records
- Verification documentation
- Discrepancy decision rationale
- Vendor performance records
- Policy review documentation

08

Policy Review, Updates & Governance

When to Review the Policy

- Annually (minimum)
- Upon regulatory change
- Upon operational change
- Geographic expansion
- Vendor change or audit

Governance & Accountability

HR Leadership

Policy ownership and screening execution oversight

Compliance / Legal

Jurisdiction review, consent, and regulatory alignment

Risk Management

Tier classification, escalation, and vendor risk control

FAQ

Frequently Asked Questions & Final Takeaway

Q Can one policy apply across all Asian countries?

A A core policy can apply regionally, but jurisdiction-specific adaptations are required for consent, legal permissibility, and data transfers.

Q Who is responsible if screening is outsourced?

A The employer remains legally responsible for lawful processing and policy governance, even when a third-party vendor performs the checks.

Q Should screening tiers differ by industry?

A Yes — financial services, healthcare, education, and government-linked sectors may require deeper screening and more formal protocols.

Q How often should the policy be reviewed?

A At minimum annually, and sooner upon regulatory change, vendor change, operational expansion, or material updates to hiring practices.

Final Takeaway:

A written screening policy transforms ad hoc verification into a governed compliance framework — supporting defensible hiring across Asia-Pacific's diverse regulatory landscape.