RECRUITMENT SOLUTIONS BY

TANGSPAC

HR Security Policy

Version 1.1

1. Introduction

Tangspac Consulting is committed to safeguarding the confidentiality, integrity, and security of all HR-related data and processes. This policy outlines the necessary security measures to ensure compliance with Singapore's Personal Data Protection Act (PDPA) and other relevant laws governing employment practices.

2. Scope

This policy applies to:

- All Tangspac Consulting employees, including full-time, part-time, and contract staff.
- HR personnel, hiring managers, and any individual handling employee, contractor, or candidate data.
- Third-party service providers involved in background screening, or benefits administration.

3. Objectives

- Ensure confidentiality of all HR-related information, including employee records, payroll data, and recruitment details.
- Mitigate security risks in HR operations, including unauthorized access, data breaches, and improper handling of sensitive information.
- Ensure compliance with PDPA, employment regulations, and contractual obligations with clients.
- Reinforce security awareness among employees through regular campaigns and training.

4. Governance and Responsibilities

HR Leadership

- Enforces HR security measures and ensures compliance.
- Investigates and takes appropriate action on security incidents.

HR Team Members

- Handles personal data securely and in accordance with this policy.
- Reports any security concerns or breaches to the HR and IT security teams.

Employees & Contractors

- Adhere to client confidentiality agreements and HR security guidelines.
- Report any suspected data leaks or unauthorized access.

5. Confidentiality & Non-Disclosure of HR Data

- All employees handling HR data must strictly comply with data confidentiality concerning confidential employment-related information.
- Employment contracts, salary records, disciplinary records, and personal employee details must be stored securely and accessible only to authorized personnel.
- Verbal discussions about salary, performance, or employment status of employees are strictly prohibited, except on a need-to-know basis within HR.

6. Background Screening & Employee Verification

- All new hires (including full-time, part-time, and contractors) must undergo pre-employment background screening steps required by clients
- Background checks may include:
    - Identity verification (NRIC/FIN/Passport checks)
    - Employment history verification
    - Educational qualification checks
    - Reference checks
    - Criminal record and regulatory checks (where applicable)
- Candidates must provide written consent before any background screening is conducted.
- The results of background screenings are strictly confidential and must be reviewed only by authorized HR personnel and hiring managers of clients

7. Access Control & Security of HR Systems

- Access to HR systems (e.g., payroll software, employee records) must be role-based and granted on a need-to-know basis.
- Upon termination or resignation, employee HR system access must be revoked immediately.

8. Secure Handling of Recruitment & Employee Data

- Candidate Applications & Resumes:
    - Stored securely and not shared externally without explicit consent.
    - Access restricted to recruiters and hiring managers only.

9. Payroll & Benefits Security

- Payroll processing must be conducted through secure, encrypted systems with role-based access.
- Third-party payroll vendors must comply with PDPA and contractual data security clauses.
- Salary details must not be disclosed to any unauthorized personnel.
- Payroll modifications require dual approval to prevent fraud.

10. HR Security Awareness Campaigns & Training

- Periodic HR security awareness campaigns will be conducted through emails, and workshops.
- Security reminders on confidentiality of employment-related documents will be sent periodically.

11. Incident Reporting & Response

- Unauthorized access, data breaches, or security lapses involving HR data must be reported to HR leadership and IT security immediately.
- Disciplinary action, including termination or legal proceedings, may be taken for security violations.

12. Remote Work & BYOD (Bring Your Own Device) Security

- Storing HR-related data on personal devices or transferring HR documents via personal email is strictly prohibited.
- Accessing HR data on public Wi-Fi networks is only permitted if a VPN is used.

13. Third-Party Vendor & Outsourcing Security

- Any third-party vendor handling HR data (e.g., background check providers, payroll vendors) must comply with this policy.

- Confidentiality clauses and data protection obligations must be included in all vendor agreements.

14. Data Retention & Disposal

- Employee and candidate records must be retained only for the legally required period, after which they must be securely disposed of.
- Physical HR records must be shredded when no longer required.
- Digital HR records must be permanently deleted from systems according to the HR data retention policy.

15. Compliance & Legal Requirements

This policy aligns with:

- Personal Data Protection Act (PDPA) – Singapore
- Employment Act (Singapore)
- General Data Protection Regulation (GDPR) (if applicable to international candidates or clients)
- Any client-specific or contractual requirements related to HR data security

16. Contact Information

For HR security concerns, incidents, or policy clarifications, contact Tangspac Consulting's HR & IT Security Teams at sg.enquiry@tangspac.com.