PERSOL

Associate Handbook & Compliance Manual

PERSOL Singapore Pte Ltd

Version 1.2, Issued August 2026
(Internal use only)

TABLE OF CONTENTS

INTRODUCTION **2**

PART I - TERMS OF EMPLOYMENT **2**
- WORKING HOURS 2
- DRESS CODE 2
- PUNCTUALITY AND ATTENDANCE 2
- ABSENCE FROM WORK 3
- RESIGNATION / TERMINATION OF EMPLOYMENT 3
- FLEXIBLE WORK ARRANGEMENT REQUESTS 3

PART II - COMPENSATION AND SALARY ADMINISTRATION **4**
- COMPENSATION POLICY 4
- SALARY PAYMENT PERIOD 4
- OVERTIME PAY 4
- TIMESHEET & CLAIMS MANAGEMENT AND SUBMISSION 4

PART III - LEAVE BENEFITS **5**
- ANNUAL LEAVE 5
- MEDICAL LEAVE AND HOSPITALISATION LEAVE 5
- MATERNITY LEAVE 5
- PATERNITY LEAVE 6
- SHARED PARENTAL LEAVE 7
- CHILDCARE LEAVE 7
- EXTENDED CHILDCARE LEAVE 8
- RESERVIST LEAVE 8

PART IV - DUTY OF CONFIDENTIALITY **9**
PART V – POLICIES **9**
PART VI – COMPLIANCES DO'S AND DON'TS **10**
PART VII – GRIEVANCES **13**
PART VIII – QUALITY AND ENVIRONMENTAL **15**
PART IX – HEALTH AND SAFETY AT WORK **16**

WORKPLACE HEALTH & SAFETY ON-SITE HANDBOOK **17**

PRIVACY POLICY (version 7.2)

COMPLIANCE MANUAL (version 8.3)

Welcome to PERSOL!

We are delighted to have you on board. You are now part of a diverse and dynamic community of professionals working across a wide range of industries and regions around the world.

At PERSOL, we take great pride in our commitment to being a leading provider of workforce solutions, and we are dedicated to supporting your success every step of the way. This handbook contains important information to help you navigate your assignment and make the most of your experience with us.

Should you have any questions or need assistance, please don't hesitate to reach out to your Consultant or our HR Shared Services Officer.

We wish you every success in your journey with us!

Note:

- The company reserves the right to amend, modify, or revoke any policy or procedure outlined in the handbook/policies manual at its discretion, without prior notice. Associates are encouraged to check for updates regularly and adhere to the most current version of the policies.
- The updated Associate Handbook and Compliance Manual is retrievable at https://www.persolsingapore.com/page/psl-associate-handbook and the Privacy Policy is available on https://www.persolsingapore.com/policies. Please contact your Consultant-in-charge and/or HR Shared Service Officer should you require further clarification about the above policies and guidelines.

INTRODUCTION

This Associate Handbook ("this Handbook") is applicable to all temporary / contract employees ("Associates") employed by PERSOL Singapore Pte Ltd ("Company") and/or its subsidiaries placed on assignment with our clients ("Clients") for whom you are providing the services. For the avoidance of doubt, any reference to "us" or "we" shall refer to the Company and its subsidiaries. The respective officer in charge of your employment matters will be termed as "Consultant" or "HR Shared Service Officer" in this Handbook. The Supervisor to whom the Associate reports is referred throughout this Handbook as "Reporting Manager".

Should any provision in this Handbook contradict any applicable laws, the laws shall prevail.

You agree to comply with this Handbook (as may be amended from time to time) and the contents of this Handbook shall form part of your employment contract with us ("Employment Contract"). In the event of a conflict between terms and conditions herein and those contained in this Handbook, the Employment Contract shall prevail. We shall have the right to revise this Handbook from time to time as we deem fit.

PART I - TERMS OF EMPLOYMENT

WORKING HOURS

- Associates should observe the Client's working hours and official break time. Please refer to the working hours as specified in the main details of your Employment Contract.

- The Client reserves the right, at its sole discretion, to revise, amend or extend the working hours should the need arise.

DRESS CODE

- Maintaining a professional, business-like appearance is very important to the success of the Company and Clients. All Associates regardless of the interaction with clients, customers, suppliers, contractors or volunteers, project the reputation of the and Clients. Unless otherwise advised, Associates should dress in appropriate business attire and maintain a positive image as specified in the Clients' policy.

- For guidance on the dress code, please seek advice from your respective Reporting Manager or Client's HR Officer.

PUNCTUALITY AND ATTENDANCE

We trust you to be at your best. This means exhibiting the following attributes:

- Responsibility - Once you accept an assignment, we trust that you will fulfil your obligations to the best of your ability. You are required to provide a notice if you are unable to do so.
- Dependability - Honour your commitment to be at work on time every day, and to finish the tasks assigned to you.

If you are going to be late or absent from work, you must contact your Reporting Manager and/or Consultant and/or HR Shared Service Officer. Prior approval should be obtained before any lateness and absence from work.

Provide adequate notice for anticipated absences, such as vacation in accordance to notice requirement stated in the Employment Contract, in the absence of specific instruction from the Clients. If the Client has specific notice requirement, please follow those requirements. In the event of leave application for illness or personal emergency, provide a minimum of four hours' notice whenever possible.

Being late or absent without calling the Reporting Manager is unacceptable and hinders the day-to-day operations of the department and causes inconvenience to colleagues.

Unauthorised absence or tardiness and failure to inform will render Associates liable to disciplinary action.

ABSENCE FROM WORK

- Any absence from work for more than two (2) working days continuously without approval or prior notification to Reporting Manager with justifiable reason is a breach of contract and shall be grounds for immediate termination.

RESIGNATION / TERMINATION OF EMPLOYMENT

- This Employment Contract may be terminated by either party with notice period as specified in the main details of the Employment Contract, failing which salary in lieu of notice shall apply. Should the Associates decide to terminate the Employment Contract, Reporting Manager and Consultant and/or HR Shared Service Officer shall be notified immediately and without unreasonable delays.

- Company reserves its right to terminate the Employment Contract without notice or payment in lieu of notice in cases of
    - poor performance, neglect of duty
    - misconduct, conduct not beneficial to the interests of Company or the Clients
    - absences from work without justifiable reasons
    - being found guilty by the Company or Clients of a material or persistent breach of the terms of the Employment Contract, or any policies, rules and regulations
    - being convicted of a criminal offence other than traffic offences and any other offences which in the Company and Client's opinion would adversely affect its reputation or business relationships
    - providing any falsified information on your employment application/during an interview or failing a background check
    - breach of the rules, regulations, business and operational procedures of the Clients

- You will return all records, correspondence, letters, manuals, mailing lists, customer lists, price lists, advertising materials, supplies, keys, thumb drives, tapes or any other documents or property relating or belonging to the Client immediately, to the Reporting Manager or Client's HR Department upon the termination of the Employment Contract, whether requested to do so or not.

FLEXIBLE WORK ARRANGEMENT REQUESTS

- You have the right to request for a reasonable flexible work arrangements as defined under the Tripartite Guidelines for Flexible Work Arrangements (FWA) Requests in accordance with the applicable laws and regulations.
- All formal FWA requests shall be made in writing to the Company via the stipulated "Flexible Work Arrangement Request Form" and such request shall be subject to the Company and Client's approval.
- All informal FWA requests will be made directly to Client, subjected to Client's approval.

PART II - COMPENSATION AND SALARY ADMINISTRATION

COMPENSATION POLICY

- Remuneration is based on skills, aptitude, experience, education and job responsibilities. Associates are to take note that pay-rates are confidential and should never be discussed with the Clients or co-workers.
- Failure to observe this rule will result in disciplinary actions being taken.

SALARY PAYMENT PERIOD

- Salary will be paid in accordance with the payment period as specified in the main details of Employment Contract.
- Time sheets and relevant supporting documents are required to be approved by Reporting Manager and submitted to Consultant and/or HR Shared Service Officer by the stipulated deadline. Consultant and/or HR Shared Service Officer shall not be responsible for any delay in salary payment caused by late submission of time sheet.

OVERTIME PAY

- Overtime pay is payment for all work done in excess of the normal hours of work (excluding breaks). Overtime work must be authorised by the Reporting Manager concerned.
- The overtime rate payable is capped at the prevailing salary threshold as per the Singapore Employment Act.
- Please refer to main details of Employment Contract for your overtime entitlement.

TIMESHEET & CLAIMS MANAGEMENT AND SUBMISSION

- Submission of approved timesheet and/or expense claims must be received by the stipulated timeline as shared by the Consultant and/or HR Shared Service Officer during on-boarding.
- Failure to submit on time may result in delay of your salary processing.
- Should you require further assistance and/or clarifications on the monthly cut-off timeline, please contact your Consultant and/or HR Shared Service Officer.

PART III - LEAVE BENEFITS

- Associates should inform their Reporting Manager of leave notifications at least 5 working days in advance.
- For leave types that require supporting documents, Associates should ensure that they are submitted in a timely manner.
- For statutory leave as mandated by the government, please refer to the Ministry of Manpower (MOM) website for the latest updates.

ANNUAL LEAVE

- All legislated leave entitlement shall be applicable based on fulfilment of qualifying conditions according to MOM regulations.
- Non-legislated leave shall be subjected to the approval of the Reporting Manager and notified accordingly.
- Annual leave entitlement for new hires and exiting Associates will be pro-rated based on the number of completed months of service in the current year.
- Usage of annual leave to offset notice period during resignation is subject to the approval of the Reporting Manager.

MEDICAL LEAVE AND HOSPITALISATION LEAVE

- Associates with at least 3 months of continuous service are entitled to paid medical leave and hospitalization leave in a calendar year according to MOM guidelines. Medical leave and Hospitalization leave taken during the first 3 months of continuous service will be considered as unpaid leave.
- Associates must inform their Reporting Managers if they are unable to turn up for work and substantiate it with a medical certificate within 2 working days after he/she returns to work.
- The medical certificate must be submitted together with the leave application for the Reporting Manager's approval. Failure to submit medical certificates will result in the leave being recorded as annual leave or unpaid leave if the annual leave has been fully utilised.
- Unconsumed sick leave benefits will not be carried forward to the new Employment Contract and no payment shall be made in-lieu-of unconsumed sick leave benefit.

MATERNITY LEAVE

- Associates who have worked for at least 3 months and meet the eligibility criteria for Maternity / Paternity / Childcare Leave under the Employment Act (EA) or the Child Development Co-Savings Act (CDCA) will be eligible for such paid leave as prescribed by MOM.

- Please refer to the MOM website for more details.

Female Associates whose children are Singapore Citizens:

Eligibility	▪ Child is registered as a Singapore Citizen. ▪ 90 days of continuous service with the Company, before the birth of her child.

Entitlement	**<u>First and Second Child</u>** ▪ Female Associates are entitled to 8 weeks of Maternity Leave and an additional 8 weeks of Government-Paid Maternity Leave for her first and second child. **<u>Third and Subsequent Child</u>** ▪ 16 weeks of Government-Paid Maternity Leave in respect of her third and subsequent child. Any unconsumed maternity leave benefits at the end of your contract would lapse.

Female Associates whose children are non-Singapore Citizens:

Eligibility	Associates are covered under the Employment Act. ▪ You are legally married to the child's father. ▪ 90 days of continuous service with the Company, before the birth of your child. ▪ You have fewer than 2 living children of your own at the time of delivery. In the case of multiple births (e.g. twins, triplets, etc.) during the first pregnancy, it will be treated as single delivery and your employer is still required to pay 8 weeks of maternity leave for the current pregnancy. *If a female Associate subsequently registers the child as a Singapore Citizen within 12 months of the child's birth, she will be eligible for the remaining maternity leave from the date she meets all the criteria.
Entitlement	Female Associates are entitled to **12 weeks of maternity leave (8 weeks paid and the last 4 weeks unpaid)** Any unconsumed maternity leave benefits at the end of your contract would lapse.

- Associates are not entitled to paid medical leave should they fall sick during their maternity leave.
- The extended maternity leave shall lapse if not utilised. The leave also cannot be used to offset notice period, nor can it be encashed or carried forward for more than 12 months from the birth of the child.
- Associates should discuss with their Reporting Manager and come to an agreement on the arrangement that will best suit the needs of both parties before the Associate goes on maternity leave.
- Associates cannot resign from service while on maternity leave and use the maternity benefit period as notice of resignation.
- A copy of the birth certificate belonging to the Associate's child must be submitted to the Company for the leave to be valid.

PATERNITY LEAVE

- **From 1 January 2017**, eligible working fathers are entitled to 2 weeks of government-paid paternity leave (GPPL) funded by the Government.
- Male Associates must meet the following requirements to qualify for GPPL:
  - Your child is a Singapore Citizen
  - You are/were lawfully married to the child's mother at some point between conception and birth; and
  - You must have served the Company for at least 3 months before your child's birth
  - You are an adoptive father of a child who is a Singapore Citizen below 12 months of age

- This can be taken either in a continuous block of 2 weeks, or flexibly, within 12 months after the birth of the child subject to approval of Reporting Manager as well as Consultant and/or HR Shared Service Officer
- Associates are not allowed to use paternity leave to offset notice of resignation.
- A copy of the birth certificate belonging to the Associate's child must be submitted to the Company for the leave to be valid.

For eligible working fathers of children born **from 1 April 2025 and onwards**:

- Eligible fathers will be entitled to **mandatory 4 weeks of Government Paid Paternity Leave (GPPL)**.
- Male Associates must meet the following requirements to qualify for GPPL:
    - Your child is a Singapore Citizen
    - You are/were lawfully married to the child's mother at some point between conception and birth (whether or not such marriage remains subsisting at the time of your child's birth); and
    - You must have served the Company for at least 3 months before your child's birth
    - You are an adoptive father of a child who is a Singapore Citizen below 12 months of age
- This can be taken either in a continuous block of 2 weeks, or flexibly, within 12 months after the birth of the child subject to approval of Reporting Manager as well as Consultant and/or HR Shared Service Officer
- Associates are required to **provide at least 4 weeks' advance notice** or as much notice as possible before consuming the leave under any of the parental leave schemes.
- Associates are not allowed to use paternity leave to offset notice of resignation.
- A copy of the birth certificate belonging to the Associate's child must be submitted to the Company for the leave to be valid.

SHARED PARENTAL LEAVE

- Eligible parents will be entitled for 10 weeks of paid parental leave, shared between both parents. It will be implemented in two phases:
    - Effective 1 April 2025
        - Eligible working parents with Singapore Citizen children born on or adopted on or after 1 April 2025 will be eligible for **6 weeks*** of Shared Parental Leave.
    - Effective 1 April 2026
        - Shared Parental Leave will be increased to **10 weeks*** for eligible working parents with Singapore Citizen children born on or adopted on or after 1 April 2026.

*The new Shared Parental Leave will be equally allocated between parents (i.e. 3 weeks per parent from 1 April 2025 – 31 March 2026, 5 weeks per parent from 1 April 2026). Parents have the flexibility to discuss and reallocate their share of the leave to each other, based on the caregiving arrangement that is most suited for their families' needs. Parents who wish to change their leave sharing arrangement should do so within the first 4 weeks of their child's birth via LifeSG, after they have obtained their employers' agreement.

CHILDCARE LEAVE

- Associates who meet the following criteria are eligible for a total of 6 days of childcare leave per year:
    - The youngest child (including legally adopted children or stepchildren) is below 7 years of age
    - The child is a Singapore Citizen
    - Have worked in the Company for at least 3 continuous months

- Your childcare leave will be pro-rated based on the duration of your employment, subject to a minimum of 2 days.

- Associates whose child is not a Singapore Citizen (below 7 years of age) will be eligible for a total of 2 days of childcare leave per year after 3 continuous months of service.
- Childcare leave entitlement must be consumed by the end of the year; unconsumed childcare leave will be forfeited by the end of the year and cannot be carried forward to the following year.
- Associates shall be entitled to childcare leave for the relevant period based on the table below:

Completed months of service	Eligible days of childcare leave
0 month	Not eligible
1 month	Not eligible
2 months	Not eligible
3 months	2
4 months	2
5 months	3
6 months	3
7 months	4
8 months	4
9 months	5
10 months	5
11 months	6
12 months	6

EXTENDED CHILDCARE LEAVE

- Associates who meet the following criteria are eligible for 2 days of extended childcare leave:
  - The youngest child is between 7 to 12 years of age (inclusive)
  - The child is a Singapore Citizen
  - Have worked in the Company for at least 3 continuous months
- For those with Singapore citizen children in both age groups (below 7 years old and 7 to 12 years old), the total paid childcare leave for each parent is a maximum of 6 days per year.
- Unconsumed leave will be forfeited by the end of the year.
- The documents required for submission to apply for Childcare/Extended Childcare Leave are as follows:
  - Birth certificate of the youngest child
  - Singapore citizenship certificate (for a child who is not born as a Singapore Citizen)

RESERVIST LEAVE

- On receipt of the order to report for duty/ training or routine reporting, Associates must notify and submit the NS Call-Up Notification Letter and service remuneration form from the Commanding Officer (MINDEF) to their Reporting Manager as well as Consultant and/or HR Shared Services Officer in charge at least 4 weeks in advance for the Company to make the necessary claims from MINDEF.
- Associates called upon for National Service shall be entitled to make-up pay claims from MINDEF and contribution from the Company to their CPF accounts.
- Associates are not allowed to use National Service leave to offset notice of resignation.
- Reservist training is not considered part of notice period.

PART IV - DUTY OF CONFIDENTIALITY

- All trade secrets and proprietary information acquired in the course of one's work is to be treated as confidential.
- Confidential information includes without limitation:
  - (a) Technology know-how, processes, computer software and database technologies
  - (b) Technical information, plans and product specifications
  - (c) Associates' records
  - (d) Business plans and forecasts
  - (e) Financial records, reports, accounts and proposals
  - (f) Customer's intellectual property
  - (g) Quotations and tenders submitted or prepared for submission to clients and potential clients
  - (h) Trade secrets, proprietary information, customer lists, names of customer contacts and terms of trade with customers
  - (i) Information on customer suppliers, customer vendors or other customers which the Company would consider commercially valuable and/or secret
  - (j) Telephone lists, contact lists, policy documents, training documents, quality documents and any other internally used information regarding the operations of the Client
  - (k) Salary and salary details; and
  - (l) Any such other information concerning the Company or its affiliates, in printed, electronic or any other form.
- No information or copies of information are to be removed from the Client's premises except where the Clients have given express written consent.
- The obligation of confidentiality exists both during and after the contract has ceased.
- Any breach of confidentiality shall be regarded as serious misconduct and result in dismissal or termination without notice or payment in lieu of notice.
- Upon termination of the Employment Contract, all papers, records and documents in possession shall be returned to the Clients.

PART V – POLICIES

The following summary of policies are incorporated by reference into this Handbook:

(1) Code of Ethics
(2) Anti-Bribery and Anti-Corruption Policy
(3) Internal Personal Data Protection Guidelines
(4) Cyber and Information Security Policy
(5) Corporate Communications and Social Media Policy
(6) Anti-Harassment Policy
(7) Whistleblowing Policy

You shall comply with those Policy and Guidelines as through you are named as Employee in those Policy.

Please contact your Consultant and/or HR Shared Service Officer should you require further clarification about the above policies and guidelines. The policies are incorporated in this handbook for reference. However, the Privacy Policy is also available on https://www.persolsingapore.com/policies

PART VI – COMPLIANCES DO'S AND DON'TS

CODE OF ETHICS	
DO'S	**DON'TS**
• **Comply with all laws, rules and regulations**; Protect and safeguard **confidentiality of company information** from unauthorized use, disclosure or loss.	• Do not use company resources for personal gain, divert business opportunities, compete with the company directly or indirectly, or engage in unfair dealing practices. **Risky business activities** putting people or our integrity or financial well-being at risk will not be tolerated.
• When in doubt, report **dishonest or unethical behaviours** to your Reporting Managers and/or Consultant and/or HR Shared Service Officer.	• **Engaging in inappropriate behaviour** in the workplace will result in disciplinary action, up to and including termination.
• Perform duties with **skill, honesty, care, and diligence**, utilizing authority in a fair and equitable manner.	• **Do not neglect responsibilities, act dishonestly, or misuse authority** or participate in activities that may create conflicts of interest.
• Take all reasonable care to **secure your safety and health** while at work.	• **Do not disregard safety protocols or procedures that ensure the well-being of yourself and others in the workplace.**
• Treat all individuals encountered in the course of your employment with sensitivity and courtesy.	• **Do not discriminate on any unlawful grounds** when dealing with people in the course of your duties.
CONFLICT OF INTEREST AND RELATED PARTY TRANSACTIONS	
• Employees, Associates, Service Delivery Personnels must **promptly disclose and obtain approval Reporting Managers and/or Consultant** from for any actual, potential, or perceived Conflict of Interest, including Related Party Transactions. Failure to do so may result in disciplinary action, including termination if your failure to disclose causes loss or reputational damage to the Company.	
ANTI-BRIBERY AND ANTI-CORRUPTION POLICY	
TO THIRD PARTIES	**FROM THIRD PARTIES**
• Do **not give, promise, or offer anything** of value to any customer, government employee or other person for the purpose of improperly influencing a decision, securing an advantage, avoiding a disadvantage or obtaining or retaining business.	• **No payment or reward should be received or requested** in circumstances where it could be perceived as intended for the purposes of improperly influencing a decision, encouraging or influencing the performance of an illegal or improper act.
INTERNAL PERSONAL DATA PROTECTION GUIDELINES	
DO'S	**DON'TS**
Housekeep your emails and files regularly to review whether you need to continue retaining personal data in your care (printed and electronic form).	• **Do not leave** personal data lying around on your desk unattended. Always keep hard-copy personal data documents in **locked cabinets** when you leave your desk.
• **Shred or securely dispose** all unneeded personal data in your care; do not simply tear and throw into the dustbins.	• **Do not leave** unwanted personal data printouts at the printer; **Do not reuse** such printouts as rough paper.
• Apply **password protection** to computers, screensavers, and documents.	• **Do not disclose** any personal data or company's confidential (including giving references) to an individual without first checking that the individual consents to such disclosure.

• **Encrypt** the file and personal data when send to authorise individual. Be extremely careful about passing personal data to third parties.	• **Do not email** company's confidential data to your personal email; **Do not download or store** personal data on unauthorized devices, such as personal laptops or mobile devices.
DO NOT CALL POLICIES	
DO'S	**DON'TS**
• **Your role DOES NOT, AND MUST NOT involve making marketing calls, unless expressly authorized by your Reporting Manager.** If your role involves making marketing calls or sending of marketing messages, you must conduct a prior check with your Reporting Manager / Marketing head / Data Protection Officer to ensure that the recipient(s) has given **clear, unambiguous, and valid written consent** to receiving such marketing messages at his Singapore telephone number.	• **Do not attempt to send out** any form of marketing messages to any individuals without checking the validity of the given consent as well as against the DNC Registry, as such actions are a **breach** of the DNC regime and will constitute a **criminal offence** under the Personal Data Protection Act 2012. Such actions may be viewed by the Company as a breach of your employment contract and subject you to disciplinary proceedings and **possible termination** of your employment.
• Ensure that the Singapore telephone number has been checked against the **DNC Registry** within the prescribed period and that the marketing message contains clear and accurate information identifying the Company as well as how the recipient may contact the Company.	• **Do not ignore** any form of communication from any individuals seeking to **withdraw their consent** to receive marketing messages. Immediately notify your Reporting Manager / Marketing head / Data Protection Officer of such communication.
CYBER & INFORMATION SECURITY POLICY	
DO'S	**DON'TS**
• Be cautious of **online fraud or theft** carried out by compromising legitimate business e-mail accounts through requesting to conduct unauthorized transfers of funds.	• Do not open or click **suspicious links or file attachments** in emails or websites. Check with the sender directly to make sure it is legitimate.
• Contact your Reporting Manager / Marketing head immediately of any suspected online fraud or theft incidents. Any **observed or suspected security weaknesses** should be reported to your Reporting Manager / IT head.	• **Do not accept** unsolicited offers to remove viruses or install security patches or download "clean up" tools or similar utilities, or click on sites claiming security gaps or offers to speed up the performance of your computer.
• If you are working from home, **use a secure Wi-Fi** and send important, confidential, and sensitive Company information over Virtual Private Network (VPN).	• **Do not use non-company email accounts** for sending or receiving company information, including personal data. You must use official company business email accounts to send emails to recipients' company or business email addresses.
• Ensure that **confidential or internal information is protected** in accordance with the information classification guidelines.	• **Do not store** Company information on non-Company provisioned cloud storage or unencrypted removable media.
• **Password lock** your workstations and Company-issued mobile devices to prevent unauthorized access to information.	• Do not make any adjustments to the **security configuration** of the systems installed on your desktop or laptop computers.
• Company emails and messaging systems are intended to be for **business use**, therefore there will be no expectation of personal privacy.	• **Unauthorized use** of Company email or messaging systems to transmit classified information or storing offensive material is **strictly prohibited**.
CORPORATE COMMUNICATIONS & SOCIAL MEDIA POLICY	
DO'S	**DON'TS**
• **Direct all inquiries** from news media, the investment community or industry analysts to your Reporting	• **Do not disclose** proprietary Company information such as branding strategies, proposed initiatives and

Manager / Marketing head to ensure consistent disclosures of information to the public.	services, financial information, customer information, without permission.
• This includes opinions sought by student researchers (Competitors occasionally pose as students or researchers in an attempt to gather proprietary Company information. Please **direct such callers** to your Reporting Manager / Marketing head).	• **Do not discuss or disclose customer relationships**. Customer contracts generally prohibit discussion of customer relationships unless prior customer consent and corporate approval has been obtained.
• You are **personally responsible** for any comments about and on behalf of the Company you post on social media. Make it clear your comments are your own and not those of the Company.	• **Do not infringe** on the Company's logos, brand names, images, or trademarks, which includes, without limitation, setting up Company-branded pages or sites on social networks.
• **Be respectful**, stick to the facts and always credit sources with citations or links.	• **Do not use statements** meant to intentionally harm someone's reputation or post anything that may contribute to a hostile work environment.
• Contact your Reporting Manager / Marketing head if any **negative posts, discussions about trade secrets, violence or workplace harassment** are found online.	• **Do not request** or require anyone to provide any password or related account information to gain access to their social network profile.
ANTI-HARASSMENT POLICY	
ILLUSTRATION OF HARASSMENT	**REPORTING HARASSMENT**
• **Workplace harassment** can include unwanted physical contact, bullying, intimidation or offensive, suggestive, humiliating, demeaning or unwelcome jokes and may relate to a form of discrimination. Harassment conducts may occur through different modes of communications such as email, text messaging, social media or phone calls or face-to-face harassment or bullying.	• **When in doubt** about the best action in a particular situation, employees / associates / service delivery personnels should talk to their Reporting Managers or promptly report to the Consultant or HR Shared Service Officer.
• Any **hostile conduct** directed at an individual based on his or her race, age, religion, nationality, or disability is expressly prohibited under our Code of Ethics.	• Whilst the investigation is taking place, the complainant and witnesses should **avoid discussing the incident or complaint** with each other or with other employees unless necessary. Any employee / associate / service delivery personnel who is found guilty of harassment, shall be subject to **corrective or disciplinary action**, including termination of employment.
WHISTLEBLOWING POLICY	
POLICY COVERAGE	**REPORTING AND COMMUNICATION CHANNELS**
• Fraud or forgery, Dishonest acts, Bribes • Removal/inappropriate use of Company's assets and records, Violations of Company policies, material laws and regulations • Conduct that is an offence under any Commonwealth law that carries a penalty of twelve (12) months or more for imprisonment	• When in doubt about the best action in a particular situation, employees / associates / service delivery personnel should talk to their Reporting Managers, Consultant or HR Shared Service Officer. • Genuine concerns should be reported via Noggin  • The Whistleblowing Committee will ensure concerns are fairly and properly considered and not false or made in bad faith. • Any employee / associate / service delivery personnel who victimises or retaliates against the Whistleblower will be subjected to disciplinary action.

PART VII – GRIEVANCES

- A grievance is defined as an Associate's expressed feeling of dissatisfaction concerning conditions of employment or treatment by the Associate's Reporting Manager or colleague.
- The Associates concerned may channel the grievances to his/her respective Reporting Manager and/or Consultant in charge.
- If the grievance is against the Reporting Manager or next level manager, the Associate concerned can report the grievance directly to Consultant in charge. This may be brought to the Division Director's attention for involvement, if required.
- The Associates may raise a formal grievance including but not limited to the following through the Grievance Resolution Steps.
  - ✓ Harassment (include unwanted and unjustified verbal or physical advances)
  - ✓ Bullying (e.g. Physical, Verbal, Emotional Intimidation, Racist, Sexual, Cyber)
  - ✓ Unlawful Stalking
  - ✓ Threatening, abusive, or insulting language, comments or other non-verbal gestures
  - ✓ Discrimination on gender, ethnicity, disability or other unjustified grounds in the workplace
  - ✓ Offensive Jokes
  - ✓ Adverse changes in employment conditions and work
  - ✓ Conditions of work (related to safety and health conditions, discriminatory acts and unfair treatment)

ASSOCIATE'S GRIEVANCE RESOLUTION STEPS:

- **STEP 1. The Associates concerned to officially lodge grievance to his/her respective Reporting Manager and/or Consultant in charge via email or phone call.**
  - Respective Reporting Manager should escalate the grievance to Consultant in charge at first instance, vice versa
  - In making a report, the Associates should provide as much details as possible, such as names, dates, time of the incident(s) and supporting information or other evidence.

- **STEP 2. Investigation by respective Reporting Manager and/or Consultant in charge**
  - The Reporting Manager in the presence of the Consultant in charge and/or are responsible for handling all reported cases and ensuring that issues raised are properly resolved by the manager or such parties as appropriate. If the matter is substantiated, it will be referred to by the police or other law enforcement agencies where appropriate.
  - Consultant in charge to fill in "Incident Report" and "Incident Statement" for investigation/findings (including meeting with any witnesses) and proposed solution to grievance.
  - Discussions to be documented and confidentiality of information observed.

- **STEP 3. Respond to Associates concerned with update**
  - The Reporting Manager and Consultant in charge will respond on the update resolution action items and decision to the Associate concerned within 14 – 30 working days from the date of escalation (depending on the complexity of the grievance incident).

- **STEP 4. Resolved and closed for record & filing purpose**
  - If the Associates concerned do not feel that a reported incident has been addressed after the Associate's Grievance Resolution procedures, he or she should escalate the grievance incident to the Division Director for a final resolution through Consultant in charge within 3 working days.
  - The final decision will be made at this level within 14 working days from the date of escalation.
  - All reports will be treated with strict confidentiality.

GRIEVANCE HANDLING ADVICE – WHAT AFFECTED ASSOCIATES CAN DO WHEN FACING A HARASSMENT:

Taking Charge of Yourself

- The Associates are reminded to take charge of your personal safety, health and wellbeing at the workplace. Associates should take all reasonable steps to protect yourself and keep away from potential harassment situations. Here are some tips for Associates to protect themselves from harassment:
  - ✓ Keep a distance from people who exhibit unacceptable social behavior, where reasonably possible.
  - ✓ Be familiar with workplace harassment-related procedures in the organization.
  - ✓ Adopt a buddy system in situations where personal safety may be compromised
  - ✓ Summon helps using pre-arranged distress signal or other appropriate means such as the personal duress system, in situations where personal safety may be compromised
  - ✓ Escalate or report potential cases to the appropriate parties promptly.
  - ✓ Responding to Harassment

There are different ways to deal with harassment. Depending on the situation, the Associates can consider pursuing one or more of the following options in no particular order.

1. Dealing with harassment yourself
   Affected Associates upon recognizing that they are caught in harassment situations, can consider defusing the situation or resolving it on their own, only when it is considered safe and reasonable to do so. If the affected Associate is unable to deal with the harassment alone, you are strongly advised to seek formal and/or informal help immediately.
   Some suggested measures include:
   - ✓ Adopting effective body language (e.g. stand firm on the ground), staying alert and looking for escape routes.
   - ✓ Telling the harasser assertively to stop his/her unreasonable behavior.
   - ✓ Warning the harasser that stern action will be taken if harassment persists e.g. report to manager or HR
   - ✓ Documenting and keeping a record of evidence e.g. photographs, screenshots, messages, audio recordings.

2. Getting informal help
   The affected Associates can:
   - ✓ Approach the harasser with a trusted person e.g. colleague or friend, you are uncomfortable to confront the harasser personally.
   - ✓ Seeking guidance from someone who is trained or knowledgeable in defusing difficult situations (e.g. manager).

3. Getting formal help
   The affected Associates is advised to raise a Grievance Report on the harassment encounter to your manager or the Consultant in-charge when organizational intervention is required. The company will intervene promptly upon receipt of such reports and take all appropriate action necessary.

PART VIII – QUALITY AND ENVIRONMENTAL

As a valued Associate, you play an important role in upholding the quality and environmental standards that define our service excellence and commitment to sustainability. The following outlines our expectations for your conduct and responsibilities in these areas.

COMMITMENT TO QUALITY

We are committed to delivering services that meet or exceed our clients' expectations, and this commitment extends to all Associates. As such, you are expected to uphold high standards of quality in your day-to-day work such as but not limited to the following areas:

- Adhere to the PERSOL and client's quality policies, guidelines, and operational standards.
- Perform your duties diligently, professionally, and in accordance with the client's procedures and performance expectations.
- Contribute to a culture of continuous improvement by supporting efforts to enhance productivity and operational efficiency.
- Respect and protect PERSOL and client confidentiality, as well as ensure the integrity of all data handled.
- Promptly report any non-conformities, incidents, or process deviations to your Reporting Manager, PERSOL Consultant, and/or HR Shared Services Officer.

By maintaining these standards, you help foster a positive, reliable, and accountable work environment that reflects our shared commitment to service excellence.

ENVIRONMENTAL CONTROL MEASURES

PERSOL supports environmental protection initiatives and is committed to promoting sustainable practices across all operations. As part of this commitment, all Associates are expected to contribute to the conservation of resources both within our organization and while working at client sites.

You are encouraged to comply with the following environmental control practices and adhere to client's environmental policies, guidelines, and operational requirements.

- **Energy Conservation:** Reducing electricity consumption by turning off lights and equipment (e.g., computers, monitors, printers) at the end of each workday and when not in use.
- **Water Conservation:** Adopt water-saving habits such as turning off faucets while lathering hands and reporting any leaks or malfunctioning fixtures immediately to prevent water wastage.
- **Paper Conservation:** Reduce paper usage by printing double-sided where necessary, shifting to digital communication tools (e.g., corporate email) instead of printed memos, and using collaborative platforms (e.g., Microsoft SharePoint) for document sharing. Utilize cloud storage to minimize reliance on physical file storage.
- **Optimization of Other Resources:** Optimizing the use of office supplies and equipment and reducing resource wastage. Reuse items like binders, folders, and pens where possible to reduce waste.
- **Management of Waste:** Dispose of waste properly and in accordance with site-specific recycling and waste management procedures.
- **Prevention of Environmental Harm**: Avoid any actions that may directly or indirectly cause environmental damage.
- **Incident Reporting**: Promptly report any environmental incidents or hazards (e.g., spills, leaks, emissions) to the designated site representative.

PART IX – HEALTH AND SAFETY AT WORK

The Company is committed to provide and maintain safe and healthy working conditions for all our Associates. It is our intention that its work will be carried out in accordance with the relevant statutory provisions and all reasonable, practicable measures will be taken to avoid risk to its staff and others whilst visiting the Client's premise.

Associates also have the responsibility in contributing, maintaining and ensuring the health and safety of the workplace/client's premises. To provide and ensure a safe working environment, all Associates have the following responsibilities:

- Follow the workplace safety and health system, safe work procedures or safety rules implemented at the workplace.
- Not engaging in any unsafe or negligent acts that may endanger yourself or others working around you.
- Use personal protective equipment provided to you to ensure your safety while working. You must not tamper with or misuse the equipment.
- Ensure that you understand and carry out all emergency procedures, fire precautions and evacuation procedures.
- Fully adhere to the Client's Business Continuity Plans at all times when carrying out your duties in the premise of the Client or assigned workplace.
- Report immediately to your Reporting Manager and Consultant and/or HR Shared Service Officer any potential hazard to any staff or the general public.
- In the event of an infectious disease outbreak such as a pandemic (e.g. SARS, COVID-19, H1N1), you must comply and strictly adhere to the measures, protocols and rules that are set by the government, including additional measures put in place by PERSOL or clients at the workplace. For information and updates, you may visit the following websites:
  - https://www.gov.sg/
  - https://www.moh.gov.sg/
  - https://www.mom.gov.sg/

WORKPLACE HEALTH & SAFETY ON-SITE HANDBOOK

(ON-SITE ASSIGNMENT AT CLIENT LOCATIONS)

1. INTRODUCTION

PERSOL Singapore Pte Ltd and its group of companies are committed to ensuring a safe and healthy workplace environment exist for you when you work on-site at our client locations. This Workplace Health & Safety Handbook ("Handbook") is designed to help you understand your responsibilities as an Associate or Contractor to ensure protection of your own workplace health and safety at work.

Terms used in this Handbook have the following meanings:

"**On-Site Reporting Manager**" means the client's employee appointed to manage associates and contractors working on-site.
"**PERSOL Representative**" means the appointed representative (such as HR Shared Service Officer) of PERSOL entity who is managing the client's account where you work on-site.

The joint efforts of PERSOL and our clients cannot completely protect you from injury on the job. We need your cooperation. This Handbook is designed for you to learn about your responsibilities on workplace health and safety. You should:

- Know the safe work practices for your work area and your job
- Comply with PERSOL and customer safety policies, including personal protective equipment requirements
- Report unsafe work conditions or practices to both your On-Site Reporting Manager and your PERSOL Representative immediately
- Notify your PERSOL Representative of any customer-requested changes in your job duties
- Participate in periodic safety meetings and/or safety training programs, as required

2. OUR COMMITMENT TO SAFETY

We promote workplace health and safety. Our goal is zero harm, achieved by preventing workplace injuries and illnesses. Each of us must take personal responsibility for our own safety and the safety of our co-workers and those for whom we are responsible.

3. YOU AND YOUR SAFETY

As an Associate or Contractor of PERSOL, you are expected to:

- Accept responsibility for your own behavior and actions.
- Know and comply with all safety policies, standards and procedures that apply to your job.
- Actively participate in all required training.
- Actively participate in safety meetings.
- Know and manage your own personal limitations.
- Assess the hazards of the job area before starting any assignment and plan the job so that the work can be done safely.
- Manage any situations that affect your ability to do the job safely.
- Continuously evaluate conditions that affect your ability to do the job safely.

- Use the correct tools and use them safely.
- Maintain good housekeeping in your work area.
- Not letting job pressures affect your ability to safely perform your job.
- Work with your PERSOL Representative to identify additional training needs.

Additionally, to help ensure your safety and the safety of those around you, you are expected to:

- Immediately report all incidents, near misses and unsafe conditions to your On-Site Reporting Manager and PERSOL Representative.
- Intervene to address unsafe conditions or behaviors.
- Immediately report to your On-Site Reporting Manager and PERSOL Representative upon becoming aware of an injury or illness that may be work-related.

4. GENERAL STANDARDS OF CONDUCT

We expect you to be professional, conscientious, and courteous to our customers, your co-workers and your supervisor.

Please refer to the Compliance Manual for basic principles on behaviors in the workplace, compliance with laws, confidentiality, anti-bribery and anti-harassment.

5. PARTICIPATION IN CLIENT SAFETY ACTIVITIES

All Associates and Contractors are required to participate in recurring safety activities while on assignment at Client locations. The purpose is to raise awareness of risks and to provide a safe working environment for everyone.

6. SAFETY AWARENESS

There are two types of general hazards to the job: unsafe acts and unsafe conditions.

UNSAFE ACTS: behaviors people carry out that disregard safety procedures

UNSAFE CONDITIONS: machines, tools, protective equipment or work areas that do not comply with safety guidelines and require mitigation or control changes in order to protect the people who work in your workplace.

A key part of your safety responsibility is to know what a safety hazard is, be on the lookout for safety hazards and correct or report them immediately. Listed below is a Do's and Don'ts Checklist.

DO'S:

- Treat safety as a core job responsibility
- Plan each job before you start
- Think about what could go wrong and how you will prevent problems and accidents
- Keep work areas clear of potential fire, spill or tripping and falling hazards
- Check for proper ventilation
- Pay attention to what you are doing

- Know what to do in an emergency
- Ask questions when you are unsure of what to do or how to do it
- Use labels, protective equipment where applicable
- Wash thoroughly before eating, drinking or smoking

DON'TS:

- Eat, drink or use tobacco in the work area, unless otherwise designated.
- Use any malfunctioning tool or machine.
- Ignore a safety hazard.
- Ignore other workers' unsafe practices.
- Let others talk you into bypassing safety procedures.
- Take shortcuts.

Remember a safe workplace is what everyone wants. Combination of training and experience makes it relatively easy to identify on-the-job hazards and protect us from dangers.

OFFICE SAFETY RULES

Safety in office environments is often taken for granted. In fact, an accident in the office can be serious and costly.

HOUSEKEEPING

- Keep your work area clean and orderly. Good housekeeping can eliminate many offices hazards
- Do not put desk materials and equipment near the edge of the desk, where they can be bumped or jarred off.
- Keep sharp objects such as staples, tacks and scissors in a closed container.
- Do not leave desk and cabinet doors and drawers open.
- Store materials inside cabinets and files, from the bottom up.
- Keep aisles, doorways and/or stairways clear of unnecessary materials.
- Report spills or broken objects to your On-Site Reporting Manager if you cannot efficiently and safely clean them up yourself.

OFFICE MACHINERY

- Exercise care and follow directions when using office machinery.
- Be alerted to frayed electrical cords and overloaded electrical outlets.
- If you notice a machine sparking or smoking, do not use it. Report it to your On-Site Reporting Manager and put a sign on the machine to indicate to others that it is out of order and dangerous.
- Even if a machine is in good working order, turn it off before making any adjustments or adding flammable solutions.

LIFTING AND CARRYING

- Use proper lifting techniques: bend your knees and, keeping your back as straight as possible, use leg muscles to lift the load.
- Do not stand on tables, desks or chairs to reach materials.

- Do not try to move office furniture or equipment. Your On-Site Reporting Manager should arrange to have this work done.
- When carrying bulky loads, maintain a clear visual path.
- If you must use a stairway when carrying materials, keep one hand free to use the handrail. If necessary, get help or use an appropriate cart or dolly.

REPETITIVE MOTION DISORDERS

Description/Summary:
This category of injury generally involves damage or irritation of soft tissues, tendons, muscles, joints, and nervous system. Cumulative trauma disorders, repetitive motion disorders, upper extremity disorders, and carpal tunnel syndrome all have associated risk factors that may relate to the following list items:

- High levels of repetitive movements
- High amount of hand force (greater than seven pounds of hand force)
- Working in awkward postures (raised elbows and arms, bent wrists, poor standing posture, leaning over, etc.)
- Mechanical stress (hands, arms, thighs rest on sharp surfaces or surfaces that inhibit blood flow or tendon flexion)
- High degrees of vibration (from power tools, machinery)
- Exposures to hot or cold temperatures
- Usage of personal protective equipment which inhibits normal movements and requires the application of additional hand strength (gloves), bulky smocks that require the elbows to be away from the body, etc.
- Use of hand tools (may produce repeated awkward application of force)
- Manipulation of small objects which require extremely high levels of hand dexterity
- Extensive utilization of muscle groups previously not normally used

Symptoms:

- Tightness, discomfort, stiffness, soreness or burning in the hands, wrists, fingers, forearms, or elbows
- Tingling, coldness, or numbness in the hands
- Clumsiness or loss of strength and coordination in the hands
- Pain that wakes you up at night
- Feeling a need to massage your hands, wrists, and arms

Procedures for reporting any of the above early symptoms:

- If you are experiencing any of the above-mentioned symptoms, **contact your On-Site Reporting Manager and PERSOL Representative immediately.** We care about the environment you work in.

Prevention:
Correct typing technique and posture, the right equipment setup, and good work habits are important in the prevention of Repetitive Motion Disorders. Simple ergonomic guidelines:

- Wrists should be straight and level, not bent down, back, or to either side
- Fingers should be in a straight line with your forearm
- Wrists should not rest on anything while typing
- Use a light touch on the keyboard
- Take breaks to stretch and relax
- Hold the mouse lightly

- Eliminate unnecessary computer usage
- Don't tuck the telephone between your shoulder and ear
- Pay attention to your body - if it hurts, stop doing it!
- Evaluate other activities – sports, carrying children, hobbies, they may have an enormous impact, too

Exercise can also help prevent injury. Try these simple exercises before work and during a mid-day break:

- Extend and stretch both wrists and fingers acutely as if they are in a handstand position. Hold for a count of 5.
- Straighten both wrists and relax fingers.
- Make a tight fist with both hands.
- Bend both wrists down while keeping the fist. Hold for a count of 5.
- Straighten both wrists and relax fingers for a count of 5.
- Make a fist and rotate your entire hand (from the wrist) in one direction. Repeat 15 times. Switch directions and repeat 15 times.
- Release your hands, and with your fingers extended, do the same rotations.
- Make a fist and then extend your fingers as far apart as possible. Hold for a count of 10. Relax.
- Repeat the entire sequence 5-10 times until hands and fingers feel relaxed.

PERSONAL PROTECTIVE CLOTHING AND EQUIPMENT

Assignment of personal protective clothing and equipment will be determined based on the job.

PERSONAL CLOTHING

Where protective work clothes are not required, each Associate and Contractor is expected to wear personal clothing that is safe and proper for the job.

JEWELLERY

Individuals, other than those working in an office environment, shall not wear any type of jewellery that is exposed or hangs loosely away from the body such as long necklaces, earrings other than stud earrings, loose fitting bracelets or watches.

PROTECTING IDENTIFICATION CARDS

Your identification card is your key to accessing Client Location. In addition, it contains a wealth of personal information about you. As a result, your card should be protected at all times.

The card should be visibly displayed on your person, or, if for safety reasons, it cannot be displayed, at least in your possession at all times while at Client Location. In this way, you are identified as "authorized" to be in the plant. More importantly, "unauthorized" persons are more easily identified.

Identification cards should not be left unprotected.

7. EMERGENCY EVACUATION PROCESS

Where our Client has emergency evacuation processes, Associates and Contractors should be familiar with such processes for your own safety. If you have any additional questions regarding the emergency evacuation process, please contact your On-Site Reporting Manager and PERSOL Representative.

8. SAFETY VIOLATION PROCEDURES

Violations will be reviewed on a case-by-case basis. Disciplinary action up to and including termination will be based on the severity and cognizant reasoning of the violation. The following procedures apply to any Associate or Contractor cited for a Safety Violation at Client Location.

First Violation:

- Associate or Contractor receives verbal and/or written reprimand describing the violation with a copy placed in his/her personnel file for a minimum period of three months. Verbal reprimands are documented via PERSOL's Candidate database (ATS). PERSOL management counsels the Associate or Contractor and documented corrective actions are completed by the Associate or Contractor to prevent repeat of violation.

Second Violation:

- Associate or Contractor receives a written reprimand describing violation and disciplinary action with copy placed in his/her personnel file for a minimum period of six months.
- Documented corrective actions are completed by Associates or Contractor to prevent repeated violation.

Third Violation:

- PERSOL is subject to termination of employment with PERSOL depending on severity of violation and as deemed appropriate by PERSOL management.

9. WORKPLACE VIOLENCE

Acts or threats of violence including intimidation, harassment, and/or coercion, which involve or affect the Associate or Contractors, or which occur on Client Location, will not be tolerated.

Specific examples of conduct that may be considered threats or acts of violence include, but are not limited to, the following:

- Hitting or shoving an individual.
- Threating harm to an individual or their family, friends, associates, or property.
- The intentional destruction or threat of destruction of Company property.
- Harassing or threatening phone calls.
- Harassing surveillance or stalking.
- The suggestion or insinuation that violence is appropriate.
- Unauthorized possession or inappropriate use of firearms or weapons.

Every Associate or Contractor and every person working on-site at client's property is required to report incidents of threats or acts of violence of which he/she is aware. The report should be made to both the On-Site Reporting Manager and PERSOL Representative. Nothing in this policy alters any other reporting obligations required under any applicable laws.

If you have any questions or concerns, contact your PERSOL Representative. If you are issued an AIA Medical card or other medical insurance cards, and in case medical treatment is required during business hours, please check the information provided on your cards.

10. INCIDENT INVESTIGATIONS

You should report incidents that result or could result in injury at work to your both your On-Site Reporting Manager and PERSOL Representative to enable them to conduct an incident investigation.

An incident investigation is designed to identify the root cause of the incident and prevent future occurrences. Reporting is the most important part of the process. We NEED your support to report to help prevent you or other people from sustaining a similar incident.

(a) TIMELINES

- An incident must be reported immediately.
- The timeliness of reporting is crucial to the Associate's/Contractor's welfare and to meet the deadlines in the rest of the incident investigation process.

(b) YOUR RESPONSIBILITIES

- Report incidents, no matter the severity, immediately.
- Attend all meetings, as requested, related to the incident.
- If you are required to take part in preventative measures act promptly.
- Keep in touch with your On-Site Reporting Manager and PERSOL Representative when new information arises about the incident to ensure consistent information is communicated.
- Educate other Associates and Contractors of the outcome and preventative measures to make your work environment and other's safety.

---------- END OF WORKPLACE HEALTH & SAFETY ON-SITE HANDBOOK ----------

Thank You

Prepared by:
Business Operations Excellence

PERSOL

1. Introduction

1.1 PERSOL Singapore Pte Ltd (the "**Company**", "**We**". "Us**",** "**Our**") respects your privacy and we acknowledge that you have certain rights related to any personal data we collect from you and we have certain obligations in respect of the same. The Company is compliant with certain local privacy laws, including the Singapore Personal Data Protection Act 2012 ("**PDPA**") and its regulations, and has procedures in place to meet the requirements of those laws.

1.2 This privacy policy ("**Privacy Policy**") describes our privacy principles and/or our practices for gathering, collecting, storing, using and/or disclosing your personal data. We encourage you to review this Privacy Policy so that you may understand how we may collect, use, disclose, process and share your personal data.

1.3 For the avoidance of doubt, "**personal data**" means data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access.

2. Information We Collect, Use or Disclose

2.1 In order for us to provide our services and for the operation of our business, provide services of recruiting and placing individuals for potential work assignments (and related services) with our customers and/or directly at the Company, act as employer or hirer of record for individuals employed or engaged by the Company, or provide human resources related services to our customers, we must collect certain personal data from and about individuals who are candidates, employees, contractors, and former employees. In the event we are unable to collect the required personal data from such individuals, we may not be able to proceed with the abovementioned services, including providing potential job placements, for such individuals.

2.2 The types of personal data collected, used, processed, disclosed and stored by us depends on the circumstances and/or the purposes for which we may need to process your personal data. Hence, subject to the aforesaid, such personal data may include:

- Name
- Contact information (address, phone number, e-mail address);
- Employee identification number;
- Date of birth;
- Contents of any other identification provided to the Company for application or employment purposes;
- Education and employment history;
- Work-related skills and experience;
- Professional credentials or licenses;
- Membership in professional organisations;
- Any other information contained on an individual's Curriculum Vitae (CV);
- Citizenship and work authorisation status;
- Disability and health-related information;
- Next-of-kin or emergency contact information;

- Information from and related to publicly published profiles you've created on job-related
- social media platforms and job boards (such as LinkedIn, Monster, or Indeed);
- Information provided by references;
- Information regarding your career interests, preferences, and qualifications; and
- Any information that you provide to us through various channels (including but not limited to any AI chatbot feature) on a voluntary basis.

2.3 In addition, under certain circumstances and consistent with prevailing laws, we may request types of personal data that are viewed by some countries as "**sensitive**":

- National identification, tax identification, passport number or social security number(s);
- Financial or bank account information;
- Results of drug, criminal, and/or background screenings;
- Benefits selections, potentially including health insurance and retirement planning information;
- Biometric data;
- Information contained within your personnel file with the Company, such as performance reviews, disciplinary action, and other payroll related information; and
- Health information, including that related to a work-related claim (e.g. workers' compensation claim).

2.4 In some jurisdictions, in order to comply with statutes, rules, and regulations pertaining to equal employment opportunities or to assist the Company or its related corporations in compiling data for its equal opportunities' practices and reporting, we may also ask you to provide gender, race/ethnicity or disability information. The provision of this type of information will be voluntary, unless it is required by law, and failure to provide this information will not hinder your employment or project opportunities.

2.5 Your interactions with our websites and mobile applications may also result in the collection, processing, and storage of the following types of information from you:

- Geolocation data, and
- Other information you may provide to us, such as through surveys, interactions with our social media, or other mediums used to contact the Company.

2.6 Some of our websites require you to provide your personal data, such as when you create a profile and log-in credentials. Instead of having to type in your personal data, some of these functionalities may allow you to use third-party authentication tools such as Facebook, Twitter, and Google to populate certain fields. By authenticating through one of the social media options, you allow us to receive your personal data and other information that is accessible through these tools. This information may be incorporated into your profile. For any such tool you choose to use, we encourage you to also review the tool provider's privacy policy and any terms and conditions.

2.7 We may use your personal data to permit you to participate in live social media feeds. If you choose to participate, your public username may be displayed on the sites along with your post, including, but not limited to, any comments, images, and videos that you may have posted.

2.8 We may provide you with access to third-party functionality that allows you to post content to your social media account(s). Any information that you provide to your social media account(s) through use of such third-party functionality is governed by the applicable third party's privacy policy, and not by this Privacy Policy. For the avoidance of doubt, we are not responsible for any personal data that you provide to such third party.

2.9 In today's data economy, businesses are leveraging on innovative technologies such as artificial intelligence and machine learning technology, which process data including personal data, for one or more of the purposes set out at paragraph 3 below. We are no different from such businesses as the use of such innovative technologies has become a necessary part of business operations.

3. The purposes for Which We Collect, Use or Disclose Your Personal Data

3.1 We will/may collect, use, disclose and/or process your personal data for one or more of the following purposes:

(a) administering, processing and/or dealing with any transactions between you and the Company and/or any of its related corporations including but not limited to any application by you for employment or work with the Company;

(b) recruiting, assessing and/or matching you with/for potential positions or assignments with third party organisations (or our customers), and/or dealing with matters related thereto such as offering you a placement of work or job with such third-party organisations (or our customers) or referring you for employment to a third-party organisation (or our customer);

(c) administering, managing and/or dealing with the provision of work or job placement services to you. This includes us sharing your personal data with our customers or third-party organisations, for your potential placement or employment opportunities with those customers/third party organisations who are seeking employees or workers, or to the organisation to which you have been assigned to work;

(d) carrying out your instructions or responding to any enquiry given by (or purported to be given by) you or on your behalf;

(e) administering, facilitating, processing and/or dealing in any matters relating to your use of any of the Company's or its related corporations' websites, any functionalities on the websites or any transactions or activities carried out by you on or through any of the Company's or its related corporations' websites, such as but not limited to live social media feeds;

(f) monitoring, processing and/or tracking your use of any of the Company's or its related corporations' websites in order to provide you with a seamless experience, facilitating or administering your use of any of the Company's or its related corporations' websites, and/or to assist us in improving your experience in using any of the Company's or its related corporations' websites;

(g) contacting you or communicating with you via phone/voice call, text message and/or fax message, email and/or postal mail for the purposes of administering your use of any of the Company's or its related corporations' website or any transactions you have with us, or for the provision of our services to you. You acknowledge and agree that such communication by us could be by way of the mailing of correspondence, documents or notices to you, which could involve disclosure of certain personal data about you to bring about delivery of the same as well as on the external cover of envelopes/mail packages;

(h) carrying out due diligence or other screening activities (including background checks) in accordance with legal or regulatory obligations applicable to us (whether from Singapore or any other country), the requirements or guidelines of governmental authorities which we determine are applicable to us (whether from Singapore or any other country), and/or our risk management procedures that may be required by law (whether from Singapore or any other country) or that may have been put in place by us;

(i) to prevent or investigate any fraud, unlawful activity or omission or misconduct, whether or not there is any suspicion of the aforementioned; dealing with conflict of interests; or dealing with and/or investigating complaints;

(j) managing, internal operations including conducting data analytics for the purpose of system and process improvements and enhancements to human resources processes;

(k) complying with or as required by any applicable law, governmental or regulatory requirements of any jurisdiction applicable to us or our related corporations, including meeting the requirements to make disclosure under the requirements of any law binding on us or our related corporations, and/or for the purposes of any guidelines issued by regulatory or other authorities (whether from Singapore or any other country), with which we or our related corporations are expected to comply;

(l) complying with or as required by any request or direction of any governmental authority (whether Singapore or non-Singapore) which we are expected to comply with; or responding to requests for information from public agencies, ministries, statutory boards or other similar authorities. For the avoidance of doubt, this means that we may/will disclose your personal data to the aforementioned parties upon their request or direction;

(m) storing, hosting, backing up (whether for disaster recovery or otherwise) of your personal data, whether within or outside Singapore;

(n) facilitating, dealing with and/or administering external audit(s) or internal audit(s) of the business of the Company and/or its related corporations;

(o) for marketing, if you have separately indicated that you consent to such purpose. If so, we may/will send you by email, postal mail or other modes of communication marketing and promotional information and materials relating to products and/or services (including products and/or services of third party organisations whom the Company may collaborate or tie up with) that the Company or its related corporations may be selling, marketing or promoting, whether such products or services exist now or are created in the future. In the case of the sending of marketing and promotional information and materials to you by voice call and instant messaging applications like SMS/MMS, WhatsApp or Telegram to your Singapore telephone number, we will not do so unless we have complied with the requirements of the PDPA in relation to use of the latter modes of communication to send you such marketing information or materials or where you have expressly consented to such mode of communication;

(p) dealing with and/or facilitating a business asset transaction or a potential business asset transaction, where such transaction involves the Company as a participant, and there may be other third-party organisations who are participants in such transaction. The term "**business asset transaction**" means the purchase, sale, lease, merger or amalgamation or any other acquisition, disposal or financing of an organisation or a portion of an organisation or of any of the business or assets of an organisation;

(q) developing, testing and/or implementing artificial intelligence and machine learning technologies (collectively "**AI**") to facilitate, enhance and/or improve our business operations including but not limited to automate and enhance our recruitment processes (such as screening resumes, conducting initial assessments of candidates, identifying skills gaps, and improving matching between candidates and job opportunities);

(r) processing your personal data through automated systems and/or AI to analyse and assess your experience, qualifications, and suitability for employment opportunities with us or our customers;

(s) using AI to transform and analyse your personal data and/or recruitment data into insights to identify patterns and trends that improve hiring efficiency, candidate experience, and placement outcomes;

(t) using AI to conduct analysis of job market trends and patterns to provide more accurate job recommendations, career advice, and skills development guidance;

(u) storing and processing your personal data through cloud-based platforms and services which incorporate artificial intelligence features and tools for the provision of our services to you; and

(v) using AI for one or more of the purposes set out in this paragraph 3.1;

(the purpose set out above shall be collectively referred to as "**Purposes**").

3.2 The Company may/will need to disclose your personal data to third parties, whether located within or outside Singapore, for one or more of the above Purposes, as such third parties, would be processing your personal data for one or more of the above Purposes. In this regard, you hereby acknowledge, agree and consent that we may/are permitted to disclose your personal data to such third parties (whether located within or outside Singapore) for one or more of the above Purposes and for the said third parties to subsequently collect, use, disclose and/or process your personal data for one or more of the above Purposes. Without limiting the generality of the foregoing or of the immediately preceding paragraph setting out the Purposes, such third parties include:

(a) our associated or affiliated organisations or related corporations;

(b) any of our agents, contractors or third-party service providers that process or will be processing your personal data on our behalf including but not limited to those which provide administrative or other services to us such as mailing houses, telecommunication companies, information technology companies, data centres, cloud service providers, artificial intelligence and machine learning technology providers, algorithm developers, and data analytics service providers;

(c) our customers or third-party organisations, who may be your potential employers or hirers or organisations which engage you for your services; and

(d) third parties to whom disclosure by the Company is for one or more of the Purposes and such third parties would in turn be collecting and processing your personal data for one or more of the Purposes.

3.3 Your consent pursuant to this Privacy Policy is additional to and does not supersede any other consents that you had provided to the Company with regard to processing of your personal data. We may collect, disclose or use your personal data pursuant to an exception under the PDPA or other written law such as during the following situations:

- To respond to an emergency that threatens your life, health and safety or of another individual; and
- Necessary in the national interest, for any investigation or proceedings.

3.4 Data that has been anonymised does not personally identify you and is not covered by this Privacy Policy.

3.5 We hold our employees, agents, and suppliers accountable for maintaining the trust that you place in us with your personal data. Your personal data will not be used or shared except as in accordance with applicable law relating to personal data.

3.6 Your personal data may be shared with third party service providers as set out at paragraph 3.2 above.

3.7 Consistent with paragraph 3.2 above, as a result of the scope of the Company's operations, the sharing of your personal data with our other group entities, service providers, and customers may result in your personal data being sent to countries outside of your country of residence, which may have data protection laws that differ from those in your country of residence. Regardless of the source or destination location of your information, we will at all times protect your personal data as described in this Privacy Policy, and in accordance with applicable data protection laws when transferring your personal data.

4. Cookies and Web Beacons

4.1 The Company's websites use "**cookies**" to help personalise the online experience. A cookie is a piece of data stored on the user's computer or mobile device tied to information about that user. They also allow us to identify those devices when they return to a website. You can set your browser to notify you before you receive

a cookie, giving you the option of whether to accept it. You can also set your browser to turn off cookies. If you do so, some areas of our websites may not function properly. We use both session ID and persistent cookies. A session ID cookie simply expires once the user closes the browser. A persistent cookie is a small text file stored on the user's hard drive for an extended period of time. These can be removed by following the instructions in your Internet browser's help file.

4.2 To help us provide better service, we sometimes collect anonymous information from visits to our websites through the use of "**web beacons**." These do not access your personal data, but rather allow us to log users who have visited our websites. This anonymous information is sometimes known as "**clickstream data**." We or our vendors may use this data to analyse trends and statistics to help us provide better customer service. If you do not want your transaction details used in this manner, see the paragraph above on cookies.

4.3 We allow third-party companies to collect certain anonymous information when you visit our websites. These companies may use non-personally identifiable information during your visits to our websites in order to provide advertisements about goods and services likely to be of greater interest to you. These companies typically use a cookie or a third-party web beacon to collect this information.

4.4 Links: For links to organisations not affiliated to us, we are not responsible for the privacy practices or the content of such websites. We recommend you review the terms and conditions of use and privacy policies in place on such websites.

5. Your Rights and Choices

5.1 The amount of personal data you are required to supply when requesting our services will be limited to that which is relevant to and reasonable for the supply of such services or for the Purposes for which such personal data is being collected.

5.2 Where you have asked us to do the following, or have otherwise given us your consent to do the following, we may periodically use your contact information to send you updates via e-mail in order to alert you to our marketing and promotional materials or services relevant to your interactions with us, such as jobs in our database that match your selected criteria. This may include job recommendations generated or enhanced by our AI systems based on your profile and preferences. Each notification will provide instructions on how to opt out of receiving similar e-mails from the registered service or resource. At the point where we request personal data about you, our site also gives you the opportunity to decide which communications you wish to receive. The database is automatically updated with your preferences when you opt out. When your interactions with the Company have resulted in your registration for multiple services or resources it may be necessary to opt out from each service separately.

5.3 Additionally, you have the right to request access to, to withdraw your consent to the use and processing of, and request the correction of inaccuracies of, personal data that the Company maintains about you, or that is in the Company's possession or under its control. We may limit or deny requests for access or charge reasonable fees for access, in accordance with applicable law data protection law.

5.4 Where you seek access to and/or seek to correct the personal data currently in our possession or control, we will need enough information from you in order to ascertain your identity as well as the nature of your request, so as to be able to deal with your request.

5.5 For a request to access personal data, once we have sufficient information from you to deal with the request, we will seek to provide you with the relevant personal data within 30 days. Where we are unable to respond to you within the said 30 days, we will notify you of the soonest possible time within which we can provide you with the information requested. Note that the PDPA exempts certain types of personal data from being subject to an access request.

5.6 For a request to correct personal data, once we have sufficient information from you to deal with the request, we will correct your personal data within 30 days. Where we are unable to do so within the said 30 days, we will notify you of the soonest practicable time within which we can make the correction. Note that the PDPA exempts certain types of personal data from being subject to your correction request as well as provides for situation(s) when correction need not be made by us despite your request.

5.7 We will process your request to withdraw your consent within a reasonable time from such a request being made, and will thereafter not collect, use and/or disclose your personal data in the manner stated in your request. However, your withdrawal of consent could result in certain legal consequences arising from such withdrawal. In this regard, depending on the extent of your withdrawal of consent for us to process your personal data, it may mean that we will not be able to continue providing our services such as recruitment, placement, or employment, as the case may be.

5.8 Where we use automated decision-making in our recruitment process, we will use reasonable efforts to ensure that the automated decision-making does not create discriminatory or unjust impacts. Furthermore, if you find that you may have been materially affected by a fully-automated decision, you may request for an explanation of the associated data driving such decision or a human review of such decision.

6. Administration, Management, Protecting and Retaining Your Information

6.1 We will take reasonable efforts to ensure that your personal data is accurate and complete, if your personal data is likely to be used by the Company to make a decision that affects you, or disclosed to another organisation. However, this means that you must also update us of any changes in your personal data that you had initially provided us with. We will not be responsible for relying on inaccurate or incomplete personal data arising from you not updating us of any changes in your personal data that you had initially provided us with.

6.2 We will also put in place reasonable and appropriate administrative, physical and technical measures such as up-to-date antivirus protection, encryption, use of privacy filters, access control, password protection and disclosing personal data both internally and to our authorised third-party service providers and agents only on a need-to-know basis to prevent any unauthorised access, collection, use, disclosure, copying, modification, disposal, leakage, loss, damage and/or alteration of your personal data. However, we cannot assume responsibility for any unauthorised use of your personal data by third parties which are wholly attributable to factors beyond our control.

6.3 You should be aware, however, that no method of transmission over the Internet or method of electronic storage is completely secure. While security cannot be guaranteed, we strive to protect the security of your information and are constantly reviewing and enhancing our information security measures.

6.4 We will also put in place measures such that your personal data in our possession or under our control is destroyed and/or anonymized as soon as it is reasonable to assume that (i) the purpose for which that personal data was collected is no longer being served by the retention of such personal data; and (ii) retention is no longer necessary for any other legal or business purposes.

6.5 Where your personal data is to be transferred out of Singapore, we will comply with the PDPA in doing so. In this regard, this includes us taking appropriate steps to ascertain that the foreign recipient organisation of the personal data is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA. This may include us entering into an appropriate contract with the foreign recipient organisation dealing with the personal data transfer or permitting the personal data transfer without such a contract if the PDPA or law permits us to.

7. Data Breach Notification

7.1 In the event a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, we shall promptly assess the impact and once assessed that it is a notifiable data breach, we shall report this breach within 3 calendar days to the Personal Data Protection Commission (PDPC). We will notify you when the data breach is likely to result in significant harm to you after our notification to the PDPC. We may also notify other relevant regulatory agencies, where required.

7.2 If we are a Data Intermediary, we shall inform the relevant Data Controller without undue delay of any data breach so they can promptly assess the impact and comply with their data breach notification obligation.

8. Updates to this Privacy Policy

We may update this Privacy Policy from time to time. If we change our Privacy Policy, we will post the revised version here, with an updated revision date.

9. How to Contact Us

If you have any questions, requests, grievances or complaints, or comments about this Privacy Policy and/or the handling of your personal data by us, please contact our Data Protection Officer at:

Address: PERSOL Singapore Pte Ltd, 50 Raffles Place, #07-01 Singapore Land Tower, Singapore 048623

Attention: Ms. Edlyn Wee

Email: sg.dataprotection@persolapac.com

Please note that any resumes or job applications sent to this mailbox will NOT be attended to as this mailbox is solely for the purposed of personal data protection related feedback. For submissions of resumes or job applications, please send them to us at info_sg@persolapac.com visit our website at https://www.persolsingapore.com/.

PERSOL

COMPLIANCE MANUAL

PERSOL ASIA PACIFIC PTE LTD & SUBSIDIARIES

Version 8.3
Issue Date: 1 Apr 2026
S/No: Legal-19

TABLE OF CONTENTS

INTRODUCTION **2**

CHAPTER 1
CODE OF ETHICS **3**

CHAPTER 2
ANTI-BRIBERY AND ANTI-CORRUPTION POLICY **7**

CHAPTER 3
INTERNAL PERSONAL DATA PROTECTION GUIDELINES **8**

CHAPTER 4
RECORD RETENTION POLICY **18**

CHAPTER 5
CYBER AND INFORMATION SECURITY POLICY **23**

CHAPTER 6
CORPORATE COMMUNICATIONS & SOCIAL MEDIA POLICY **25**

CHAPTER 7
ANTI-HARASSMENT POLICY **29**

CHAPTER 8
WHISTLEBLOWING POLICY **31**

INTRODUCTION

1. Overview

This Compliance Manual sets out the basic principles designed to guide employees, officers, managers and directors (collectively referred as "**employees**") of PERSOL ASIA PACIFIC PTE LTD and its subsidiaries (individually and collectively the "**Company**", "**We**" or "**Us**") in our business activities. Contract, contingent or temporary workers, part-timers, trainees and consultants are expected to comply with this Compliance Manual and other Company policies applicable to their location and function. All pronouns used in this Compliance Manual shall be deemed to refer to the masculine, feminine or neuter, singular or plural, as the identity of the referenced person or persons.

2. Commitment

We are committed to doing the right thing, conducting ourselves in a legal, ethical and trustworthy manner, upholding our regulatory obligations and complying with both the letter and spirit of this Compliance Manual and applicable local laws in the countries where we operate.

3. Details and Reporting

Every employee is responsible for complying with this Compliance Manual, Company policies and procedures. Our subsidiaries may establish further details on policies and procedures which are consistent or within the scope of this Compliance Manual, hence all employees should comply with those policies and procedures where applicable. If you know or suspect any breach of this Compliance Manual, Company policies or procedures, you should report immediately to your supervisor, Country Head, Regional Headquarters Legal ("**RHQ Legal**") or through the whistle-blowing channel.

4. Disciplinary Action

Any violation of this Compliance Manual or any Company policy or procedures may constitute grounds for corrective action, up to and including termination of employment or engagement. Disciplinary actions may also be taken against supervisors who condone, permit or have knowledge of improper conduct. Reports of known or suspected violations will be promptly investigated by the relevant function heads.

5. Revisions

This Compliance Manual supersedes all previous Company policies issued by RHQ Legal. We reserve the right to modify, revise or supplement this Compliance Manual from time to time. For clarification, please contact RHQ Legal.

6. Inconsistency with Laws

This Compliance Manual shall be subject to all applicable local laws, rules and regulations. In the event any provision in this Compliance Manual conflicts or is inconsistent with any such applicable provision of law or regulation, the latter shall prevail.

1. General

This Code of Ethics is intended to help us and our employees recognise and deal with ethical issues, deter wrongdoing, provide mechanisms to report and prevent dishonest or unethical conduct and foster a culture of honesty and accountability.

2. Behaviors in the Workplace (in the office setting or working from home)

Each of us has a personal responsibility to conduct ourselves, and ensure that our suppliers, agents and representatives are aware of their obligation to conduct themselves, in a legal, ethical way and to comply with both the letter and the spirit of this Code of Ethics. Employees are encouraged to ask their managers questions about particular circumstances that may involve the provisions of this Code.

We are committed to maintaining a work environment, whether in the office setting or working from home, which promotes mutual respect and individual dignity. Inappropriate behaviour in the workplace, which extends to business travel and after-hour Company sponsored events, will result in disciplinary action, up to and including termination.

We strive to ensure a safe workplace for all our employees. We are each responsible for paying close attention to our surroundings, following all safety rules including safe distancing measures to curb the spread of COVID- 19, and reporting any unsafe conditions. The use of alcohol or illegal drugs while at work is not permitted as it can prevent us from thinking clearly and can endanger the safety of others.

It is the Company's policy to protect the employment rights of qualified applicants and employees regardless of an individual's race, age, religion, nationality and/or any other protected categories under applicable laws, and to comply with all applicable laws concerning the employment of persons with disabilities. Consistent with that commitment, it is the Company's policy not to discriminate against qualified individuals with disabilities with regard to application procedures, hiring, advancement, discharge, compensation or other terms and conditions.

To avoid perceptions of favoritism, Conflicts of Interest, lack of confidentiality, unfair treatment or potential liability, (i) a relative of an employee, (ii) a person living in the household of an employee, or (iii) a person in a dating, romantic or other intimate relationship with an employee should not be hired or transferred into a position that results in him or her being in the same chain of command as that employee without the prior written approval of the Country Head and/or the Regional Head of Human Resource ("**HR")**. In the event circumstances develop between employees that would have required the written approval noted above, the employees are required to escalate and report accordingly as mentioned above.

We believe that violence in the workplace is unacceptable. To help protect our co-workers and ourselves, we have an obligation to immediately report any situation involving violence, threats, bullying, or intimidation. If you have concerns about the immediate safety of yourself or others, please contact local authorities before reporting the situation internally.

3. Compliance with Laws, Rules and Regulations

Each of us shall, and shall ensure that our suppliers, agents and representatives are aware of their obligation to comply with all laws, rules, regulations applicable to the Company including all anti-bribery and anti- corruption laws, employment and labour laws, insider trading laws, health, safety and environmental laws, personal data protection laws, and all policies established by the Company.

4. Confidentiality and Privacy

The Company is committed to safeguarding the integrity, availability, and confidentiality of the Company's information and information systems, as well as those entrusted to the Company by its customers, employees, candidates, applicants, vendors, and suppliers. Accordingly, each of us is expected as a condition of employment, to safeguard the data and systems from unauthorised use, disclosure, modification, destruction or loss by complying the Company's Privacy Policy and Internal Personal Data Protection Guidelines.

Confidential and private information includes personal data, as well as Company information that has not been made public, such as business plans, research or strategies, and inside financial information that could be used for personal gain.

Employees are personally responsible for any comments about, and on behalf of the Company, posted to social media networks e.g., Facebook, LinkedIn, Twitter, YouTube, blogs or forums. Please refer to the Corporate Communications and Social Media Policy for further details. Confidentiality obligation continues even after you have ceased employment or engagement with the Company.

5. Protection and Proper Use of Company Assets

We must each protect the Company's assets and ensure their efficient use. No one is to use Company assets for personal benefits.

6. Fair Dealing

We have a responsibility to deal fairly with each other and our customers, employees, applicants, candidates and suppliers. No one must take unfair advantage of anyone else through manipulation, concealment, abuse or confidential information, misrepresentation of material facts or any other unfair dealing practices.

7. Conflicts of Interests and Related Party Transactions

Conflicts of Interest

A "**Conflict of Interest"** arises where an individual's personal interests interfere, or appear to interfere, with the interests of the Company. Conflicts of Interest may compromise, or be perceived to compromise, an individual's ability to act objectively and in the best interests of the Company and its shareholders.

Some common examples of Conflicts of Interest that employees should avoid include:

(a) an employee or a "**Family Member"** receiving an improper personal benefit as a result of the employee's position with the Company. A *Family Member* includes a spouse, parents,

children, siblings (whether by blood, marriage or adoption), or any person residing in the employee's household;

(b) accepting compensation, benefits or advantages in any form from any source other than the Company where such acceptance could affect, or appear to affect, the employee's job performance or objectivity; and

(c) offering, giving or receiving gifts, hospitality or other benefits to or from any person or entity that deals with the Company, where such conduct is intended to influence, or could reasonably be perceived as influencing, the employee's actions or decisions.

If you believe that you are involved in, or may be perceived to be involved in, a Conflict of Interest, you must promptly disclose the matter to Country Head, Country HR or Regional HR so that it can be properly assessed and managed.

Related Party Transactions

The Company recognises that "**Related Party Transactions"** may give rise to actual or potential Conflicts of Interest. A Related Party Transaction refers to any transaction, arrangement or deal between the Company and a party with whom there is a pre-existing business relationship or common interest.

While transactions with related or familiar parties are not inherently unlawful, they may create a conflict of interest or the perception that decisions are influenced by considerations other than the best interests of the Company or its shareholders. Accordingly, such transactions must be reviewed and managed carefully.

If you think that you are involved in, or propose to enter into, any Related Party Transaction, you must promptly inform RHQ Legal through submitting a written declaration (Related Party Risk Register template available on RHQ Legal intranet) and seek approval from the following parties before proceeding with the transaction:

- Approval from Executive Committee ("EXCO") required where related party involves Strategic Business Group ("SBG") Head
- Approval from SBG Head required where related party involves Country Head or Deputy Country Head
- In all other cases, approval from Country Head is required

All Related Party Transaction disclosures will be kept strictly confidential by RHQ Legal and other stakeholders strictly on a need-to-know basis. In the event that internal audit uncovers any transaction which qualifies as a Related Party Transaction but was not previously or not fully disclosed to RHQ Legal, you acknowledge that you may face the following consequence:

- Suspension or termination of the transaction in question
- Internal disciplinary action, up to and including termination of employment
- Liability for loss, damages or financial penalties incurred by the Company due to the suspension or termination of transaction in question

8. Corporate Opportunities

Each of us has a responsibility to the Company to advance its legitimate interests. We must not:

(a) personally take for ourselves or divert to others opportunities that are discovered through the use of Company property, information or our respective positions;
(b) use Company employees, property, information or our respective positions for personal gain; or
(c) compete with the Company directly or indirectly for business opportunities.

9. No Loans or Fees from Candidates

All employees are prohibited from asking for or obtaining loans or fees from candidates. Doing so could create a perception that you're asking for a bribe and breaching our Anti-Bribery & Anti-Corruption Policy (Chapter 2), and possibly breaching local anti-bribery and corruption laws.

10. Reporting Dishonest or Unethical Behaviors

When in doubt about the best course of action to take in a particular situation, employees should talk to their managers. Known or suspected violations of laws, rules and regulations applicable to the Company, of this Code or this Compliance Manual, must be promptly reported to your Country Head, RHQ Legal or through the whistleblowing channel.

11. Co-operating during Investigation

All employees must cooperate fully with the Company during internal investigations on any incidents or any allegations. This includes without limitation, providing truthful information, relevant documentation and any other assistance deemed necessary by the Company. All employees must maintain confidentiality regarding such investigations including any related discussions and refrain from discussing any details with unauthorized individuals.

1. Zero-Tolerance Commitment

The Company adopts a **zero-tolerance** approach to bribery and corruption. Any form of bribery-direct or indirect, public or private, is strictly prohibited. The Company and its employees (collectively "**We**" or "**Us**") have a responsibility to conduct ourselves and ensure that our suppliers, agents and representatives are aware of their obligation to conduct themselves in a legal, ethical way and to comply with both the letter and spirit of this Anti-Bribery & Anti-Corruption Policy.

2. Prohibited Conduct

Each of us have an obligation to comply with all anti-bribery and anti-corruption laws. We must not give, promise, offer or request anything of value to any customer, government employee or other person for the purpose of improperly influencing decisions or gaining business advantage. "**Anything of value**" includes gifts, services, employment opportunities and business opportunities.. We must not engage in conduct that exposes ourselves and the Company to civil and/or criminal liability, significant reputational harm and undermine the trust that our customers, shareholders and communities have placed in us.

We must ensure that no payment (such as facilitation payments or unofficial fees) or reward is received or requested in circumstances where it could be perceived as intended for the purposes of improperly influencing a decision, encouraging or influencing the performance of an illegal or improper act.

Gifts, entertainment and hospitality offered or received by the Company must not be extravagant and must comply with the Gifts & Entertainment Policy.

3. Reporting

If you know or suspect any forms of bribery or corruption, you must report immediately to your supervisor, RHQ Legal or through the whistleblowing channel.

4. Disciplinary Action

Any violations of this Policy may result in disciplinary action, including termination of employment or engagement. The Company may also lodge a policy report or report to relevant government authorities against you.

1. General

All employees must comply with these Guidelines. You must immediately report to your Country Head, Data Protection Officer ("**DPO**") or RHQ Legal if you are aware of any personal data breach or potential breach. If your actions or omissions results in the Company being fined for breaching personal data protection laws, we reserve the right to claim compensation and damages from you.

2. What is "Personal Data"

The term "**personal data**" (also referred to as "**personal information**") means data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access.

Personal data may include:

- Name;
- Contact information (address, phone number, e-mail address);
- Passport or identification details;
- Employee identification number;
- Date of birth;
- Contents of any other identification provided to the Company for application or employment purposes;
- Education and employment history:
- Work-related skills and experience;
- Professional credentials or licenses;
- Membership in professional organisations;
- Any other information contained on an individual's Curriculum Vitae (CV);
- Citizenship and work authorisation status;
- Disability and health-related information;
- Next-of-kin or emergency contact information;
- Information from and related to publicly published profiles you've created on job-related social media platforms and job boards (such as LinkedIn, Monster, or Indeed);
- Information provided by references; and
- Information regarding your career interests, preferences, and qualifications.

In addition, under certain circumstances and consistent with prevailing laws, we may request types of personal data that are viewed by some countries as "**sensitive**":

- National identification, tax identification, passport number or social security number(s);
- Financial or bank account information;
- Results of drug, criminal, and/or background screenings;

- Benefits selections, potentially including health insurance and retirement planning information;
- Biometric data;
- Information contained within your personnel file with the Company, such as performance reviews, disciplinary action and other payroll related information; and
- Health information, including that related to a work-related claim (e.g. workers' compensation claim).

Such sensitive personal data must only be collected, used and/or disclosed if it is required or authorised under any applicable law or where it is reasonably necessary for the purpose and with the individual's consent.

Any data that is not personal data or sensitive data will not be regulated by these Internal Guidelines. For example, data about a Company's share capital, a Company's business address, do not constitute personal data. When dealing with companies, we may come into possession of the personal data of an individual in that Company. Where such personal data is not provided by the individual solely for his personal purposes, such personal data could be considered business contact information ("**BCI**"). BCI is exempted from the application of the data protection obligations (explained below).

3. The Data Protection Guidelines

3.1 Consent and Notification Obligations

We must obtain the prior consent of the individual for the collection, use or disclosure of his personal data for any purpose. Consent may be express or deemed. As far as possible, we should obtain express written consent. You must ensure that you do not misrepresent whenever obtaining consent. We should include contractual terms requiring third parties to obtain the individual's consent for disclosure to us, or directly approach the individual to obtain consent.

Where we intend to disclose personal data to third parties for certain purposes, we must obtain the consent of the individual. These purpose(s) must be notified to the individual and that individual's consent obtained prior to disclosure. If you receive a request from a public agency for disclosure, you must immediately consult and seek approval from Country Head, Data Protection Officer or RHQ Legal before disclosure.

Where the individual is below twenty-one (21) years of age but thirteen (13) years or older, we may treat consent as valid. However, if you think that the minor does not have sufficient understanding of the nature and consequences of giving consent, you must seek the consent of the minor's parent or legal guardian.

An individual is entitled to withdraw his consent at any time. Upon receipt of such a notice, you must immediately:

(i) inform the individual of the likely consequences of his/her withdrawal of consent, i.e. the Company would no longer be able to provide services to him/her;
(ii) cease collecting, using or disclosing the individual's personal data;
(iii) inform our data intermediaries and agents to cease collecting, using or disclosing that individual's personal data as well; and
(iv) confirm to your Data Protection Officer that the above steps are done.

3.2 Purpose Limitation Obligations

We will collect personal data in a manner consistent with the notice provided to the individual. We shall not use or disclose personal data other than the primary purpose of collection, unless:

(i) The individual has consented to the use or disclosure; or
(ii) The individual would reasonably expect us to use or disclose personal data for a secondary purpose and the secondary purpose is related to the primary purpose; or
(iii) We have reason to suspect that unlawful activity has been, or may be engaged in, and uses or discloses the personal data as a necessary part of its investigation of the matter or in reporting its concerns to relevant authorities; or
(iv) The use or disclosure is required or authorised by or under law, rule or regulation; or
(v) We reasonably believe that use or disclosure is necessary to prevent or lessen a serious and imminent threat to public health or public safety of the life or health of the individual.

Any new purpose that will not satisfy any of the conditions above requires fresh consent before you can process the personal data. Each department is to keep track of and map the movement or transfer personal data of an individual. If you intend to take photographs or video of an individual at Company door events, and use the photograph or video for a significant period of time, please notify the individuals beforehand and obtain the consent of the individual.

3.3 Access Obligations

Any individual has the right to request from us the following:

(i) Details of personal data of the individual that is in the Company's possession or control; and
(ii) Information on how we have used or disclosed, or may have used or disclosed such personal data, in the one (1) year preceding the date of the individual's request.

Once you receive an access request from an individual, you must verify the identity of the requestor to ensure the legitimacy of the access request and provide such requested information within thirty (30) calendar days from the date of request. Concurrently, please notify your Data Protection Officer if you receive such a request.

If it is appropriate to not provide some or all of the personal data requested in the access request ("**withheld personal data**", you shall preserve a copy of the withheld personal data for a period of at least thirty (30) calendar days after rejecting the access request – as the individual may seek a review of the decision. In the event the individual submits an application for review to the Personal Data Protection Commission ("**PDPC**") and the PDPC determines that it will take up the review application, it should, as good practice, preserve the withheld personal data until the review by PDPC is concluded and any right of the individual to apply for reconsideration and appeal is exhausted.

3.4 Correction Obligations

Any individual may request us to correct an error or omission in the personal data that is in the Company's possession or control. Once you receive a correction request from an individual, you must verify the identity of the requestor and ensure the legitimacy of the correction request and within thirty (30) calendar days:

(i) Correct the personal data as soon as practicable; and

(ii) Send the updated personal data to every other organisation(s) to which the personal data was disclosed by us within a year before the date the correction was made, unless those organisation(s) do/does not need the corrected personal data for any legal or business purpose or we have the consent of the individual to only send to specific organisation(s).

We would need to respond to a correction request that we receive in writing. This includes writing that is in electronic form, such as an online submission of a request or an email. If the request is made verbally, you should ask for the request in writing.

Where we do not correct the personal data pursuant to a correction request received from an individual or from another Company because we are satisfied that there are reasonable grounds for a correction not to be made, we must make an internal note or comment on the personal data that a correction was requested but not made. For any correction request that we denied, we may provide the requestor with reasons.

3.5 Accuracy Obligations

We must ensure that all personal data is accurate and correctly recorded. If you rely on third party data intermediaries or service providers to provide personal data, you must ensure that the personal data provided to the Company is accurate and complete.

3.6 Protection Obligations

We must protect personal data in our possession or control (whether in physical or electronic form) by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Examples of data breaches:

(i) Loss or theft of personal data, equipment on which personal data is stored (e.g. a memory stick) or paper records;
(ii) Inappropriate access controls allowing unauthorised use of personal data (e.g. uploading personal data to an unsecured web domain, using unsecure passwords);
(iii) Equipment failure where personal data stored in such equipment may be affected;
(iv) Personal data left unlocked/unprotected in accessible areas (e.g. leaving IT equipment unattended when logged into a user account);
(v) Disclosing personal data to unauthorised individuals;
(vi) Collection of personal data by unauthorised individuals;
(vii) Human error/accidental disclosure of personal data (e.g. emails containing personal information sent to the wrong recipient);
(viii) Hacking, viruses or other security attacks on IT equipment systems or networks;
(ix) Breaches of physical security (e.g. forcing of doors/windows/filing cabinets) where the intruder may gain access to personal data.

If a breach arises or is suspected, please refer to the Personal Data Breach Response Plan for guidance.

Examples of Security Arrangements – Administrative Measures	
1	Requiring employees to be bound confidentiality obligations in their employment agreements.
2	Implementing and enforcing the policies and procedures (with disciplinary consequences for breaches including termination from employment) that have been put in place including with regard to confidentiality obligations.
3	Conducting regular training sessions for staff to impart good practices in handling personal data and strengthen awareness of threats to security of personal data.
4	Implementing procedures/practices to regularly check the security arrangements.

5	Whether to disallow the use of personal devices and thumb drives in the office and prohibiting the connection of such devices to the office network. This would depend on the nature of personal data handled by the Company on an operational basis and its operational needs.
6	Auditing or assessing data intermediaries or third party services providers to ascertain what they have done for personal data protection compliance and their security measures in place, such as IT maintenance companies, security companies, recruitment companies, courier companies, and only engaging those who have passed the internal assessment. Thereafter, if possible, conduct regular audits of the data protection policies and internal procedures that are adopted by third party data intermediaries.
7	Where personal data is to be disclosed to any third party (including data intermediaries), prior to that, putting in place a suitable contract with adequate clauses requiring the recipient Company to protect the personal data and to indemnify the Company from loss or damage.
8	Ensuring that only the appropriate amount of personal data is held, as holding excessive data will also increase the efforts required to protect personal data.

Examples of Security Arrangements – Physical Measures	
1	Marking confidential documents clearly and prominently.
2	Implementing secure storage processes, for example storing confidential documents or documents containing personal data in locked file cabinet systems with access given to only selected staff.
3	Adopting a clear/clean desk policy.
4	Restricting employee access to confidential documents or documents containing personal data, on a need-to-know basis. This includes not indiscriminately sharing personal data with other colleagues.
5	Using privacy filters to minimise unauthorised personnel from viewing personal data on laptops.
6	Disposing of confidential documents or documents containing personal data, that are no longer needed, by shredding or similar means.
7	Other mediums containing personal data such as flash drives should be appropriately destroyed physically when no longer required.
8	Implementing security measures for the intended mode of delivery or transmission of personal data that affords the appropriate level of security (e.g. Registered mail instead of normal mail, or use of encryption instead of normal passwords, where appropriate).
9	Not reproducing in physical form electronically stored personal data such as those in an electronic database unless necessary to conduct the business and if so, to then promptly destroy under secure circumstances such physical documentation containing the personal data.
10	Deploying CCTV cameras outside storage places (such as storage rooms) where personal data is kept.
11	Confirming that the intended recipient of the personal data is the correct recipient to avoid undue disclosure of personal data.

Examples of Security Arrangements – Technical Measures	
1	Ensuring computer networks are secure including adoption of use of firewalls and passwords to protect systems and networks from unauthorised access, modification and disclosure.
2	Backing up data by the Company.

3	Adopting appropriate access controls (e.g. Considering stronger authentication measures where appropriate) not only for access to computer networks but also to office premises, and implementing security alarm systems to prevent unauthorised access to premises.
4	Encyrpting personal data to prevent unauthorised access.
5	Considering disabling USB ports (subject to operational requirements or requirements of other law) on computers.
6	If personal devices and thumbdrives are permitted, to ensure that all data stored on such devices are encrypted and password protected.
7	Activating self-locking mechanisms for the computer screen if the computer is left unattended for a certain period and passwords are not to be shared with any other employees.
8	Installing appropriate computer security software and using suitable computer security settings, including those able to track when someone plugs his personal device or thumbdrive to the computer network.
9	Disposing of personal data and formatting of all storage media/components in IT devices that are to be recycled, sold, disposed or returned to the lessor. This includes photocopier machines[1].
10	Using the right level of email security settings when sending and/or receiving highly confidential emails or documents containing personal data.
11	Updating computer security and IT equipment regularly.
12	Ensuring that IT service providers are able to provide the requisite standards of IT security.

3.7 Retention Limitation Obligations

We must securely delete or destroy documents containing personal data as soon as it is reasonable to assume that the personal data is no longer needed for the purpose(s) for which it was collected and no longer required for business or legal purposes. Please refer to Chapter 4 on Record Retention for details.

3.8 Transfer Limitation Obligations

We must not transfer personal data to a foreign country unless we ensure that the recipient is bound by legally enforceable obligations with a level of protection that is comparable to the protection under the Singapore data protection laws.

Personal data may be transferred to recipients located outside if the transferor's country under certain conditions:

(i) The recipient can implement all the necessary controls to fulfil applicable obligations regarding the processing of personal data taking account of security and privacy risks and the scope of processing; and

(ii) The recipient can demonstrate evidence of compliance with the Company's instructions and/or agreements/contracts.

[1] Note that a photocopier machine potentially could have a hard disk drive and if it is on lease and upon expiry of lease, or if it is to be discarded, measures must be put in place to permanently erase all personal data on such hard disk drive.

3.9 Accountability Obligations

We are required to ensure and demonstrate compliance with the PDPA, and be able to demonstrate proper management and protection of personal data.

We must attend to enquiries and complaints related to how we collect, use and/or disclose personal data, or about our internal policy on data protection, as well as entertain and institute an investigation in relation thereof. Our DPO business contact information shall be made available publicly for this purpose.

We must conduct data protection impact assessment for every new process or systems that involves personal data and when there are events that significantly change in our environment which may affect the processing of personal data.

We must ensure that contract terms with clients include data protection clauses to cover instances where the engagement involves collecting and processing personal data, and we should obtain clear clients' instructions for such. Similarly, we must ensure the same for our suppliers if they will receive or have access to any personal data or process personal data on our behalf.

3.10 Data Breach Notification

The Personal Data Breach Response Plan serves as a guide to deal with a data breach including critical timelines and notification requirements.

All employees must immediately notify the DPO if they become aware of a data breach to enable the appropriate assessment, investigation and remediation measures to be taken in a timely manner, including possible notification to PDPC (where the Company acts as the Data Controller), or notification to our clients (where the Company acts as the Data Intermediary/Processor on behalf of the client).

4. Offences

In Singapore, the Personal Data Protection Commission ("**PDPC**") is the regulatory body charged with enforcing the data protection laws and has powers to carry out investigations and impose directions and financial penalties of up to S$1 million or ten per cent (10%) of organisation's annual turnover in Singapore, whichever is higher, for a data breach.

Criminal offences under the Singapore data protection laws include, but not limited to:

(i) Disposing of, altering, falsifying, concealing or destroying, or directing another person to dispose of, alter, falsify, conceal or destroy a record containing personal data or information about the collection, use or disclosure of personal data, with an intent to evade an individual's access or correction request;
(ii) refusing any PDPC officer access to any premises;
(iii) obstructing PDPC officers in the exercise of their powers or performance of their duties; and
(iv) knowingly or recklessly making a false statement to the PDPC, or knowingly misleading or attempting to mislead the PDPC, in the exercise of their powers or performance of their duties.

Any party who suffers losses or damages resulting from a breach of the data protection obligations by the Company can file a civil claim against the Company for damages.

4.1 Do Not Call Registry

There are strict requirements and prohibitions with regard to the sending of marketing text messages or faxes or making of marketing voice calls where the recipient is in Singapore, even if the sender is overseas. A breach is a criminal offence. Please refer to and comply with paragraph 5 below.

4.2 What To Do in a Raid by the Personal Data Protection Commission Official

In the event that representatives of the personal data protection regulatory officials arrive at the Company, you must allow them entry and, to the extent it is legally permissible, IMMEDIATELY inform your Country Head, Data Protection Officer or RHQ Legal. You should comply with the regulatory officials' request to search premises after verifying identities of the regulatory officials. Please refer to the Personal Data Breach Response Plan for further details.

5. (Applicable if you contact Singapore telephone numbers) Internal Do Not Call Policy

A Do Not Call ("**DNC**") regime has been established under the Personal Data Protection Act 2012 (the "PDPA") to enable individuals to register their Singapore telephone number(s) with the DNC registry if they do not wish to receive marketing messages through their Singapore telephone number. The DNC registry is operated by the Personal Data Protection Commission.

All employees and agents of our Singapore companies must strictly comply with these Internal Guidelines. For overseas subsidiaries, please note that the DNC framework applies to recipient of Marketing Messages (herein defined) in Singapore. This means that if the sender is overseas, the DNC framework would apply to the sender.

A breach of the DNC regime/framework carries with it criminal liability under the PDPA. If any of our Singapore companies are fined for breaches of the DNC framework as a result of your action or omission, the Company reserves its right to claim compensation and damages from you.

5.1 Messages Impacted by the DNC Framework

The DNC framework applies to all forms of messages, whether in sound, text, visual or other form, e.g. Short Messaging Service ("**SMSes**") messages and Multimedia Messaging Service ("**MMSes**") messages, voice calls and any data applications which use a Singapore telephone number[2]. A voice call includes a call that involves a recorded or synthetic voice.

The DNC framework imposes restrictions on marketing telephone or voice calls, marketing text messages (SMSes and MMSes) and/or fax messages, that are sent to a Singapore telephone number (landline no., mobile no. or fax no.). The DNC framework does not apply to telephone numbers outside of Singapore.

Under the DNC framework, a Do Not Call registry ("**DNC Registry**"), comprising of three (3) registers maintained by the PDPC, namely one for marketing telephone or voice calls, one for marketing text messages (SMSes and MMSes) and one for fax messages (the "**DNC Registers**").

A user of a Singapore telephone number who doesn't wish to receive any marketing messages to his/her Singapore telephone number may choose to register his/her number on any or all of the three (3) DNC Registers.

[2] For example, WhatsApp, iMessage etc.

Under the DNC framework, marketing messages ("**Marketing Messages**")[3] subjects to certain conditions, a breach of which will be criminal. A "Marketing Message" includes (but not limited to) a message:

(i) To offer to supply goods or services;
(ii) to advertise or promote goods or services;
(iii) to advertise or promote a supplier, or prospective supplier, of goods or services;
(iv) to offer to supply land or an interest in land;
(v) to advertise or promote land or an interest in land;
(vi) to advertise or promote a supplier, or prospective supplier, of land or an interest in land;
(vii) to offer to provide a business opportunity or an investment opportunity;
(viii) to advertise or promote a business opportunity or an investment opportunity; or
(ix) to advertise or promote a provider, or a prospective provider, of a business opportunity or an investment opportunity.

5.2 Checklist Prior to Sending of Marketing Messages

Please refer to the Checklist below before sending a Marketing Message to Singapore number:

- ☐ Determine if the message (voice call, SMS/MMS or fax) to be sent is to a Singapore telephone number.
- ☐ Find out if the individual has provided clear and unambiguous consent to receive such Marketing Message on his/her Singapore telephone number.
- ☐ Ensure that the individual's consent (if any) is evidenced in written or other form so as to be accessible for subsequent reference.
- ☐ Determine if the consent has since been withdrawn.

  If there is such consent and the consent has not been withdrawn, you may proceed to send the Marketing Message but only send via the method of communication that the individual has consented to. For example, if the individual has only consented to receiving Marketing Messages via SMS, you must only send the Marketing Message via SMS. You must not make a marketing voice call to him/her.

- ☐ Find out if the exemption relating to marketing fax messages or marketing text messages applies.
- ☐ Check to see if the Singapore telephone number has been checked previously and if the present time is within the validity period for the results of the DNC registry check.
- ☐ Ensure that the Singapore telephone number has been checked against the relevant DNC Register within the prescribed period.
- ☐ Ensure that the Marketing Message contains clear and accurate information identifying the Company as well as how the recipient may contact the Company.
- ☐ Ensure that such information remains valid for at least thirty (30) days after the receipt of the message.
- ☐ If the Marketing Message is a voice call, ensure that the calling line identity is not concealed.
- ☐ Ensure that all requirements for Marketing Messages as set out by regulations under the Singapore Personal Data Protection Act ("**PDPA**") are complied with.
- ☐ Ensure that the Marketing Message is sent during the validity period of the results of the DNC Registry check.

[3] In the PDPA, such messages are defined as "specified message" but for ease of understanding, we have referred to them as Marketing Message instead.

- Monitor and be watchful for any communication by recipients indicating that they wish to cease receiving Marketing Messages and ensure that this withdrawal of consent is immediately communicated to the Data Protection Officer and acted upon.
- Ensure that any withdrawal of consent is immediately communicated to any third parties engaged to send Marketing Messages on behalf of the Company.
- Ensure that no Marketing Messages are sent to the individual (whether by the Company itself or by third parties engaged by the Company to send Marketing Messages on its behalf) after the stipulated period of time.

5.3 Extra-territorial Effect

The requirements and prohibitions of the DNC regime/framework have extra-territorial effect. They apply where the sender or the recipient of the Marketing Message is in Singapore. The sender and the person who authorised the sender will be liable for a breach of the DNC regime.

1. General

It is to ensure that necessary Company records and documents (both in hard copy and electronic form) are adequately maintained for the business operations as well as to comply with applicable legal requirements and that documents that are no longer needed are discarded at the proper time.

2. Administration

Any documents and records that are part of any of the categories listed in the Record Retention Schedule must be retained for the amount of time indicated in the Schedule. If you are unsure whether to continue to retain or to destroy a certain record or document, please contact your Country Head or RHQ Legal.

Each Country Head (or their respective delegate(s)) ("**Administrator**") is in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed. The Administrator is authorised to modify the Record Retention Schedule from time to time to ensure compliance with applicable laws and appropriate for the operational needs of the Company, subject to RHQ Legal's approval.

You agree that we may regularly audit employee files and computer hard drives to ensure compliance with this policy. If you feel that you or another employee may have violated this policy, please report the incident immediately to your supervisor.

3. Storage

The Company's records and documents must be stored in a safe, secure and accessible manner. Hard copies of confidential records such as personal data of candidates, employee P-files, unpublished financial statements, shall be locked away when not in use, and electronic records shall be password protected. Access to confidential records should only be granted to authorised personnel. Please refer to the chapter on Cyber and Information Security for further details.

Most correspondence and internal memoranda should be retained for the same period as the document they pertain to or support. For example, a letter pertaining to a particular contract should be retained for as long as such contract is required to be retained in the Record Retention Schedule. Records that support a particular project or transaction should be kept with the project or transaction and be subject to the same retention time of that particular project or transaction.

3.1 Routine Documents

Documents and records that are not listed in the categories in the Record Retention Schedule which relate to routine matters (such as routine letters and notes e.g. Notes of appreciation, plans for meetings, letters of inconsequential subject matter and where no further reference will be necessary, etc) may be discarded after **three (3) months from the date of the documents.**

3.2 Non-Routine Documents

Documents and records that are **not** listed in the categories in the Record Retention Schedule which relate to non- routine matters or have significant lasting consequences should be retained for **ten (10) years from the date.**

4. Destruction

Each Country Head is responsible for the continuing process of identifying the records and documents that have met their required retention period and supervising of their destruction. It is also the responsibility of all employees to periodically review and delete/destroy documents and records in compliance with this Policy.

The destruction of confidential, financial and personnel-related records must be conducted by shredding if possible. Each country team or business team must coordinate with your local IT team or PAPAC IT for the destruction of emails, electronic records and documents.

For personal data records, disposal should be in a manner that the personal data shall be unreadable (paper) or irretrievable (for electronic records). Below summarises the main approaches for the disposal of personal data:

(i) Paper disposal
- Shred using at least P-3 security level cross cut shredder
- If a 3rd party is engaged for disposal of huge volume of paper records, a certificate of destruction must be obtained

(ii) Electronic destruction
- As electronic files are not completely destroyed after they have been deleted and the recycle bin is cleared, any of the following steps will be used to permanently destroy or removed electronic data:
  - Using a dedicated software that can overwrite selected files or the entire storage drive; or
  - Using a specified hardware appliance that cater for the destruction (e.g., a degausser machine that produces a strong electromagnetic field that can destroy magnetically recorded data); or
  - Physically destroying the storage device by crushing, drilling, or shredding it.
- Alternatively, where it applies, we may decide to anonymise the personal data. If this option is considered, we must assess the risk to address possible re-identification.

Where your team/department is engaging with an external third party service provider for disposal and/or destruction services, you must obtain the prior written approval(s) from either your Reporting Manager and/or the respective Country IT Manager to ensure such disposals and/or destructions comply with the following criteria:

(i) exercise due care in selecting an appropriate and reputable service provider;
(ii) ensure that we sign a valid binding contract with the service provider, which imposes confidentiality and where personal data is involved, personal data protection obligations on the service provider to keep our information confidential and not disclose to unauthorised parties; and
(iii) keep records of these Agreements for future audit / compliance checks.

5. Suspension of Destruction

If you believe or are informed that the Company records or documents are relevant to current or pending litigation, government investigation, audit or other similar events, you must preserve and not delete, dispose, destroy or change such records and documents, including emails, until the Company determines those records and documents are no longer required.

You may also be requested by the Company to suspend any routine document disposal or destruction from time to time, including without limitation, where such records or documents may be relevant to group restructuring, merger, etc.

RECORD RETENTION SCHEDULE

NO.	RECORD TYPE	RETENTION PERIOD
1.	**OPERATIONS MANAGEMENT**	
(a)	Terms of Business[4]	Ten (10) years from the date of completion of the contract
(b)	Service Agreements or Master Service Agreements[5]	
(c)	Employment contracts signed between candidates and the Company's clients[6], e.g. candidates placed to work for banks/other clients i.e. candidates are NOT the Company's employees. Where candidates are the Company's employees, please refer to paragraph 4 below (Human Resource and Personnel Records)	
(d)	Candidates' application forms of successfully placed candidates with the Company's clients i.e. candidates are NOT the Company's employees. Where candidates are the Company's employees, please refer to paragraph 4 below (Human Resource and Personnel Records)	
(e)	Curricula Vitae or resumes of successfully placed candidates with the Company's clients i.e. candidates are NOT the Company's employees. Where candidates are the Company's employees, please refer to paragraph 4 below (Human Resource and Personnel Records)	
(f)	Application forms, Curricula Vitae or resumes of candidates who are NOT placed with any of the Company's clients or NOT employed by the Company	Five (5) years from the date of the collection or the date of refreshed consent from the candidate, whichever is later
(g)	Documents and records related to International Organisation for Standardisation ('ISO") and Data Protection Trustmark ("DPTM") certification and/or standards (which does not contain any personal data)	Three (3) years from the date of certification, or such period as necessary for business purposes or required by applicable laws, whichever is later
2.	**ACCOUNTING, FINANCE & TAX**	
(a)	Accounts Payable and Receivable ledgers and schedules	Five (5) years or such other period as required by applicable laws, whichever is later
(b)	Annual audit reports and financial statements	
(c)	Annual plans and budgets	
(d)	Bank statements, cancelled cheques, deposit slips and similar documents	
(e)	Employee / business expense records	
(f)	General ledgers	

[4] These documents fall within the same category as item 3(a) (Legal Contracts or Agreements) and is restated here for easy reference by operations teams.

[5] As above footnote 1.

[6] Documents in 1(c) – (e) should follow the retention period of the underlying contracts signed between the Company and the Client.

(g)	Invoices	
(h)	Tax Returns	
(i)	Tax exemption documents and related correspondence	
(j)	Tax receipts, invoices, statements	
3.	**LEGAL CONTRACTS OR AGREEMENTS**	
(a)	Contracts and related correspondence	Ten (10) years from the date of completion of the contract
(b)	Legal opinions	Ten (10) years from the date of the legal opinion
(c)	Litigation records and Court Orders	Ten (10) years from the date of the statement of claim (if no court order is issued) or the court order, whichever is later
(d)	Documents pertaining to investigations and other correspondence with government authorities	Ten (10) years from the date of completion of the investigation or date of correspondence
(e)	Documents and correspondence pertaining to intellectual property rights (e.g. patent and trademark applications, etc.)	Ten (10) years from the date of expiry of the grant of intellectual property rights
(f)	Licenses and permits	Ten (10) years from the date of Licences and Permits, or ten (10) years from the date of expiry of the Licence, whichever is later
(g)	Corporate Records (minute books, annual and other corporate fillings, signed minutes of boards or shareholders' meetings, corporate, seals, Constitutions), policies and manuals	Five (5) years from the date of dissolution of the relevant Company or such period as required by applicable laws[7]
4.	**HUMAN RESOURCES OR PERSONNEL RECORDS**	
(a)	Employment contracts	In accordance with Annex 2 or such other period as required by applicable laws
(b)	Employee personnel records (including individual attendance records, benefits, application forms and resumes, records relating to background checks on employees, job or status change records, performance evaluations, retirement and pension records)	
(c)	Payroll registers	
(d)	Documents and records pertaining to illness and injury claims	
5.	**INSURANCE**	
(a)	Insurance claims / applications	Ten (10) years from the date of claim or date of payout, whichever is later
(b)	Insurance contracts / policies (director and officers, general liability, property, workers' compensation)	Ten (10) years from the expiry of the insurance contracts / policies, where no claims are made. Where claims are made, then refer to row above

[7] Section 320 of the Companies Act of Singapore provides, inter alia, that when a company has been wound up the liquidator shall retain certain books and papers for a period of 5 years from the date of dissolution of the company and at the expiration of that period may destroy them, except in prescribed situation.

6.	REAL PROPERTY OR MOVABLES	
(a)	Correspondence, purchase / sale / lease agreement	Ten (10) years from the disposal of the property or expiry of the lease, whichever is applicable
(b)	Property insurance policies	Ten (10) years from the disposal of the property or expiry of the lease, whichever is applicable

Retention periods for **Human Resource and Personnel Records** are set out below based on consultation with the respective local HR teams. If changes are required, please notify RHQ Legal.

COUNTRY	RETENTION PERIOD for Human Resource and Personnel Records (calculated from the employee's last date of service)
Singapore	5 years
Malaysia	7 years
China	2 years
Hong Kong	7 years
India	7 years
Indonesia	10 years
South Korea	3 years
Taiwan	5 years
Thailand	10 years
Vietnam	4 years

The full contents of the CHAPTER 5 CYBER & INFORMATION SECURITY POLICY are integrated into our PAPAC IT policies. Please refer to the following link for more details on our updated IT policies: link to Group IT Policies and Procedures.

In general, please take not of the following:

1. Clear Desk and Clear Screen

Employees shall ensure that their workstations are clear of information, whether in electronic or paper form, to reduce the risks of unauthorised access, loss and compromise:

(i) Whenever unattended or not in use (e.g., if you leave your desk for any reason), all workstations must be left logged off or protected with a screen or keyboard locking mechanism controlled by a password or similar user authentication mechanism.
(ii) A password-protected screen saver must be enabled on workstations and automatically activated after fifteen (15) minutes of inactivity. The screen saver configurations must be managed by IT.
(iii) When viewing confidential information including personal data on a screen, users must be aware of their surroundings and must ensure that unauthorised parties are not permitted to view the information.
(iv) Passwords must not be posted on or under a computer / desk or in any other accessible location.
(v) Laptops and all portable electronic media must be locked away in a drawer or cabinet when the work area is unattended or at the end of the workday.
(vi) Restrict the creation of hardcopy material with personal data to the minimum needed to fulfil the identified processing purpose. All hardcopies of personal data and other confidential information must be removed from desk and locked in a drawer or file cabinet when the workstation is unattended and at the end of the workday.
(vii) Drawer or file cabinets containing personal data and other confidential information must be locked when not in use or when not attended.
(viii) Keys used to access confidential documents including those with personal data must not be left at an unattended work area.
(ix) Copies of documents containing personal data and other confidential information must be immediately removed from printers and facsimile machines.
(x) Copies of documents containing personal data and other confidential information must not be left in unattended boxes or bins and must be secured until the time that they can be shredded, or their retention period ends.

2. Employee Privacy

All Personal Information collected by Company shall be handled in accordance with the Company's Privacy Policy and Internal Data Protection Guidelines. In order to ensure the security of Company's network and information, to access any information passing across the network, and to ensure the proper and permitted usage of the network by all users, the Company reserves the right to monitor any and all aspects of its Communication and Information Systems and terminate access to and use of such systems at any time without notice to the extent permitted by applicable law where the user resides.

The monitoring of Company's Communication and Information Systems may result in the collection and processing of Personal Information being transmitted over these mediums. Accordingly, except where otherwise required by law, employees and other users of the Communication and Information Systems will not be afforded privacy when communicating

through voice mail, e-mail, and the Internet. In using and accessing Company networks and systems, all users explicitly agree to this as an express condition of usage.

3. Incident Response

All employees, contractors and third-party users of information systems and services should report any observed or suspected security weaknesses such as breach involving Company information to PAPAC IT team immediately.

4. Enforcement

Employees who are suspected of committing breaches of security will be handled under formal disciplinary procedures. We may suspend, block or restrict access to information and network resources when it reasonably appears necessary to do so in order to protect the integrity, security, of functionality of Company resources or to protect the Company from liability. We may refer suspected violations/security breaches of applicable law to appropriate law enforcement agencies. This also can result in disciplinary action up to and including termination.

1. Corporate and Media Communications

1.1 You are not to respond, under any circumstances, to inquiries from the news media, investment community or industry analyst ("**Inquiries**") unless specifically authorised to do so by our Executive Committee ("**EXCO**"), RHQ Marketing team and/or their respective duly authorised representatives (jointly and severally "**Spokesperson(s)**"). Employees who receive such inquiries either directly or indirectly must refer the inquirer to the appropriate Spokespersons.

1.2 Our financial performance and related financial information should not be disclosed without the prior written consent of PAPAC Finance Director, unless such information is already publicly disclosed by the Company, or where the disclosure of the information is required by law. Where disclosure of any information by you is required by law, you shall immediately notify RHQ Legal of that fact so that we may (if appropriate) seek to prevent that disclosure, and take such steps to prevent or minimise the scope of disclosure.

1.3 All proprietary Company information, including patent, copyright, and trade marks (whether registered or unregistered), trade secrets, branding and marketing strategy and initiatives, future and proposed products and services of the Company (which includes, without limitation, their respective information concerning research, experimental work, development, processes, intentions, product information), know- hows, software, discoveries, creations, inventions, confidential information, marketing opportunities, financial information, acquisition and expansion strategy, performance, forecasts, market share, and customer information, should not be disclosed to the social media or any other third parties, including without limitation, internet, television, radio and print media, students, or researchers, unless authorised to do so by our CEO and in accordance with this Policy. Only information released through our official website, media releases, annual report, press room, and other approved material, may be provided to media, students, or researchers.

1.4 In the event of an emergency where you are unable to seek timely approval from the Spokesperson(s), prior to responding to any Inquiries, please do the following:

(a) refer to the Guidelines in Annex A to help you in responding to inquiries; and
(b) promptly (within 12 hours) notify RHQ Marketing or the team representing the relevant Company that you have been contacted by the media, and consult and keep RHQ Marketing or the team representing the relevant Company updated throughout the event.

1.5 In the event of Inquiries concerning any current or potential litigation, please inform RHQ Legal promptly. In such event, all communications should be in such manner as advised by RHQ Legal to preserve legal privilege. Legal privilege protects confidential communications between the Company's employees and RHQ Legal and/or external lawyers.

2. Social Media Use

2.1 As an employee of the Company, you are personally responsible for any comments about and on behalf of the Company that you post on the social media network, e.g. Facebook, LinkedIn, Twitter, YouTube, Blogs or forums. Therefore, be mindful that your postings will be available to the general public, reflect on the Company reputation and business interests and ensure that your postings do not interfere with your work or create a conflict of interest between you and the Company. If your social media post(s), whether in a personal or official capacity, causes or is

likely to cause the Company any reputational damage or loss, or otherwise taint the public image of the Company, you shall co-operate with the Company to immediately remove or amend your post(s), and take such other steps as may be reasonably requested by the Company. This requirement for co-operation and amendment/removal of posts remains regardless whether your social media posts includes a disclaimer that you were only expressing your personal views and not those of the Company.

2.2 Any intellectual property created by you on such social media networks that is created during the course of your employment and/or using the property of the Company shall be considered "work made for hire" and shall be the property of the Company.

2.3 **Guidelines on Social Media Use:**

(a) Clearly identify yourself and your role within the Company when communicating about the Company, its products and services, customers, suppliers, vendors, and competitors. Only authorised Spokespersons can speak on behalf of the Company as a whole. When posting comments on the Web, make it clear your comments are your own and not those of the Company.

(b) If you identify yourself as an employee of the Company, post a prominent disclaimer stating that you are only expressing your personal views and not those of the Company. For example: "*The views expressed on this Website/Weblog are mine alone and do not necessarily reflect the views of my employer.*"

(c) Do not infringe on the Company's logos, brand names, images, or trademarks, which includes, without limitation, setting up Company-branded pages or sites on social networks such as a Company-branded Facebook page or Company -branded Twitter account. Only the RHQ Marketing or the team representing the relevant Company is authorised to create Company- branded pages or sites on social networks.

(d) Use good judgment. Be smart about what you publish; once you post something, assume it lives forever. You are responsible for what you post. Take it seriously.

(e) Be respectful to other employees, customers, competitors, and members of the public.

(f) Be truthful. Strive for accuracy. Stick to the facts.

(g) Always credit sources with citations or links. Respect intellectual property laws governing copyright, fair use of copyrighted material, trademarks, and other intellectual property, including that of third-parties.

(h) All Company policies and standards apply, including, but not limited to, policies related to illegal harassment, code of conduct, non-competition, conflict of interest, and protecting trade secrets and other confidential and/or proprietary information. When posting, be aware of these policies.

2.4 **Prohibited conduct on social media includes without limitation:**

(a) Disclosing trade secrets and other confidential or proprietary information, belonging to the Company, customers, candidates, or employees, such as candidate lists, customer lists, pricing information, strategy discussions, personal data, personal health information, information regarding the development of systems, processes, products, know-how, technology, internal reports, policies, procedures, or other internal business-related confidential communications and Company proprietary information.

(b) Violating the Company's internal employee handbook and other policies.

(c) Exposing yourself or others to material online or through e-mail that may create a hostile work environment.

(d) Using statements that could be viewed as malicious, obscene, threatening or intimidating, that disparage employees, applicants, candidates, customers, members, associates, or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts

that could contribute to a hostile work environment on the basis of race, sex, disability, age, religion, or any other status protected by law or Company policy.

(e) Forming biases against an applicant based on information that is not appropriate to consider when making a networking or hiring decision.

(f) Spamming (i.e., sending unsolicited bulk e-mail that is not work related, such as commercial advertising).

(g) Allowing the use of social media to interfere with work responsibilities - while you are on work time, refrain from online activities that are not work related.

2.5 **Reporting Social Media Postings**

If a negative post or comment is found online about the Company, or a post that may violate this Policy, please contact RHQ Marketing for review and evaluation to determine appropriate action, if necessary. For instance, if a post is found online of an employee disclosing a Company trade secret, an employee threatening violence, or an employee complaining about harassment at the workplace, contact RHQ Marketing and RHQ Human Resource immediately.

2.6 **Employee, Applicant, and Candidate Social Media Usernames and Passwords**

Do not request or require any employee, applicant or candidate to provide any password or other related account information in order to gain access to employee, applicant or candidate's account or profile on a social network.

ANNEX A

Guidelines on Responding if You Could not Get Timely Approval

No.	When commenting on:	Guidelines
1	Company Financial Performance	The financial performance of the Company and related financial information should not be disclosed without the prior written consent of PAPAC Finance Director, unless such information is already publicly disclosed by the Company, or where the disclosure is required by law. Where disclosure of any information by you is required by law, you shall immediately notify RHQ Legal of that fact so that the Company may, if it wishes, seek to prevent that disclosure, and take such steps as required by the Company, to prevent or minimise the scope of disclosure.
2	Acquisitions and Expansion Strategy	Any acquisition and expansion strategy should be safeguarded at all times in order to maintain our competitive position. To that end, the following is a generally accepted position to take when asked about the Company's acquisition and expansion strategy: *"We continually review our goals and objectives to build on the Company's leadership position in providing workforce solutions. Specific information on corporate strategy is proprietary".*
3	Market Rumours	Our policy is not to comment on any market rumours. If it is learnt that rumours about the Company or any of its brands are circulating, authorised spokespersons should state only that it is the Company's policy not to comment on rumours. RHQ Marketing however reserves the right to issue a statement in response to a rumour should it be deemed necessary due to impacts sufficiently injurious to the Company's valuation and reputation.
4	Customers	Our policy is not to discuss or disclose our customer relationships. In fact, many of our customer contracts prohibit us from discussing our relationship. However, upon a customer's request or with prior customer consent and with the Company's corporate approval, we may discuss specific customer relationships.
5	Current on Potential Litigation	Our policy is not to comment on current, pending or potential litigation. Any exceptions to this policy must be approved by RHQ Legal.
6	Handling Inquiries from Students and Researchers	Competitors occasionally pose as students or researchers in an attempt to gather proprietary Company information. Whether you deem the request innocent or not, it is suggested you direct such callers to RHQ Marketing.

1. Overview

We are committed to maintaining a harassment-free, safe and conducive work environment. We understand and acknowledge that every employee should be treated equally with respect and dignity. We have a **zero-tolerance** policy against any forms of harassments and that such conduct of harassment will not be condoned and/or tolerated. We will take immediate action upon becoming aware of such cases or suspicions. Always be mindful to maintain a professional and respectful tone when interacting with colleagues, including on a virtual forum.

This Policy aims to:

(a) Prevent conducts of harassment in the workplace and provides a channel to address harassment cases occurring within the Company; and

(b) Educate employees (including officers, directors, agents, volunteers, interns, contractors, sub- contractors, clients, suppliers, and business partners) to acknowledge that harassment in any form is unethical and unacceptable practice that violates the human rights of persons.

2. Scope

This Anti-Harassment Policy applies to all employees working for us or on our behalf and organisations that we have business dealings with, including employees, officers, directors, agents, volunteers, interns, contractors, sub-contractors, clients, suppliers, and business partners.

3. Illustration of Harassment

3.1 Harassment is when an individual at the workplace feels threatened, abused or insulted by words or behaviour from another individual which is heard, seen or otherwise perceived as likely to cause harassment, alarm or distress. Such behaviour can violate a person's dignity or create an unfavourable work environment for that person, which poses a risk to the person's safety and healthy.

3.2 Harassment conducts includes unwanted physical contact, bullying, intimidation, or offensive, suggestive, humiliating, demeaning or unwelcome jokes, and may relate to a form of discrimination. For clarity, discrimination means any unequal treatment or hostile conduct directed at an individual based on their race, age, gender, sexual orientation, family status, marital status, religion, nationality, disability or any other protected categories under applicable laws, is expressly prohibited under our Code of Ethics.

3.3 Harassment conducts may take place in many forms of work settings, namely, performing any work- related at our premises, client's premises or any locations which the employee is doing business trips. Harassment conducts may occur through different modes of communications such as email, text messaging, social media or phone calls or face-to-face harassment or bullying.

3.4 Examples of harassment include, but not limited to:

(a) **Discrimination of Power** – where an individual of authority creates a hostile work environment for their subordinates;

(b) **Sexual Harassment** – any circumstances which causes an individual to feel sexually violated or to receive unwanted sexual advancements or conducts;

(c) **Cyber Bullying** – any circumstances on any online platform which causes harassment to an individual;

(d) **Personal Prejudice** – any circumstances where an individual is denied benefits or imposed extra burdens due to personal prejudice or beliefs; and

(e) **Psychological or Mental Harassment** – any harassments which affects an individual's mental health, i.e. dismissing valid opinions of an individual or belittling an individual's existence or work.

4. Reporting Incidents of Harassment

4.1 Employees are encouraged to report incidents of workplace harassment through the Employee Grievance Resolution Management procedures (in order of priority) set on the Employee Handbook. When in doubt on reporting or dealing/facing harassment cases, such employees should raise their concerns to their respective managers. Known or suspected violation of this Policy must be promptly reported to your Country HR head or the Regional HR head.

4.2 In making a report, employees should provide as much details as possible, such as names, dates, time of the incident and supporting information or other evidence to help the investigation process.

4.3 The management will investigate, assess and deal with all concerns, complaints/reports and incidents of workplace harassment in a fair and timely manner. Whilst the investigation is taking place, the complainant and witnesses should avoid discussing the incident or complaint with each other or with other employees unless necessary.

4.4 Upon receiving a report/complaint, we will take immediate action or measures to remediate any incidents relating to harassment the best possible way as it thinks fit so as to prevent the recurrence of harassment conducts to such employees.

4.5 The investigation documents, including the findings of investigations will not be disclosed unless necessary to investigate an accident or complaint of harassment, take remedial action or otherwise as required by law.

5. Compliance with this Policy

5.1 Each employee must read, understand and comply with this Policy and avoid any activity that might lead to a breach of this Policy. We expect business partners and organisations that we have business dealings with, to understand and observe this Policy.

5.2 Breach of this policy will be treated as a misconduct and may result in disciplinary actions taken, including termination of employment.

5.3 This Policy shall not be misused by any employee or persons to lodge a false complaint or accusation. A disciplinary action will be taken against any employee that is found liable of misusing this Policy.

6. Action Against Harassers

Any violation to this Policy by any employee shall be subject to corrective or disciplinary action, which may include termination of employment or engagement. We may terminate our relationship with other individuals and organisations working on our behalf or we have business dealing with if they are found to be in breach of this Policy.

1. Scope

This Whistleblowing Policy applies to all employees working at all levels of the Company, including but not limited to the Company's existing and former directors, officers, managers, employees, trainees, part-timers and contractors working on-site at the Company's premises, and families of such persons. All the above-mentioned individuals are eligible to be whistleblowers.

This Policy covers the following areas:

- Fraud or forgery
- Dishonest acts
- Bribery or corruption
- Remove/inappropriate use of Company's assets and records
- Violation of Company policies, material laws and regulations
- Conduct that is an offence under any Commonwealth law that carries a penalty of twelve (12) months or more for imprisonment

This whistleblowing Policy does not cover complaints relating to harassment, discrimination, personal circumstances in the Company, slander, complaints about salary or compensation, complaints about personal relationship, which would normally be dealt with under the Grievance Handling Procedure in the employee handbook.

2. Reporting and Communication Channels

2.1 When in doubt about the best action in a particular situation, you should talk to your managers. In making a report, you should provide as much details as possible, such as names, dates, time of the incident(s) and supporting information or other evidence.

2.2 We will not tolerate any harassment or retaliation of any employee who makes a report in good faith and any such conduct may be subject to disciplinary action.

2.3 The individual should report his or her concerns to the Whistleblowing Committee comprising the CEO, Regional General Counsel, Regional Director - Head of Operations and PAPAC HR Director. The Whistleblowing Committee is responsible for handling all reported cases and ensuring that issues raised are properly resolved by the manager or such parties as appropriate. If the matter is substantiated, it will be referred to the police or other law enforcement agencies where appropriate. In the event that the Whistleblowing report involves any member of the Whistleblowing Committee, the Whistleblower may escalate the report to PERSOL Holdings' compliance office.

2.4 The available communication channels are as follows:

Online reporting form (via Noggin* QR code)	 *Noggin is an online system that is co-managed by PAPAC and Programmed
Email	For complaint **relating to the Whistleblowing Committee**, submit the report to: compliance@persol.jp

3. Confidentiality

All concerns raised will be independently assessed by the Whistleblowing Committee to ensure that they are fairly and properly considered. Any individual making a whistleblowing report can choose to remain anonymous or reveal his or her name. If you choose to reveal your name, we will not disclose it without your consent. We reserve the right to take disciplinary action against any employee who makes a report in bad faith. All reports will be retained for a period of five (5) years from the date of the report, and kept strictly confidential, unless required by law or court order.

4. Protection for Whistleblowers

The Whistleblower shall inform the Whistleblowing Committee immediately if he/she believes that he/she is being subjected to retaliation as a result of raising concerns under this Whistleblowing Policy. The Whistleblowing Committee will take the following steps where possible:

- Assess the protection needs of the Whistleblower;
- Advise the Whistleblower of types of protection available to him/her; and/or
- Listen and respond to any concern of harassment, intimidation or victimisation of the Whistleblower for making the report

Any reporting under this Whistleblowing Policy will not result in disciplinary action unless the Whistleblower makes an allegation despite knowing or believing it to be false or it is made in bad faith. Any employee who victimises or retaliates against the Whistleblower will be subjected to disciplinary action.

The Whistleblower reporting a wrongdoing or improper conduct that he/she has committed will not be relieved from potential prosecution, but such reporting will be taken into consideration in the determination of the disciplinary action against the Whistleblower.

// End //