The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (hereinafter referred to as the 'Act') is the law that provides protection to women against sexual harassment at workplace in India and also details the mechanism in place to deal with complaints of sexual harassment.

Sexual Harassment is defined under the Act to mean the following unwelcome acts or behavior, amongst others:

(a) Physical contact and advances; or
(b) A demand or request for sexual favours; or
(c) Making sexually coloured remarks; or
(d) Showing pornography; or
(e) Any other unwelcome physical, verbal or non-verbal conduct of sexual nature.

The Act provides for the constitution of an Internal Committee by every organization, to which an aggrieved woman can complain to, if she is subjected to sexual harassment.

During the pendency of the inquiry before the Internal Committee, the employer can grant the following reliefs:
(a) Transfer the complainant or the respondent to any other workplace; or
(b) Grant leave to the complainant for a period up to 3 months; or
(c) Recommend to restrain the respondent from reporting on the work performance of the aggrieved woman or writing her confidential report and assign the same to another officer.

Under the Act, an inquiry has to be completed by the Internal Committee within 90 (ninety) days.
On completion of the inquiry, if the Internal Committee comes to the conclusion that the allegation of sexual harassment stands proved, then the Internal Committee can direct the employer to take any one of the following actions:
(a) Written Apology
(b) Warning to the Respondent
(c) Reprimand or Censure
(d) Withholding of promotion or pay rise or increments
(e) Terminating the Respondent from service
(f) Undergoing a counselling session
(g) Carrying out community service.

I hereby acknowledge that I have read and understood the above note that details the key features of the Act and the mechanism in place to deal with complaints of sexual harassment. I further acknowledge that while the Act is restricted to sexual harassment faced by women in a workplace in India, I am entitled to approach appropriate forums under the law for any harassment that is not specifically covered under the provisions of the Act.

Date: 28 October 2024
Place: Bangalore   **Signature:**
Name: Sraban Kumar Pahadasingh
Signature: **Email:**
                                                              Title:
                                                      Company:

CONFIDENTIALITY AGREEMENT

I, the undersigned, contracted by O2F Info Solutions to Infosys to work on an assignment for a client of Infosys acknowledge that:

a. I am allotted to an engagement (either onsite or offshore), where scope of such services provided to any client, will involve processing of information, including both proprietary and Personal Data of employees, Subcontractors, vendors and client, client end users.

b. I am informed that any information that allows the identification of a natural person, either directly or indirectly, is considered Personal Data, including but not limited to information such as an identification number, location data, an online identifier or one or more characteristics specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

c. Infosys Limited and its affiliates (collectively referred as either "Infosys") provide specific written instructions with reference to the processing of Personal Data, pursuant to applicable data protection laws and regulations, including and not limited to laws, regulations, such as DIFC Law No. 5, 2020, LGPD (Brazil), POPIA (South Africa), General Data Protection Regulation (GDPR), UK GDPR, Implementing Laws of GDPR etc. ('Data Protection Legislation").

Notwithstanding the above, which forms an integral part of my engagement with Infosys, I hereby undertake to:

1. Collect and/or process Personal Data only according to the written instructions received by Infosys from the Client, and in any case, according to the applicable data protection provisions, including those set forth in the applicable Data Protection Legislation.

2. Process Personal Data only in strict compliance with the law and the instructions received as part of scope of engagement. In particular, I undertake to make sure that all the data processed as a result of the performance of my services is:
    *   processed only if and to the extent required to fulfil the purposes of processing ("data minimization") for the purposes agreed.
    *   processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful access or processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

3. Observe strictest confidentiality with respect to the personal data I shall collect, process, or access as a result of the performance of my job, and refrain from disclosing it to any other natural or legal person, including co-workers and other staff members, where the

latter are not expressly authorised to access such data by virtue of instructions by contract or law.

This non-disclosure and confidentiality obligations are not subject to any time limits and shall survive termination of my relationship (directly or indirectly) with Infosys. I am aware that any infringement against this obligation or against the applicable Data Protection Legislation may result in significant fines, and potentially cause damage to natural or legal persons, including Infosys.

I am aware of the binding nature of the instructions provided by Infosys and that the breach of any such instructions, and I hereby agree to indemnify Infosys against any such claims or compensations, arising due to any violation of this document.

Name: Sraban Kumar Pahadasingh

Signature: **Signature:**

Subcontractor ID: **Email:**
                                       Title:

Date: 28 October 2024   **Company:**

Place: Bangalore

Security Guidelines and Acknowledgement for

Subcontractors

COPYRIGHT NOTICE

Infosys Limited
Hosur Road
Electronic City, 3rd Cross
Bangalore 560 100
India.
Telephone :(00 91) (080) 28520 261-270
Fax: (00 91) (080) 8520 362
***Website:** www.infosys.com*

Contents

Overview

The purpose of this document is to provide guidelines on Infosys's information security requirements and expectations that subcontractors including their agents, sub-contractors, employees, etc. (hereinafter collectively referred to as "**Subcontractors**") shall understand, comply, and provide signed acknowledgment.

Scope

The process of signing acknowledgment in this document is applicable only to the Subcontractors those who cannot access Security Awareness Quiz (SAQ) intranet portal as they,

- Do not have access to Infosys network
- Are working from client network or client office permanently and has no provision to access Infosys network

Acceptable Usage of IT Resources

Scope

The scope of IT resources used by the Subcontractors includes but not limited to Infosys and/or its client provided network infrastructure, e-mail access, internet access, server access, application access, database access, desktop and laptop computers, printers, network devices, mobile computing devices, software, digital files, electronic or hardcopies of information or data, etc. The terms IT resources and IT infrastructure in this document shall refer this scope.

- Infosys's and its client's IT infrastructure and IT resources shall be used only for authorized business purposes and not for any personal use.
- Prior authorization shall be obtained before any Infosys's or client's property, or asset is removed from the premises.
- Infosys's and its client's IT infrastructure and IT resources shall not be used in any manner engaging in unethical activities, illegal activities, defamation, copyright or trademark infringement, misappropriation of trade secrets, discrimination, harassment, fraudulent activities, unauthorized usage or sharing of information or data and/or access or any action that

impacts reputation and goodwill of Infosys or Infosys's client and/or not in the best interest of Infosys and its clients.

- All Subcontractors shall perform only those activities which are authorized for their respective job roles.

- Subcontractors shall ensure that all adequate measures are taken, and security practices followed while creating or processing or handling Infosys's or Infosys's client's asset or information or data, to ensure that Infosys's or Infosys's client's data or information or assets are protected from unauthorized, malicious, fraudulent access and/or usage.

- The use of inappropriate language in any electronic communication (email, instant messaging, web etc.) is prohibited, including the transmission and/or re-transmission of electronic mail containing illegal, slanderous, libelous, defamatory, abusive, derogatory, threatening, obscene, racist, sexist, or otherwise offensive materials

- Uploading or sharing of Infosys or client internal/confidential/proprietary information or data, code etc. in personal mails, public forums, code repositories (like GitHub, Bitbucket and Stash etc.), online code conversion or decompile tools, blogs, online discussion rooms, social media, cloud storage sites etc. is strictly prohibited.

- Subcontractors shall not engage in electronic mail practices such as spamming, retransmission of chain messages, spoofing, automatic email diversion to external email addresses, unauthorized personal encryption of email or attachments, publishing sensitive personal information or data on social media, etc.,

- Unauthorized sharing of Infosys's and its client's information or data shall not be done.

- Infosys's and/or its client's email ID shall be used for authorized business purpose only and shall not be used for any personal online or offline registrations

- Internet access provided by Infosys, or its client shall not be used in any manner that would be discriminatory, harassing, or obscene, or for any other purpose that is malicious, illegal, and not in the best interest of Infosys or its clients

- Subcontractors shall not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any malicious programs (e.g., viruses, worms, Trojan horses, email bombs etc.) into Infosys's or its client's network

- Irrespective of the work location (Infosys office, client office, home, or any other location), connectivity (corporate LAN, remote access, VPN, Citrix, VDI etc.) and device used (Infosys

provided or client provided or personal), all subcontractors shall always ensure compliance to the requirements explained in this document by implementing and/or adhering to applicable security controls, measures, and practices.

Proprietary of Information

- Infosys reserves the right to monitor and inspect all Infosys property to ensure compliance with its policies and regulations, without notice to the subcontractor and at any time, not necessarily in the subcontractor's presence.

- All electronic information or data created by any subcontractor using Infosys IT resources as explained in the scope of Acceptable Usage of IT Resources above, is the property of Infosys and remains the property of Infosys.

- Infosys reserves the right to access and review such electronic information or data and other digital archives, and to monitor the use of electronic communication as necessary to ensure that no misuse or violation of Infosys policy or any law occurs

- Infosys reserves the right to monitor the use of any of its IT resources as explained in the scope of Acceptable Usage of IT Resources, without notice and for any reason, including, security and/or network management. Subcontractors using this infrastructure shall have no expectation of privacy with respect to any use of the infrastructure.

- Infosys reserves the right to disconnect or revoke the access or block any device connected either by physical or wireless means to Infosys network.

- Infosys reserves the right to access, modify or delete all information or data stored on or transmitted across its network. This includes information or data stored in network folders, mailboxes etc.

Adherence to Infosys's Client Security Requirements

- When working for any of Infosys's clients, subcontractors shall ensure full understanding and compliance to all applicable security requirements, policies, standards, and procedures of Infosys's client.

Protection of Information

- Subcontractors shall ensure all Infosys's and its client's processes and security requirements are adhered, required security controls and practices are followed to ensure confidentiality, integrity and availability of Infosys's and its client's information or data are always protected.

- Subcontractors shall ensure Infosys's and its client's information or data that are entrusted to them is always secured and protected from unauthorized, malicious, fraudulent access and/or usage.

Do's and Don'ts

- ✓ Ensure strong passwords are set for all Infosys or client infrastructure. Do not reveal any Infosys or client infrastructure related passwords (credential of Active Directory / email, VPN, applications, database etc.) to others or allow use of Infosys/client's IT Resources by others. This includes managers, team members, any auditors, family, friends, or any other.

- ✓ Due care (not saving information or data locally, not saving passwords, removal, and deletion of sensitive information or data, avoiding sensitive transactions etc.) shall be taken while using shared/public machines (kiosks) while accessing Infosys information or data.

- ✓ Use your Infosys/Client email ID only for official purposes and shall not share the same in online forms/forums etc.

- ✓ Beware of phishing emails and other fraudulent methods used by hackers like social engineering (the use of deception to manipulate individuals into divulging confidential or personal information or data that may be used for fraudulent purposes), etc.

- ✓ Do not forward chain mails. Do not click on spam or phishing or suspicious email links, attachments, or suspected malwares. Always promptly report them to the respective authorities.

- ✓ Do not indulge in any form of fraudulent activities, like outsourcing the work to unauthorized individuals/groups by means of sharing information or data over screen share, e-mail etc.

- ✓ Always use only licensed and authorized software. Do not violate the licensing terms and conditions and download unauthorized software even if it is for a business-critical need.

- ✓ Refrain from using Unauthorized Peer to Peer (P2P) software and sharing folders.

- ✓ Do not attempt to modify or disable the security tool installed in your laptop like anti-virus etc.

- ✓ Do not share any Personally Identifiable or sensitive Information or data (Including, but not limited to email id, contact number, health information or data, financial information, or data

etc.) of any individual, including Infosys employee(s) /third parties'/Infosys clients with any unauthorized recipients and/ or without the express consent of the concerned individual(s).

✓ Do classify all documents, information, and data as per the sensitivity and adopt appropriate protection measures

✓ Do wear Infosys or client badge/ID card when inside the respective office premises always.

✓ Do not attempt to enter or access areas not authorized to enter. Do not tailgate.

✓ Do follow the secure coding practices applicable to the project.

✓ Do not keep any official printed information or data unattended on the desk or the printer. Use a shredder to securely destroy the printed information or data after its perusal.

✓ Do lock the screen of your computer when unattended or before going away.

✓ Do discuss with your Infosys manager if any query on your security responsibilities, process to follow, etc.

Reporting of Security Incidents

- Subcontractors shall immediately notify any actual or potential incident that might impact confidentiality and/or integrity and/or availability of Infosys information or data or asset and might lead to a security or data breach. Subcontractors shall notify the incident to his or her Infosys manager and Infosys Information Security Group (ISG) via the email ID **icert@infosys.com**

- Subcontractors shall be aware of Infosys's client's security incident reporting procedures and ensure immediate reporting of any actual or potential incident that might impact confidentiality and/or integrity and/or availability of Infosys's client information or data or asset.

Return of Assets

- Upon termination of contract or agreement with Infosys, all Subcontractors shall be required to return assets, including all physical assets and all official documents, information, data, files, emails etc. which they have access to, created or stored in the physical assets, that belong to Infosys or its client, including:

  o Important documentation (e.g., about business processes, technical procedures, and key contact details) stored on portable storage media or in paper form or in the shared storage space provided by Infosys.

- Physical Assets (e.g., mobile devices, laptops, desktops, tablets, smartphones, portable storage devices, and specialist equipment).
- Software
- All official documents, information, data, files, emails etc. which employees have access to, created or stored in the physical assets (including media, documentation, and licensing information or data).
- Authentication hardware (e.g., physical tokens, smartcards, and biometric equipment).

- Subcontractors shall not delete any official documents, information, data, files, emails etc. in the physical assets and shall return all official information and data to Infosys / Infosys client as applicable.

- If a Subcontractor uses his/her own personal equipment for Infosys official work, procedures shall be followed to ensure that all relevant information and data are transferred to Infosys and securely erased from their personal equipment.

Disciplinary Action

- Any Subcontractor found violating any security requirements in this document and/or misusing any of Infosys's or its client's IT resources and infrastructure (like email, internet, instant messaging, collaboration platforms, desktop/laptop, mobile devices, etc.) and/or engaging in unethical, illegal, defamation, copyright or trademark infringement, misappropriation of trade secrets, discrimination, harassment, fraudulent activities, unauthorized outsourcing of work activities, impersonation, malicious activities, unauthorized usage or sharing of information or data and/or access, or any action that violates the security requirements in this document and/or impacts reputation and goodwill of Infosys or its clients, and/or not in the best interest of Infosys and its clients, will be subject to strict disciplinary and/or legal actions as applicable and relevant.

- Subcontractors shall be responsible for all losses which Infosys, or its clients may face due to any breach or violation of security requirements in this document, or any malicious activity listed in the above point, which is attributable to the subcontractor and the company may initiate appropriate disciplinary and/or legal action as applicable.

Acknowledgement

- ✓ I have carefully read, understood and agree to comply with all the requirements, guidelines and Do's & Don'ts in this '*Security Guidelines and Acknowledgement for Subcontractors'* document shared with me.
- ✓ I acknowledge and agree that if I fail to comply with the above undertaking, Infosys Limited and my employer can take all legal actions and claim remedies available under law or contract against me, including damages for breach of this undertaking.

Signature	**Signature:** **Email:**
Full Name	Sraban Kumar Pahadasingh **Title:** **Company:**
Date	28 October 2024
Location	Bangalore
Infosys Emp. No.	
Infosys email ID	
Project Name & Client Name	
Infosys Project Manager's Infosys mail ID	
Subcon's Organization Name	O2F Info Solutions Pvt Ltd