QUADRANT
TECHNOLOGIES

USER ACCESS AND SECURITY AGREEMENT

As a Team Member of Quadrant, I acknowledge that I will be provided with equipment and granted access to the network and necessary systems to perform my job. I understand that I am responsible for safeguarding sensitive and confidential information.

Acknowledgment and Agreement

I acknowledge and agree to the following terms:

- I will not use confidential information for personal gain or allow others to do so.
- I will comply with all company policies and regulations outlined in the privacy and security policies available on the Compliance SharePoint.
- I will not share my user ID and passwords or use another individual’s credentials.
- I will not link my work email to non-work-related accounts or websites.
- I am accountable for all activities performed under my user ID.
- I will securely store my login credentials and will not save them in my internet browser.
- I will exercise caution when opening email attachments or clicking on links.
- I will not excessively use company networks or devices for personal matters.
- I will refrain from accessing inappropriate websites, including social media, gaming, and adult content.
- I will not attempt to access unauthorized systems or information, and I will only access the minimum necessary data required for my job.
- I will not share sensitive or confidential information with unauthorized individuals.
- I will not store sensitive or confidential data on removable media such as USB drives.
- I will ensure that emails containing sensitive or confidential information are directed to the correct recipient.
- I will encrypt emails containing sensitive information by typing “Encrypt” in the subject line or adjusting Outlook sensitivity settings.
- I will avoid using unsecured public networks for work-related tasks.

- If issued portable company devices (e.g., laptops, tablets, mobile phones), I will not leave them in unsecured areas.

Remote Work Responsibilities

When working remotely, I will:

- Follow company and client work-from-home protocols.
- Ensure my work area is secure and protect information from unauthorized access.

Reporting Responsibilities

- If a company-provided device is lost or stolen, I will immediately notify Information Technology Services and the Privacy Officer.
- I will return all company-provided equipment when no longer needed, unless otherwise approved.
- If I am responsible for granting or terminating user access, I will only grant access to authorized individuals and promptly remove access when it is no longer needed.
- I will actively engage with the Privacy and Security Program by reading newsletters, participating in training, and seeking clarification when necessary.

Incident Reporting

I will promptly report any privacy or security concerns to Information Technology Services and/or the Privacy and Security Officers. Examples of reportable incidents include, but are not limited to:

- Compromise of my user ID and/or password.
- Loss of a mobile device used for work.
- Suspicious emails or phone calls that may be social engineering attempts.
- Unauthorized or inappropriate use of company systems or networks.
- Any breach of sensitive information related to organization or client.

Compliance and Consequences

I understand that failure to adhere to privacy and security policies may result in disciplinary action, up to and including termination.

User Access and Security Agreement - Team Member Acknowledgment

By signing below, I confirm that I have read, understand, and agree to comply with the provisions outlined in this agreement. I acknowledge my responsibility to report any known violations of this agreement or other Quadrant Infotech Pvt Ltd policies.

Employee Signature: ________________________________EMPID: ________________

Employee Name: ___________________________________Department: ________________

Date: ____________________________