This Team Compliance and Data Security Agreement (the "Agreement") is entered into by the undersigned team members ("Team Members" or "Employees") and V2Soft India Pvt Ltd ("Company"). The purpose of this Agreement is to ensure that all employees assigned to BCBSM adhere to the highest professional standards in handling sensitive data, maintaining system security, and safeguarding proprietary information.

As a member of the team assigned to BCBSM, you are expected to follow the protocols outlined below to ensure the security and privacy of all client and company assets. Adherence to these guidelines is mandatory and critical to the success of the project, and any violation may result in disciplinary action.

1. General Data Handling

You are required to:

- Ensure that personally identifiable information (PII) and electronic protected health information (ePHI) are shared only with authorized individuals as needed for job responsibilities.
- Access patient data only when explicitly required for your job duties and authorized accordingly.
- Store sensitive data, including ePHI and PII, exclusively on approved company devices and secure storage platforms. Avoid using personal devices or unapproved cloud storage for such data.
- Use encrypted and secure channels when sending or sharing ePHI or PII via email. If required to share this information via email, should use BCBSM outlook only.
- Print or physically copy documents containing sensitive data only when necessary, ensuring they are properly secured.
- Discuss sensitive data such as ePHI only in private, secure environments to prevent unauthorized exposure.

2. System Security & Access

You are required to:

- Use strong, unique passwords and keep them confidential. Do not share your login credentials.
- Lock or log out from all systems and devices when unattended to prevent unauthorized access.
- Access, modify, or disclose sensitive data strictly as part of your authorized job duties, and never out of personal curiosity.
- Do not upload or transfer ePHI information to unauthorized applications or personal email accounts.
- Report any security breaches, suspicious activities, or violations of company policies immediately.
- Comply with all security protocols, including firewalls, access restrictions, and multi-factor authentication, and do not bypass any security measures.
- Ensure antivirus software, security tools, and monitoring tools remain active and operational at all times on company devices.

Mohammad Ashraf B

Mohammad Ashraf B (Apr 8, 2025 15:08 GMT+5.5)

3. Virtual Desktop Interface (VDI) Usage

You are required to:

- Access the VDI only from authorized company devices that are secured by IT.
- Perform all work within the VDI environment without downloading or storing ePHI on local devices.
- Follow company policies regarding the copying or transferring of sensitive data between VDI and local systems.
- Do not use screen capture tools, recording devices, or third-party clipboard managers while in the VDI.
- Log out of your VDI session when not in use to protect against unauthorized access.
- Only use a company-approved VPN when accessing the VDI from unsecured networks, such as public Wi-Fi or from home.
- Do not use or install any software that is not approved by BCBSM and download approved software from (Add BCBSM info)
- software or plugins within the VDI.

4. Source Code Security

You are required to:

- Treat proprietary source code with the highest level of confidentiality and do not share, distribute, or modify it without proper authorization.
- Do not upload internal code repositories to public platforms like GitHub, GitLab, or Bitbucket.
- Do not postscripts or code snippets containing proprietary logic or sensitive information on public forums.
- Ensure that any changes made to the code are authorized and do not compromise the system's security or integrity of sensitive data.
- Do not use AI tools or external code generators that could expose internal source code to third parties.
- Store code only on approved devices and systems and do not use personal devices or external drives for storage unless explicitly authorized.
- Safeguard API keys, credentials, and authentication tokens from unauthorized exposure.
- Do not use or install any software that is not approved by BCBSM and download approved software from (Add BCBSM info)
- Do not access unauthorized internet sites.

5. Device & Data Disposal

You are required to:

- Dispose of documents and devices containing sensitive information following secure disposal procedures outlined by the Company.
- Ensure that printed documents with sensitive data are never left unattended in public or shared areas.

Mohammad Ashraf B
Mohammad Ashraf B (Apr 8, 2025 15:08 GMT+5.5)

6. Enforcement and Penalties

Any violation of the terms of this Agreement may result in one or more of the following actions, depending on the severity and impact of the violation:

- **Suspension or Termination of System Access:** In cases where system security is compromised or data privacy is jeopardized, access to systems or the assigned client project may be suspended or terminated.
- **Legal Action:** If a violation leads to a legal breach or damages that require legal intervention, the Company reserves the right to take appropriate legal action.
- **Financial Penalties:** The Company may impose financial penalties, either in the form of restitution or fines, as deemed appropriate based on the nature of the violation and in accordance with applicable laws.
- **Immediate Termination or Suspension of Duties:** In cases of severe or egregious violations, or where the violation poses an immediate threat to the client's or company's interests, the Company reserves the right to take legal actions, financial penalties and immediately terminate the employee's duties, with or without prior notice.

7. Approval and Deviation

- Any deviation from the above process must be approved by a BCBSM Manager and a V2Soft Manager.

8. Acknowledgment and Agreement

By signing below, I acknowledge that I have read, understood, and agree to comply with all the terms outlined in this Agreement. I understand that any violation of these terms may lead to disciplinary action, including suspension or termination of system access, legal action, or financial penalties.

Employee Name: Mohammad Ashraf B

Employee Signature: Mohammad Ashraf B
Mohammad Ashraf B (Apr 8, 2025 15:08 GMT+5.5)

Date: 04/08/2025