Privacy Policy Acknowledgment Form

Peer2Peer Recovery is dedicated to upholding the highest standards of privacy and data security to protect the personal and sensitive information of all clients, staff, and affiliates. As an employee or volunteer, I acknowledge my responsibility to maintain the confidentiality and security of all information entrusted to me. This acknowledgment form outlines my duties in accordance with Peer2Peer Recovery's Privacy Policy, and by signing, I agree to adhere to these standards.

Privacy and Confidentiality Standards

By signing this acknowledgment, I agree to comply fully with the following privacy and confidentiality obligations:

1. Comprehensive Understanding of the Privacy Policy

- I confirm that I have carefully read and thoroughly understood Peer2Peer Recovery's Privacy Policy.
- I understand that this policy applies to all aspects of my role, including, but not limited to, interactions with clients, handling of client records, communication with colleagues, and adherence to organizational protocols.
- I recognize that safeguarding privacy is integral to Peer2Peer Recovery's mission and legal responsibilities, and that protecting client data is essential for maintaining trust, compliance, and organizational integrity.

2. Protection and Handling of Client Information

- **Scope of Client Information**: I understand that client information encompasses all identifying details (e.g., name, address, date of birth), medical history, health status, recovery progress, session notes, attendance records, and any other data collected as part of Peer2Peer Recovery's services.
- **Physical Security**: I agree to securely store all physical client records in locked, restricted-access areas, and to never leave client files unattended in unsecured areas.
- **Digital Security**: I will adhere to all digital security protocols, including password protection, encryption, and secure login procedures when accessing electronic client data. I agree to log out of systems after each use and to avoid using unsecured networks to access sensitive information.
- **Minimizing Access**: I will only access client information when necessary for my role, and I will limit the scope of information accessed to what is directly relevant to my duties.

3. Permitted Use and Disclosure of Information

- **Authorized Access**: I understand that client information can only be accessed by authorized staff and volunteers who require it to perform their specific roles. I will not

disclose client information to anyone, including family, friends, or external parties, unless explicitly authorized under Peer2Peer Recovery's policies.

- **Disclosure Conditions**: I agree that client information may only be shared under the following conditions:
    - **Client Consent**: When the client provides explicit, written consent for specific information to be shared with designated individuals or organizations.
    - **Legal Requirements**: When disclosure is legally mandated, such as under a court order, or when required by public health or safety laws.
    - **Risk to Safety**: In situations where a client poses a risk of harm to themselves or others, and disclosure is necessary to prevent harm, in accordance with Peer2Peer Recovery's risk management protocols.
- **Restricted Communication**: I understand that I must avoid discussing client information in public or non-secure settings, even indirectly, and that all communication involving client data must occur through approved, secure channels.

4. Digital Security and Proper Data Handling

- **Use of Secure Systems**: I agree to use only authorized and secure systems provided by Peer2Peer Recovery for accessing and storing client information. I will not store client data on personal devices or external systems without explicit permission.
- **Data Transmission**: When transmitting client information electronically, I will use secure, encrypted methods as designated by Peer2Peer Recovery's IT policies. I will not send sensitive information via unprotected email, text messages, or other non-secure platforms.
- **Access Management**: I understand that my login credentials are for my personal use only, and I will not share passwords or access keys with anyone, including other staff members or volunteers.
- **Incident Management**: In case of a security breach, data loss, or unauthorized access, I will immediately notify Peer2Peer Recovery's IT department and Privacy Officer, following the organization's incident management procedures.

5. Protection of Confidentiality after Termination

- **Continued Obligation**: I understand that my confidentiality obligation does not end with the termination of my role. I agree that I am legally and ethically bound to maintain confidentiality indefinitely.
- **Return of Information**: Upon the conclusion of my employment or volunteer role, I will return or securely dispose of all Peer2Peer Recovery materials, including physical documents, electronic files, and any records or resources containing client information.
- **No Retention of Copies**: I agree not to retain, copy, or share any client or organizational data once my employment or volunteer service ends. I understand that failure to comply with these post-service obligations could result in legal action.

6. Incident Reporting Requirements

- **Mandatory Reporting**: I am obligated to report any suspected or confirmed breaches of confidentiality immediately to my supervisor or Peer2Peer Recovery's Privacy Officer. This includes incidents where:
    - Client information is accessed, disclosed, or used without authorization.
    - Data is compromised through a security breach, loss of devices, or accidental exposure.
    - I am uncertain about the security or privacy of any client information.
- **Reporting Confidentially**: I understand that reports of privacy breaches or security incidents will be handled with confidentiality, and I am encouraged to report any concerns without fear of retaliation.
- **Cooperation in Investigations**: I agree to cooperate fully with any investigation related to privacy incidents, including providing relevant information, following corrective measures, and participating in training as needed.

7. Consequences for Non-Compliance

- **Disciplinary Actions**: I understand that any breach of Peer2Peer Recovery's Privacy Policy—whether intentional or accidental—may result in disciplinary actions based on the severity of the incident, including:
    - Verbal or written warnings.
    - Required retraining on privacy and data protection policies.
    - Suspension or termination of my role at Peer2Peer Recovery.
    - Legal action if the breach results in a violation of state or federal privacy laws.
- **Legal Accountability**: I am aware that any serious breach of confidentiality may have legal consequences under data protection laws, and I may be personally liable for damages or penalties if my actions result in harm to clients or the organization.
