Acceptable Use

- Personnel are responsible for complying with ThinkWell Psychiatry policies when using ThinkWell Psychiatry information resources and/or on ThinkWell Psychiatry time. If requirements or responsibilities are unclear, please seek assistance from the Information Security Committee.
- Personnel must promptly report harmful events or policy violations involving ThinkWell Psychiatry assets or information to their manager or a member of the Incident Handling Team. Events include, but are not limited to, the following:
    - Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability to ThinkWell Psychiatry **Information Resources**.
    - Data incident: any potential loss, theft, or compromise of ThinkWell Psychiatry information.
    - Unauthorized access incident: any potential unauthorized access to a ThinkWell Psychiatry **Information Resource**.
    - Facility security incident: any damage or potentially unauthorized access to a ThinkWell Psychiatry owned, leased, or managed facility.
    - Policy violation: any potential violation to this or other ThinkWell Psychiatry policies, standards, or procedures.
- Personnel should not purposely engage in activities that may
    - harass, threaten, impersonate, or abuse others;
    - degrade the performance of ThinkWell Psychiatry **Information Resources**;
    - deprive authorized ThinkWell Psychiatry personnel access to a ThinkWell Psychiatry **Information Resource;**
    - obtain additional resources beyond those allocated;
    - or circumvent ThinkWell Psychiatry computer security measures.
- Personnel should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, ThinkWell Psychiatry personnel should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any ThinkWell Psychiatry **Information Resource**.
- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on ThinkWell Psychiatry time and/or using ThinkWell Psychiatry **Information Resources** are the property of ThinkWell Psychiatry.
- Use of encryption should be managed in a manner that allows designated ThinkWell Psychiatry personnel to promptly access all data.
- ThinkWell Psychiatry **Information Resources** are provided to facilitate company business and should not be used for personal financial gain.
- Personnel are expected to cooperate with incident investigations, including any federal or state investigations.

- Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using ThinkWell Psychiatry **Information Resources**.
- Personnel should not intentionally access, create, store or transmit material which ThinkWell Psychiatry may deem to be offensive, indecent, or obscene.