Integrated Design, Inc. ("IDI") is pleased to offer its Time Bank integration solution online. Since we take your security very seriously, and in order to deliver these solutions as a hosted offering, we have developed a security framework that protects your personal information from outside intrusion by utilizing the most powerful security tools that exist in the marketplace.

Our security framework begins at the user level, where processing is performed by the Secure Sockets Layer (SSL) protocol and 256-bit digitally signed certificate (DigiCert), which ensures that you are truly communicating with our server and not a third party. We can also accommodate the majority of browsers at 128-bit strong encryption. These encryption features are exceptionally powerful to ensure the highest level of security for the data being exchanged with our server.

After a secure connection has been established between your browser and our server, you then provide a valid User ID and Security Password to gain access to the services. Although SSL utilizes proven cryptography techniques, it is important to protect your User Access ID and Security Password from others; therefore, we recommend that you change your Security Password often.

Our server is protected using the latest firewall platform. This platform defends against system intrusions and secures the hardware running Time Bank by preventing associated attacks against systems connected to our server.

All transactions sent to our server must first pass through a filtering router. These routers automatically direct the request to the appropriate server after ensuring the access type is through a secured browser. The routers also verify the source and destination of each network packet and manage the authorization process of letting packets through. This process blocks all non-secured activity and defends against inappropriate access to our server.

In addition to our security measures, users of IDI's Time Bank services also have a responsibility for the security of their information, and should therefore adhere to the following security recommendations: (1) utilize the latest 128-bit encrypted browser; (2) never leave your computer unattended while logged into Time Bank; (3) log off when you are finished using Time Bank; (4) close your browser when you are finished so that others cannot view any information displayed on your computer; (5) use virus protection software to routinely check your computer for viruses; and (6) if you have questions, immediately contact us at 866-846-3226.