**Dow Hosting**

ISP/ASP Policy

|  |
| --- |
| **ISP/ASP Policy** |
| 1. All TDCC information stored at a Service Provider shall be logically separated from non-TDCC information. Yes |
| 1. Separation between outside networks and TDCC computer systems shall be maintained with appropriate physical and/or logical access controls. Outside access to TDCC networks shall be approved by TDCC. Yes |
| 1. The use, sale or release of TDCC’s information or information about TDCC either in detail, summary or aggregate form by the Service Provider is prohibited without prior written approval from TDCC. Agreed, Yes |
| 1. All authentication information such as passwords and pin numbers shall be indecipherable when displayed, and encrypted or protected by an alternative mechanism when stored or transmitted. Yes |
| 1. The Service Provider shall encrypt all TDCC information which has not been approved for public release prior to transmission over public and private networks. Yes |
| 1. The Service Provider shall provide security controls for handling TDCC information in accordance with business requirements. Yes |
| 1. The Service Provider must adhere to appropriate contingency plans as agreed to by TDCC and the Service Provider in the Agreement. Yes, within the boundaries of the agreed SLA. |
| 1. Employees and other representatives of the Service Provider shall not alter or have access to TDCC’s information unless it is in accordance to a negotiated agreement between TDCC and the Service Provider. Yes |
| 1. The Service Provider shall periodically perform security audits and monitor for security vulnerabilities and shall provide these results when requested by TDCC. Yes |
| 1. The Service Provider shall report to TDCC all known security breaches within a time specified by TDCC for the environment in which TDCC’s information resides. Yes |
| 1. The Service Provider shall cooperate with TDCC during fraud and security incident investigations. Yes, within an agreed upon approach. |
| 1. The Service Provider shall permit TDCC full access to TDCC’s information, including the right for TDCC to conduct audits and perform security compliance reviews of the Service Provider's environment. TDCC shall have full access to their data. Stroz Friedberg does not permit onsite audits by any of its clients, with the exception of physically viewing our data centers. SF will answer specific questionnaires provided by TDCC with regards to compliance of policy. |
| 1. The Service Provider shall adhere to applicable industry standards of due care throughout the duration of the Agreement. Yes |
| 1. The Service Provider shall pre-qualify all employees and other representatives who have access to TDCC’s information by means of background checks consistent with TDCC’s criteria and local law. Yes |
| 1. The Service Provider shall be in compliance with all applicable local laws and regulations (e.g., Data Privacy/Protection, Export/Import, Patent, Copyright.) Yes |