

### ***Gramm-Leach-Bliley Act (GLBA) Compliance***

GLBA seeks to protect the personal information of consumers stored in financial institutions by requiring all financial institutions to implement and maintain security measures to protect customer information and prevent unauthorized access and use of customer records. Section 501 in particular, requires all financial institutions to protect the security and confidentiality of customers' nonpublic personal information.

To achieve compliance with GLBA requirements, organizations must establish and enforce internal controls that safeguard the integrity and availability of sensitive financial information at the endpoint.

### ***Sanctuary Helps Public Companies Comply with GLBA for Endpoint Security***

Sanctuary ensures confidentiality and integrity of sensitive financial information by enforcing encryption when copied to removable media. Sanctuary also provides detailed audit information to prove GLBA compliance. With Sanctuary, only authorized users can copy sensitive financial data onto encrypted removable media with complete auditing of that action.

By employing a whitelist approach, Sanctuary is uniquely capable of enforcing application and device usage and control policies, which enables only authorized applications and devices to run or connect to a network, server, terminal services server, laptop, thin client or desktop – facilitating security and systems management, while providing necessary flexibility to the organization to easily enable the use of new/upgraded applications or devices.

Through policy-based control at the endpoints to monitor and control the inbound and outbound flow of sensitive customer nonpublic personal information, Sanctuary complements organizations' GLBA compliance strategy by implementing the proper internal safeguards around application and removable device use:

#### **GLBA Requirement**

##### ***Section 501a – Protection of Nonpublic Personal Information***

Requires each financial institution to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

##### ***How Sanctuary Addresses GLBA Requirements***

Sanctuary assures confidentiality and protects against data theft and data leakage – preventing malware, spyware, hacker intrusive software and keyloggers from executing. By employing a whitelist approach on endpoints, users can only execute software or devices that have been authorized.

## GLBA Requirement

### **Section 501b – Protection of Nonpublic Personal Information**

Requires financial institutions to establish appropriate administrative, technical and physical safeguards including:

1. Insure security and confidentiality of customer records and information
2. Protect against anticipated threats to the security or integrity of such records
3. Protect against unauthorized access to or use of such records which could result in substantial harm or inconvenience to any customer

### **How Sanctuary Addresses GLBA Requirements**

Sanctuary provides safeguards to prevent modification or disclosure of sensitive customer records, including:

1. Assures confidentiality and protects customer information from data theft and data leakage by allowing only authorized applications and portable devices from being used.
2. Protects against anticipated and unanticipated threats because of the whitelist approach that it employs, which allows only authorized applications and devices from executing or connecting to an endpoint.
3. Controls device and application use on a company-wide, user or user group, or computer basis and only allows authorized devices to connect to a machine and only allows authorized applications to run on a machine

| **Pixel IT** Network Solutions | **P** 1800 674 935 | **F** +61 3 9727 9222 |  
| **E** sales@pixel.com.au | **W** www.pixel.com.au |