|  |
| --- |
| STATE OF WASHINGTON  DEPARTMENT OF FINANCIAL INSTITUTIONS  DIVISION OF CONSUMER SERVICES  P.O. BOX 41200 Olympia, Washington 98504-1200  150 Israel Rd., SW, Tumwater, WA 98501 |

|  |
| --- |
| ***DESIGNATED BROKERS QUESTIONNAIRE*** |

**INFORMATION SECURITY**

**Information about the Person Completing the Information Security Questionnaire**

|  |  |
| --- | --- |
| **Name** |  |
| **Title** |  |
| **Phone Number** |  |
| **Email Address** |  |

**How is your institution complying with the federal** [**Safeguards Rule 314**](http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=8c1826dd937ce2fa5ed24ed1f2dd3e18&ty=HTML&h=L&n=pt16.1.314&r=PART)**?**

**314.4 (a)**

**Who has the institution designated to coordinate the information security program?**

**314.3**

**The information security program is required to contain administrative, technical, and physical safeguards in order to:**

**(1) Insure the security and confidentiality of customer information;**

**(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and**

**(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer**

**Describe the administrative, technical, and physical safeguards your institution has in place regarding information security. Particularly, consider the following topics:**

**Business Continuity Management**

Including: Disaster Recovery Plan, Information Security Incident Response Plan, Data Backup

**Data Storage, Transport, and Disposal**

Including: Data Storage, Mobile Devices, Mail Policies, Data Disposal

**Personnel**

Including: Hiring and Departure Policies, Employee Awareness / Prevention Training, User Access, Employee Password Polices

**Physical Security**

Including: Building Security, Clean Desk Policy, Environmental Damage Prevention

**Technical Security**

Including: Network Devices, Device Password Policies, Wireless, Protection (antivirus, intrusion detection system, etc.), Patch Management, Web Applications

**Other**

**How does the institution defend against the following scenarios? How would the institution respond to each scenario if the incident occurred?**

**Scenario One: An employee (or vendor) does not dispose of data properly or loses sensitive information (either electronic or on paper).**

**Defense**

**Response**

**Scenario Two: An employee (or vendor) sends data to incorrect consumer.**

**Defense**

**Response**

**Scenario Three: An employee (or vendor) steals consumer information for leads (either for self or to sell to other loan originators).**

**Defense**

**Response**

**Scenario Four: Social engineering tactics are used against employees to gain access to systems or directly gain sensitive customer information. Social engineering tactics include: phishing, vishing (voice phishing), and tailgating (entering secure areas by following closely behind someone else).**

**Defense**

**Response**

**Scenario Five: Someone outside of the organization physically steals items (electronic devices or paper documents) containing sensitive customer information.**

**Defense**

**Response**

**Scenario Six: Someone outside of the organization electronically steals sensitive customer information.**

**Defense**

**Response**

**314.4 (b)**

**Reasonably foreseeable internal and external risks to information security should be identified. Include a copy of the information security risk assessment.**

**Comments:**

**314.4 (d)**

**List the service providers being used by the company.**

**How are service providers selected?**

**What safeguards do the service providers implement regarding information security? How does the company ensure customer data is protected with the service provider?**

**314.4 (e)**

**How often is the information security program evaluated and adjusted?**

**Information Security:** **Requested Documents**

Please provide the **Written Information Security Program** as required by the federal Safeguards Rule (16 CFR Part 314).

Please also provide, if not included in the Written Information Security Program, all applicable documents listed below:

* **Organization Chart**
* **Disaster Recovery Plan**
* **Security Breach Incident Response Plan**
* **Information Security Incident Log/List**
* **Data Disposal Policies**
* **BYOD (Bring Your Own Device) Policy**
* **Employee training materials** (related to information security)
* **Terms and Conditions of Employment** (related to information security responsibilities)
* **Risk Assessment** (related to technology and information security)