****

**Sample Status Report**

**Disclaimer**

This sample status report was developed to assist various industries and organizations. This report provides one example of how the Qualified Individual can report on the status of the organization’s information security program. The areas included within this document are not intended to be all-inclusive of a comprehensive report, and there may be areas outside of this document that are relevant to your organization and should be addressed. This sample report as presented below should not be seen as the sole report to address this area.

This document is not intended to provide legal, accounting, investment, fiduciary, or information security advice. Please contact your attorney, accountant, information security support provider, or other professional advisor to discuss the application of this material to your particular facts and circumstances.

**Background**

The Standards for Safeguarding Customer Information component of the Gramm-Leach-Bliley Act (GLBA), also known as the Safeguards Rule, requires various institutions to establish an information security program to protect customer information obtained in conjunction with providing financial services.

The Rule requires a Qualified Individual to be appointed to oversee the development of the program and provide a written report regularly, and at least annually, to your board, equivalent governing body, or appropriate senior officer if no such body exists. The report should address:

* The overall status of the information security program and your compliance
* Material matters related to the program, such as risk assessment; risk management and control decisions; service provider arrangements; results of testing, security events, or violations and management’s response; and recommendations for changes

**Instructions**

To use this document for your organization:

1. Delete this cover sheet.
2. Review the sample report thoroughly and edit, remove, or update details to provide sufficient information related to the status of your organization’s information security program.
3. Review your status report periodically and update it to reflect relevant changes.

Please contact us at cybersecurity@capincrouse.com with any questions.

© 2023 Capin Technology LLC

**Annual Report on the Information Security Program**

Date: *<Insert Date>*

To: *<The Board of Directors>*

From: *<Qualified Individual, Information Security Officer>*

**Information Security Program Status and Effectiveness**

The Organization’s Information Security Program (Program) has been reviewed and updated for the year. The updated Program *<is to be approved on xxx, will be approved today, or was previously approved on xxx>*. Management feels that the updated Program adequately addresses customer information security issues and that the Organization is in compliance with the guidelines for safeguarding customer information.

*<Include any other details related to the status and effectiveness of the Program.>*

**Risk Assessment and Management**

The following new implementations were introduced in the previous year and have been incorporated into the Program. The risks associated with each were identified and controls were implemented to mitigate the risks.

*<Include details related to the new technology, products, or services, such as how they were vetted, primary risk areas, how risks were mitigated, policies that were updated to reflect critical changes, etc.>*

The following new general risk areas were also included in the Program. Each risk was assessed and appropriate controls were implemented to mitigate the risks.

*<Include details related to the new or evolving risks that were incorporated into the program, how those risks were mitigated, policies and documentation that were updated to reflect critical changes, etc.>*

**Vendor Management and Service Provider Oversight**

As part of the Program, Management has detailed vendor oversight procedures. All key vendors were evaluated for cybersecurity, operational, and financial strength as warranted. The *<insert appropriate committee, such as IS or IT Committee>* reviewed the necessary documentation on *<insert date>.*

*<List vendors and information reviewed, including security information for critical vendors. Include details about any new vendors within the list. Include any details about concerns noted, follow-up actions that were/are to be taken, and the approval to continue, discontinue, or modify any vendor relationships as a result of the review.>*

**Testing**

Controls defined in the Program were tested by *<insert employee(s) or external firm>* during *<quarterly phishing simulations, the internal audit, cybersecurity assessment, vulnerability scan, external network penetration test, etc.>* The detailed testing results and reports were previously presented to the board *<or will be presented>* on *<insert date>*.

*<Include a brief summary about the scope of testing performed and the overall outcome of the testing>*

**Program Changes**

As a result of the testing, the following changes will be made to the Program, and the Program will be presented to the board at the next scheduled meeting once the changes have been implemented.

*<Include details about new control areas that will be implemented, policies that will be updated, or any other significant changes as a result of testing>*

**Security Breaches or Incidents**

The Organization did not have any incidents resulting in compromised covered information in the previous year. However, the Organization experienced general cybersecurity threats, such as *<insert relevant threats, such as phishing or malware, and how they were addressed>*.

*<If there were incidents, include details related to the incidents or breaches, how they were addressed, information that was compromised, and any other details related to management’s response to each issue.>*

Respectfully submitted,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*<Qualified Individual Name>*

*<Information Security Officer (or relevant position)>*