****

Information Security Program
Annual Report to the Board

[[Organization Name]]

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Table of Contents

[1 Introduction 3](#_Toc124758350)

[2 Information Security Risk Assessment 4](#_Toc124758351)

[3 Information Security Policies 6](#_Toc124758352)

[4 Business Continuity Plan 7](#_Toc124758353)

[5 Incident Response Plan 9](#_Toc124758354)

[6 Vendor Management 10](#_Toc124758355)

[7 Security Awareness Training 11](#_Toc124758356)

[8 Assurance & Testing 12](#_Toc124758357)

[9 FFIEC Cybersecurity Assessment Tool 13](#_Toc124758358)

[10 Additional Topics 15](#_Toc124758359)

[11 Regulatory Updates & Proposed Changes 17](#_Toc124758360)

[12 Request for Approval 18](#_Toc124758361)

# Introduction

*“Each* *organization shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the organization’s compliance with these guidelines. The reports should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.”*

*Interagency Guidelines Establishing Information Security Standards*

The intent of this report is to provide the overall status of the Information Security Program, along with providing any updates to any of the program components. The Information Security Program was designed and is regularly updated to comply with the following laws and regulations:

* The Gramm-Leach-Bliley Act (GLBA)
* The Interagency Guidelines Establishing Information Security Standards
* Supplemental federal and state regulations and guidelines regarding the protection of customer information

To date, each element of the Information Security Program described in this document meets the objectives of the regulations.

The Information Security Program addresses cybersecurity considerations. While information security pertains to protecting information regardless of its format (e.g., paper, electronic, etc.), cybersecurity pertains to protecting the technical assets which process, store, or transmit this data.

#### Roles & Responsibilities

The Board of Directors and senior management are ultimately responsible and accountable for the success of the Information Security Program.

The Board of Directors has designated the Information Security Officer (ISO) as the organization’s representative in all areas related to information security and cybersecurity. The ISO continually monitors, reviews, and makes any necessary changes to the Information Security Program. The ISO reports directly to the Board.

To ensure the goals of the Information Security Program are met, the ISO participates in and coordinates with the following committees / teams on a regular basis.

#### [[Committee Name]]

|  |  |
| --- | --- |
| Role | Name |
| [[Role Name]] | [[Employee Name]] |

# Information Security Risk Assessment

The Information Security Risk Assessment (ISRA) has been reviewed and updated. All reasonably foreseeable threats addressed in the Information Security Risk Assessment were identified in consideration of the eight areas defined in the Interagency Guidelines Establishing Information Security Standards. See the associated Risk Assessment Matrix and Risk Management Plan documents, provided separately, for details.

#### New Threats

The following threats were added to the Information Security Risk Assessment.

|  |  |  |
| --- | --- | --- |
| Threat | Residual Risk | Risk Management Plan |
| Name | ⚫Extreme⚫High⚫Medium⚫Low⚫Insignificant | ⚫Accept⚫Mitigate Further⚫Transfer⚫Defer |

#### Updated Threats

The following threats were modified in the Information Security Risk Assessment.

|  |  |  |
| --- | --- | --- |
| Threat | Residual Risk | Risk Management Plan |
| Name | ⚫Extreme⚫High⚫Medium⚫Low⚫Insignificant | ⚫Accept⚫Mitigate Further⚫Transfer⚫Defer |

#### Removed Threats

The following threats were removed from the Information Security Risk Assessment.

|  |  |
| --- | --- |
| Threat | Notes |
| Name |  |

#### Additional Risk Assessments

In addition to the Information Security Risk Assessment, the organization has conducted the following risk assessments to evaluate the risks associated with threats to specific information assets.

See the Risk Assessment Matrix and Risk Management Plan for each risk assessment, provided separately.

|  |  |  |
| --- | --- | --- |
| Risk Assessment | Overall Risk | Status |
| Name | ⚫Extreme⚫High⚫Medium⚫Low⚫Insignificant | Created / Updated |

# Information Security Policies

The Information Security Policies have been reviewed and updated to identify controls in place to mitigate risk associated with the threats identified in the Information Security Risk Assessment. See the Policy Statements and Approval Log document, provided separately, for details.

#### New Policies

The following Information Security Policies were created.

|  |  |
| --- | --- |
| Policy | Notes |
| Name |  |

#### Updated Policies

The following Information Security Policies were modified.

|  |  |
| --- | --- |
| Policy | Notes |
| Name |  |

#### Removed Policies

The following Information Security Policies were removed.

|  |  |
| --- | --- |
| Policy | Notes |
| Name |  |

# Business Continuity Plan

The Business Continuity Plan (BCP) has been reviewed, updated, and tested to verify adequacy. See the full Business Continuity Plan document, provided separately, for details.

#### Business Processes

The following Business Processes have been identified and assigned a Criticality Level and Maximum Tolerable Downtime (MTD) according to the organization’s Business Impact Analysis.

|  |  |  |
| --- | --- | --- |
| Process | Criticality Level | Maximum Tolerable Downtime (MTD)\* |
| Name | ⚫Critical | 3 Hours |
| Name | ⚫Urgent | 24 Hours |
| Name | ⚫Important | 72 Hours |
| Name | ⚫Normal | 7 Days |
| Name | ⚫Nonessential | 30 Days |

#### Preparedness Controls

The following controls have been identified as key in ensuring the security and resiliency of operations.

|  |  |
| --- | --- |
| Control | Notes |
| Name |  |

#### Completed Exercises & Tests

The following BCP exercises and tests have been performed over the past 12 months.

|  |  |  |  |
| --- | --- | --- | --- |
| Scheduled | Completed | Title | Method |
| MM/DD/YYYY | MM/DD/YYYY | Name | Full-Scale ExerciseLimited-Scale ExerciseTabletop ExerciseTest |

#### Scheduled Exercises & Tests

The following BCP exercises and tests are scheduled for the next 12 months.

|  |  |  |
| --- | --- | --- |
| Scheduled | Title | Method |
| MM/DD/YYYY | Name | Full-Scale ExerciseLimited-Scale ExerciseTabletop ExerciseTest |

# Incident Response Plan

The Incident Response Plan (IRP) has been reviewed, updated, and tested to verify adequacy. See the full Incident Response Plan and Incident Details documents, provided separately, for details.

#### Incidents

The following security incidents have occurred within the last 12 months.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Incident ID | Incident | Severity | Occurrence | Status |
| ID | Name | ⚫Extreme⚫High⚫Medium⚫Low⚫Insignificant | MM/DD/YYYY | OpenClosedResolved |

#### Completed Exercises & Tests

The following IRP exercises and tests have been performed over the past 12 months.

|  |  |  |  |
| --- | --- | --- | --- |
| Scheduled | Completed | Title | Method |
| MM/DD/YYYY | MM/DD/YYYY | Name | Full-Scale ExerciseLimited-Scale ExerciseTabletop ExerciseTest |

#### Scheduled Exercises & Tests

The following IRP exercises and tests are scheduled for the next 12 months.

|  |  |  |
| --- | --- | --- |
| Scheduled | Title | Method |
| MM/DD/YYYY | Name | Full-Scale ExerciseLimited-Scale ExerciseTabletop ExerciseTest |

# Vendor Management

A review of third-party service provider relationships has been performed. See the full Vendor Oversight document, provided separately, for details.

#### Vendors

Contracts were signed or renewed with the following service providers in the last 12 months.

|  |  |  |  |
| --- | --- | --- | --- |
| Vendor | Date | Significance | Risk |
| Name | MM/DD/YYYY | ⚫Critical⚫Significant⚫Insignificant | ⚫Extreme⚫High⚫Medium⚫Low⚫Insignificant |

# Security Awareness Training

Employees were trained to implement the Information Security Program. See the full Training Report documents, provided separately, for details.

#### Training

The following training courses were conducted in the last 12 months.

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Topic | Department / Group | Training Completed (%) |
| MM/DD/YYYY | Name | Name | 100% |

# Assurance & Testing

The Information Security Program’s controls, systems, and procedures have been tested to validate sufficiency. See the full assurance and testing report(s), provided separately, for details.

#### Assurance & Testing

The following security testing engagements were performed in the last 12 months.

|  |  |  |  |
| --- | --- | --- | --- |
| Title | Audit Date | Audit Status | Audit Type |
|  | MM/DD/YYYY | In ProgressComplete | AuditPenetration TestVulnerability AssessmentSelf-Assessment |

# FFIEC Cybersecurity Assessment Tool

[[Organization Name]] has completed the FFIEC Cybersecurity Assessment Tool (CAT) to measure inherent risk and control maturity. See the Cybersecurity Assessment Tool Report to the Board, provided separately, for details.

#### Inherent Risk

Following is the organization’s current inherent risk level, according to the most recently-completed cybersecurity assessment.

|  |  |
| --- | --- |
| Risk Level | Description |
| ⚫Most | An institution with a Most Inherent Risk Profile uses extremely complex technologies to deliver myriad products and services. Many of the products and services are at the highest level of risk, including those offered to other organizations. New and emerging technologies are utilized across multiple delivery channels. The institution may outsource some mission-critical systems or applications, but many are hosted internally. The institution maintains a large number of connection types to transfer data with customers and third parties |
| ⚫Significant | An institution with a Significant Inherent Risk Profile generally uses complex technology in terms of scope and sophistication. The institution offers high-risk products and services that may include emerging technologies. The institution may host a significant number of applications internally. The institution allows either a large number of personal devices or a large variety of device types. The institution maintains a substantial number of connections to customers and third parties. A variety of payment services are offered directly rather than through a third party and may reflect a significant level of transaction volume. |
| ⚫Moderate | An institution with a Moderate Inherent Risk Profile generally uses technology that may be somewhat complex in terms of volume and sophistication. The institution may outsource mission-critical systems and applications and may support elements internally. There is a greater variety of products and services offered through diverse channels. |
| ⚫Minimal | An institution with a Minimal Inherent Risk Profile generally has limited complexity in terms of the technology it uses. It offers a limited variety of less risky products and services. The institution’s mission-critical systems are outsourced. The institution primarily uses established technologies. It maintains a few types of connections to customers and third parties with limited complexity. |
| ⚫Least | An institution with a Least Inherent Risk Profile generally has very limited use of technology. It has few computers, applications, systems, and no connections. The variety of products and services are limited. The institution has a small geographic footprint and few employees. |

#### Cybersecurity Maturity

Following is the organization’s maturity level for each of the domains in the CAT.

|  |  |
| --- | --- |
| Domain | Maturity Level |
| Cyber Risk Management and Oversight | ⚫Baseline⚫Evolving⚫Intermediate⚫Advanced⚫Innovative |
| Threat Intelligence and Collaboration |  |
| Cybersecurity Controls |  |
| External Dependency Management |  |
| Cyber Incident Management and Resilience |  |

# Additional Topics

The following topics have been identified as significant to the effectiveness of the Information Security Program. Following is a summary of each topic, along with identified deficiencies and recommended improvement plans.

#### Vulnerability & Patch Management

Vulnerability and patch management is the process of identifying weaknesses in the organization’s systems and creating a plan to address them in a timely manner. See the organization’s “Vulnerability and Patch Management” policy for details.

Recent security testing revealed the following deficiencies regarding patch management.

|  |  |  |
| --- | --- | --- |
| Deficiency | Status | Response  |
|  | Incomplete |  |

#### Phishing

Phishing is a highly prevalent and dangerous form of social engineering. Falling victim to phishing can result in compromised credentials or the introduction of malicious software. Teaching organization employees to recognize and correctly respond to phishing is one of the best controls for preventing phishing incidents.

The following training was offered on the topic of phishing in the last 12 months.

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Topic | Department / Group | Training Completed (%) |
| MM/DD/YYYY | Name | Name | 100% |

Recent security testing revealed the following deficiencies in the organization’s training program.

|  |  |  |
| --- | --- | --- |
| Deficiency | Status | Response  |
|  | Incomplete |  |

#### Malicious Software

Anti-malware is a program that monitors the organization’s systems to prevent, detect, and respond to forms of malicious software, including ransomware. See the organization’s “Malicious Software Protection” policy for details.

The following malicious software incidents have occurred in the last 12 months.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Incident | Severity | Reported | Completed | Status |
| Name | ⚫Extreme⚫High⚫Medium⚫Low⚫Insignificant | MM/DD/YYYY | MM/DD/YYYY | OpenClosedResolved |

Additionally, recent security testing revealed the following deficiencies regarding the organization’s anti-malware implementation.

|  |  |  |
| --- | --- | --- |
| Deficiency | Status | Response  |
|  | Incomplete |  |

#### Asset End-of-Life (EoL)

When an asset reaches its end-of-life (EoL), this means the asset has reached the end of its useful life cycle or will no longer be supported by the vendor. When an asset reaches end-of-life, this can present significant security and operational risks to the organization. See the organization’s “IT Asset Management” policy for details.

Recent security testing revealed the following assets are operating past their EoL date.

|  |  |  |
| --- | --- | --- |
| Deficiency | Status | Response  |
|  | Incomplete |  |

#### Other Relevant Topics

[[Other relevant topics could include access control, password security, shadow IT, remote access, monitoring, cloud computing, quantum computing, etc.]]

# Regulatory Updates & Proposed Changes

#### Regulatory Updates

Following is a list of new federal and/or state information security related regulations and guidance issued within the last 12 months, along with a summary of the organization’s responses.

|  |  |
| --- | --- |
| Change | Notes |
|  |  |

#### Proposed Changes

Based on a review of the Information Security Program, technological advances, and recent regulatory updates, the following changes are recommended.

|  |  |
| --- | --- |
| Change | Notes |
|  |  |

# Request for Approval

Management requests approval from the Board of Directors for the following items.

* Appointment of the Information Security Officer
* Committee and Team Members
* The Information Security Program Document
* The Information Security Risk Assessment
* The Additional Risk Assessments
* The Information Security Policies
* The Business Continuity Plan (BCP)
* The Incident Response Plan (IRP)